ACCRUENT

ACCRUENT MERIDIAN

ADMINISTRATOR'S GUIDE

2026

Accruent, LLC 11500 Alterra Parkway, Suite 110, Austin, TX 78758 www.accruent.com

Accruent Confidential and Proprietary, copyright 2026. All rights reserved.

This material contains confidential information that is proprietary to, and the property of, Accruent, LLC. Any unauthorized use, duplication, or disclosure of this material, in whole or in part, is prohibited.

No part of this publication may be reproduced, recorded, or stored in a retrieval system or transmitted in any form or by any means—whether electronic, mechanical, photographic, or otherwise—without the written permission of Accruent, LLC.

The information contained in this document is subject to change without notice. Accruent makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Accruent, or any of its subsidiaries, shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Contents

Meridian Enterprise Introduction **22**
What's In This Guide **23**
Who Should Read This Guide **24**
Technical Support **25**
Meridian Architecture **26**
EDM Server Service **28**
Accruent License Server Service **29**
Meridian Content Indexing Service **30**
Meridian Document Content Service **31**
Meridian PowerWeb **32**
Optional Modules **34**
Interprocess Communication **35**
Meridian Data Library **36**
Meridian Data **38**
Meridian Encrypted Data **39**
Document Synchronization Methods Overview **40**
Synchronize via IIS 40
Configuration 40
End-User Procedures 40
Synchronize via Publisher 41
Configuration 41
End-User Procedures 42
Synchronize via Application Integration 42
Configuration 42
End-User Procedures 42
Installation Requirements **44**
Meridian Servers **45**
Meridian Application Server Requirements **46**
Hardware Specifications table 46
Basic Server Requirements and Usage 47
Database Management Systems 47
Browsers and the Internet 49
Server Role Requirements **50**
Document Storage Space Requirements **52**
Server Time Requirements **54**

Network Requirements **55**
System Requirements For Meridian Clients **57**
Hardware Requirements 57
Software Requirements 57
Internet / Intranet Requirements 58
Additional Notes 58
System Requirements For Optional Modules **60**
Language Requirements **61**
Installation **62**
Deployment Strategies **63**
Single-Server Strategy **64**
Multiple-Server Strategy **65**
Deploy For High Availability **66**
Deployment Models **67**
Workgroup Model **68**
Department Model **71**
Enterprise Model **73**
Server Installation Checklist **76**
Prepare For Installation **83**
Install the Server Components **84**
Change License Server Type 84
Requirements for Oracle and SQL Server 84
Installation 85
Install the Server Components Silently **90**
Test Cloud License Server Connectivity **91**
Install the Client Components **92**
Installation 92
Add Components to an Existing Installation 93
Install the Client Components Silently **95**
Control Windows Installer Packages **96**
Command-Line Switches **98**
Example PowerWeb installation 98
Install Or Remove Optional Components **100**
PowerWeb 100
Install Second Language Support **102**
Supported Languages 102

Switch from Non-English Language to English 103
Switch from Non-English Language to Non-English Language 104
Set Language for All Users of a Computer 104
Switch Language in Viewer 104
Upgrade An Existing Installation 106
Deploy Standard Viewer Settings 107
Notes about Functionality 107
Deploy Standard Settings 108
Configure Default PowerWeb User Settings 109
Install the Developer Components 110
What To Expect After Meridian Installation 111
Meridian Folder Structure 112
Move the BC-Meridian Extensions Folder 114
Upgrade Meridian 115
Upgrade Meridian Vaults 116
Upgrade External Tables to Microsoft Access 117
Upgrade Vaults To a Newer Database Engine 118
Upgrade during Restore from Backup 119
Upgrade by Editing Windows Registry 119
Upgrade Meridian Client Computers Automatically 120
Add Components To An Existing Installation 121
Install PowerWeb On a Different Server 122
Install Supplemental Documentation 123
Install the Webhelp Documentation 124
Update locally-hosted webhelp 124
Install the Subscriptions Viewer 126
Installation 127
Test the Viewer 127
Install the Meridian API Service 128
Prerequisites 128
Interactive Installation 130
Unattended Installation 130
Test Installation 130
Install Apryse BIM Server 132
Prerequisites 132
Create application pool and BcBimProxy website 133

Run the BIM Server without a service 134
Additional information 134
Uninstall Meridian 135
Licenses 137
Concurrent Licenses 138
Optional Module Licenses 138
Shared Workspace Support server License 138
Special Licenses 138
Named Licenses 140
Subscription Licenses 141
Comparison Between Subscription Licensing Options 142
License Usage Example 142
Maximum Number of Licenses 142
License Release 143
Obtain Licenses and Authorization Keys 144
Register Licenses - Administrator 145
Enter Authorization Keys 147
Reserve Licenses 148
Restrict Licenses 151
Notes about functionality 151
Administrator Procedures 152
Enterprise Server Administration Console Procedures 152
View Current License Usage 154
Monitor License Usage 155
Monitor License Usage 155
Enable License Server Activity Logging 156
Reassign Named Licenses - Administrator 157
Deploy Multiple License Servers 158
One License Server For All Sites 158
One License Server For Each Site 160
One License Server For All Sites With Local Edm Servers 162
More Than One License Server At the Same Site 164
Create and Maintain Vaults 166
Meridian Enterprise Administrator 167
Toolbar Buttons 168
Common Toolbar Buttons 168

EDM Server Toolbar Buttons ... 169
PowerWeb Toolbar Buttons ... 169
Filters Toolbar Buttons ... 170
Users Toolbar Buttons ... 170
Groups Toolbar Buttons ... 170
Hypertrieve Database Engine ... 171
Create a New Vault ... 172
Notes for using an Oracle database for your vault ... 172
Procedures ... 173
Troubleshooting ... 178
Exclude Existing Property Values When Importing a Vault ... 179
View and Edit Vault Properties ... 181
Create a Subscriptions Database ... 185
SQL Server ... 185
Oracle ... 186
Monitor Vault Status ... 187
Audit Vault Activity ... 189
Activate audit log in PowerWeb ... 190
Create an Audit Log Database ... 191
SQL Server ... 191
Oracle ... 192
Configure the Audit Log Connection ... 193
Install the Audit Log Viewer ... 195
Installation ... 195
Test Audit Log Viewer ... 195
Configure the Audit Log Viewer ... 197
Change Date / Time Format of Viewer ... 197
Change Visibility and Order of Columns ... 198
Hide Viewer Header ... 199
Add an Audit Log Property Page ... 200
Localize the Audit Log Database ... 201
Localize Audit Log Database ... 201
Load Modified Description File into SQL Server Audit Log Database ... 201
Load Modified Description File into Oracle Audit Log Database ... 202
Audited Actions ... 203
Audit Table Structure ... 203

Vault Content Actions 204
Vault Configuration Actions 215
Meridian Explorer Repository Actions 216
File Filters 222
View Current File Filters 222
Add New Filter 222
Change Default Location 223
Vault Consistency Toolkit 224
Prepare the Meridian Server and Vault Configuration 225
Run the Vault Consistency Wizard 227
Run the Wizard 227
Logs 229
Run the Stream Recovery Wizard 231
Create a PowerWeb Location 232
Notes about Authentication 232
Procedures 232
Configure a PowerWeb Location 234
Configure External Domain Only Connections 236
Remove Vault History 237
Rename a Vault 238
Move a Vault 240
Move a Hypertrieve Vault 242
Move the Document Content Files 245
Disable a Vault 247
Data Library 248
Create the Data Library 249
Create a Meridian Explorer Repository 250
Prerequisites 250
Procedures 250
Configure a Data Library Synchronization Job 254
Run a Publishing Job 255
Notes about Functionality 255
Run Immediately 255
Repeat a Past Job 256
Schedule a Single Publishing Job 256
Monitor Background Tasks 257

Monitor Background Tasks ... 257
Filtering the Tasks List ... 257
Inspect a Background Task ... 259
Inspect Background Task ... 259
Export Task Details ... 259
Back Up a Repository ... 261
Report From the Repository ... 262
Backups And Recovery ... 263
Database Recovery ... 264
Level 1 Recovery ... 265
Level 2 Recovery ... 266
Level 3 Recovery ... 267
Prepare For Backups ... 268
Restore Backups ... 271
Notes about System Behavior ... 271
Restore a Vault with Restart After Restore From Backup Wizard ... 272
Restore a Vault with a Command Line ... 273
Change Operating System Versions ... 274
Reindex a vault ... 275
Run the icosnlsver tool ... 275
Create a Recovery Log ... 278
Best Practices ... 278
Recovery Log Wizard ... 279
Create a Recovery Log with a Command Line ... 281
Recover Documents ... 282
Recover All Documents in Vault ... 282
Recover Individual Documents in Vault ... 282
Recover Prior Revisions From Backup ... 284
Archive Documents ... 286
Run the Vault Archive Wizard ... 287
Vault Archive Wizard Results ... 292
Content Indexing ... 293
Configure Content Indexing ... 295
Notes about functionality ... 295
Manage IFilters ... 296
Procedures ... 296

Build and Maintain a Content Index ... **298**
Accelerate Content Index Creation ... **299**
Filter Out Text Noise ... **300**
Restore a Vault That Has Been Indexed ... **301**
Index Securely ... **302**
Troubleshoot Content Indexing ... **303**
Inconsistent Search Results ... 303
Set the Meridian word breaker mode ... 303
No Search Results ... 304
Reinstall Windows Search ... 304
Verify the Windows registry values ... 304
Verify Windows Search Integration Component is Installed ... 305
Repair the Meridian Enterprise Installation ... 305
Optimize Performance ... **306**
Hypercache ... **307**
Configure Hypercache ... **310**
Optimize Server Hardware ... **311**
Dedicated Server ... **312**
Virtualization Software ... **313**
CPU ... **314**
Physical Memory ... **315**
Disk Subsystems ... **317**
Optimize the Server Operating System ... **318**
Configure Application Response ... **319**
Virtual Memory ... **320**
Multiple Network Adapters ... **322**
Multiple Network Protocols ... **323**
Software Disk Compression ... **324**
Software Data Encryption ... **325**
Optimize the Meridian Server Software ... **326**
Configure the EDM Server Service ... **327**
Configure the BatchCallThreshold Setting ... **328**
Configure the ObjectsCacheDepth Setting ... **329**
Configure the BrowseForGlobalGroups Setting ... **330**
Configure the CopyDLL Setting ... **331**
Optimize the Vault Configuration ... **332**

Folders 333
Folder Levels 334
Files Per Folder 335
Multiple Vaults 336
Custom Properties 337
Security Role Assignments 338
Document Type Security 339
Sequence Numbers 340
Optimize Vault Performance 341
Configure the MaximumCacheSize Setting 342
Configure Setting in Administrator 343
Configure Setting using Registry Key 343
Configure the RelativeCacheSize Setting 344
Configure Setting in Administrator 345
Configure Setting using Registry Key 345
Configure the MaximumLogSize Setting 346
Configure Setting in Administrator 346
Configure Setting using Registry Key 346
Temporarily Disable Snapshot Creation 347
Configure the MinimumSnapShotInterval Setting 348
Configure Setting in Administrator 348
Configure Setting using Registry Key 349
Temporarily Disable Snapshot Creation 349
Optimize Client Computer Performance 350
Multiple Network Providers 351
Multiple Network Protocols 352
Viewer Refreshes 353
AutoCAD Font Files 354
Optimize PowerWeb Performance 355
Optimize Antivirus Applications 356
Optimize Batch Operations 357
Remote Site Caches 358
Integrate Meridian Enterprise with Meridian Portal 362
What is Meridian Portal? 362
Prerequisites for the Integration 363
Subscription 363

Technical requirements 364
Set up the Integration 364
Configure the Connection To Meridian Enterprise Server 364
Register the Meridian Enterprise Vault you want to integrate with Portal 364
Vault Configuration 364
Create a Folder Type and Project Definition to use with Portal 365
Configure Scopes 365
Connect Meridian Cloud tenancy in Administration Console 365
Repository Settings 366
Create a Repository Synchronization Job 366
Create a Package Export Job 367
Create and Configure Import Profile 367
Configure VBScript to Assign Document Numbers to New Documents 368
Show Export Package and Import Package Property Pages in PowerWeb 368
Configure Package Scanning Options 369
Save Temporary Package Files 369
Cloud Connector 370
End-User Documentation 371
Meridian Cloud Subscription Levels 372
Cloud Connector Installation 373
Enable Users to Change the Site Cache URL 373
INI Settings 374
Features Section 375
Install Package from a Command Line 376
Example 376
Integrate Meridian With SQL Server 377
How Meridian Works With SQL Server 378
Accruent SQLIO 379
Create the Vault Database Manually 380
Vault Cache Memory 381
SQL Server Vault Backups 382
Integrate With a Separate SQL Server Computer 383
Configure the Windows Account Used By Meridian 384
Create a SQL Server Account For Use By Meridian 386
Configure the SQL Server Account Used By Meridian 388
Configure the type of account used by Meridian 388

Formatting the registry values 389
Migrate a Hypertrieve Vault To SQL Server 390
Move a SQL Server Vault To a Different Folder 391
Monitor SQL Server Vault Performance 392
Minimize SQL Server Log File Size 393
Integrate Meridian With Oracle 394
How Meridian Works With Oracle 395
Accruent ORAIO 396
Vault Cache Memory 398
Oracle Vault Backups 399
EDM Server Service Account Requirements For Oracle 401
Configure the Oracle Account Used By Meridian 402
Configure ODAC for Oracle 403
Prerequisites 403
Configuration 403
Migrate a Hypertrieve Vault To Oracle 406
Restore an Oracle Vault To Another Server 407
Integrate Meridian With Meridian Enterprise Server 411
Configure a Vault For Publisher 412
Create Custom Page Sizes for Meridian Enterprise 416
Enable Print Management Console 416
Create Custom Page Sizes 416
Add Custom Page Sizes to Configurator 417
Configure the Connection To Meridian Enterprise Server 418
Local Workspace 421
When is a document copied to the Local Workspace? 421
When is a document copied from the Local Workspace? 422
Advantages and Disadvantages 422
Filepath Length Recommendations 422
32-bit vs. 64-bit Configurations 423
Use Local Workspaces in Remote Mode 423
Optimize Local Workspace Configuration 424
Best Practice Recommendations 424
How Local Workspace affects disk space 425
Local Workspaces in Offline or Remote Mode 425
Unlock Local Workspace Documents 427

Unlock One Document 427
Unlock All Documents 428
Automatically Synchronize and Unlock Documents 429
Disable Offline Mode 431
Network Administration 432
Meridian Security Requirements 433
Client Computer Privileges 434
Meridian Server Privileges 435
PowerWeb Server Privileges 436
Allow PowerWeb Access Through a Firewall 437
Security Delegation 440
Meridian Support For Microsoft Active Directory 442
Active Directory Security Problems 443
Grant Domain Privileges With a Service Account 444
Create Service Account 444
Non-Admin Service Accounts 446
Grant Domain Privileges To the Meridian Server 449
DCOM Problems 450
Enable DCOM 451
Enable DCOM on Client Computers 451
Enable DCOM on Meridian Server Computers 451
Configure DCOM Permissions 452
Grant permissions in DCOM applications 452
Configure the DCOM Identity Of Remote Services 453
Use Meridian With Nested Groups 454
Use Meridian With Multiple Domains 455
Grant Membership Query Access 456
Configure Computer Name Resolution 458
Run Accruent License Server On a Different Computer 459
Meridian User Administration 460
Role-Based Security 461
Create and Edit User Accounts 462
Create an Account 462
Edit an Account 464
Create and Edit User Groups 466
Create User Group 466

Synchronize User Groups With Active Directory ... **467**
Notes about functionality ... 467
Procedures ... 468
Command Line Parameters ... **470**
Map the User Properties And Groups ... **471**
Edit User Property Mapping ... 471
Edit User Group Mapping ... 473
Create a Rescue Account For Security Administration ... **474**
Secure the Rescue Account ... **475**
Create an Impersonation Account for Vault Access ... **476**
Specify a Mail Server ... **477**
Specify One Mail Server for all Vaults ... 477
Specify Different Mail Server per Vault ... 478
Administer Meridian Enterprise Remotely ... **479**
Remote Access Support ... **480**
Reserve Licenses For Remote Access ... **482**
Prepare the Meridian Server For Remote Access ... **483**
Prepare the Remote Access Host Computer ... **484**
Notes about functionality ... 484
Procedures ... 484
Prepare the Remote Access Client Computers ... **486**
Configure OpenId Connect ... **488**
Troubleshoot Server Performance and Stability ... **490**
Configure the Application Event Log Filter ... **492**
Configuring the Windows Performance Monitor ... **493**
System Status Reporting ... **495**
Create a System Status Report ... **496**
Review the Server Configuration Information ... **500**
Event Logs ... **503**
Review the System Event Log ... **504**
Review the Application Event Log ... **505**
Windows Registry Keys ... **507**
Server Registry Keys ... **508**
HKEY_CLASSES_ROOT\CLSID ... **509**
HKEY_LOCAL_MACHINE ... **510**
HKEY_LOCAL_MACHINE\Software\Cyco ... **511**

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian 512
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\<PatchLevel> 513
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\File System\Connections 514
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\File System\Parameters 515
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\File System\Shares 516
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Hypertrieve 517
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores 520
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<vaultname> 521
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<vaultname>\CompoundItemService 524
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<vaultname>\DataServer 528
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<vaultname>\RegisterBehaviors 529
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<vaultname>\Services 530
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<vaultname>\StreamService 531
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\OML 532
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\OML\AMFSSharePath 536
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\OML\AMServerManagerAccount 537
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server 538
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server\Licensing 545
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server\UserDatabase 547
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink 548
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\Auth 559
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\LockOnCheckOut 560
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\Published Locations\<ID> 561
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server for a format string 563

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\Style Sheets 564
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\UserPreferences\Default 565
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\UserPreferences\Default\Find Templates 571
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\WelcomeScreen 572
HKEY_LOCAL_MACHINE\Software\Wow6432Node 573
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\InetStp\Components 574
Client Registry Keys 575
HKEY_CURRENT_USER 576
HKEY_CURRENT_USER\Software\Cyco\AutoManager View Control2 577
HKEY_CURRENT_USER\Software\Cyco\AutoManager View Control2\Settings 578
HKEY_CURRENT_USER\Software\Cyco\AutoManager View Control2\Settings\AVLandscape 579
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion 580
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Administrator 581
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMDocUpdateUtl\Settings 582
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMDownload 583
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMEdmUI 584
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMEdmUI\Settings 585
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMFind\Settings 586
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHook\Contexts 587
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHook\Contexts\<executable> 588
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHook\Contexts\<executable>\Dialog Detect 589
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHook\Contexts\<executable>\Last View 590
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHook\Contexts\<executable>\Quick Find 591
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHookTray\ForceList\<executable> 592
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHookTray\RejectList\<executable> 593
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHookTray\Settings 594
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMLink\Settings 595

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMOfficeAddIn ... 596
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMOfficeAddIn\Excel ... 597
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMOfficeAddIn\PowerPoint ... 598
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMOfficeAddIn\Word ... 599
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMPersistEnv\Settings ... 600
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AmSldWorksEx\Settings ... 601
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMStationEx\Settings ... 602
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMSync\Settings ... 603
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMVault\Most Recent Opened Vaults ... 605
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMWFMTUI\Init ... 606
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\<application>\Layout\BarLayout-ToolBarManager ... 607
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\<application>\Most Recent Opened Vaults ... 608
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\<application>\Most Recent Opened Workareas ... 609
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\<application>\Settings ... 610
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\<application>\Settings\Assistant ... 615
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\<application>\Settings\Columns\<GUID> ... 617
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\<application>\Settings\<MachineName_VaultName>\Commands ... 618
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AssetManagement 619
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AutocadLink ... 620
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\BCSharedFolderSync\Settings\Log ... 624
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\CCL\Settings ... 625
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Client ... 626
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\Currentversion\Client\Bcsitecacheauth ... 627
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Client\Settings ... 628
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Configurator ... 637

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Configurator\Settings 638
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\InventorLink 639
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\LotusManagerUI 641
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\MicroStationLink 642
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\OfficeClient 643
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Offline\Settings 644
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\ScriptEditor 645
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\ScriptEditor_Full 646
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\UIBeh 647
HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\WPTEditor 648
HKEY_LOCAL_MACHINE 649
HKEY_LOCAL_MACHINE\Software\Cyco 650
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian 651
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\<PatchLevel> 652
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion 653
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMAdmin 655
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMDownload 656
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHook 657
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHookTray\ForceList\<executable> 658
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHookTray\RejectList\<executable> 659
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHookTray\SupportedTypes 660
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMOfficeAddIn\Excel 661
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMOfficeAddIn\PowerPoint 662
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMOfficeAddIn\Word 663
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMOMLUI\SafeProperties 664
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AssetManagement 665
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AutocadLink 666
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client 671
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\Currentversion\Client\Bcsitecacheauth 680

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client\Options for all scanners 681
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\ICWLink 682
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\InventorLink 683
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\MicroStationLink 685
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\RevitLink 686
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager View Control2 687
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager View Control2\Settings 688
HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager View Control2\Settings\AVLandscape 689
HKEY_LOCAL_MACHINE\Software\Microsoft\Visio\AddIns\AMOfficeAddIn.AMOfficeAddIn 690
HKEY_LOCAL_MACHINE\Software\Wow6432Node 691
HKEY_CLASSES_ROOT 692
HKEY_CLASSES_ROOT\BlueCielo 693
Meridian Task Server 694
Set Up the Task Server 695
Set Up Task Server 695
Set Task Server Computer Name 695
Task Server System Requirements 697
Task File Management 700
Task Server With PowerWeb 701
Submit a Task 702
Reset method 703
Syntax 703
Remarks 703
Example 703
Set method 704
Syntax 704
Remarks 704
Submit method 705
Syntax 705
Remarks 705
Apryse / PDFTron Local Fonts 706
Configure Apryse / PDFTron Local Fonts in PowerWeb 707
Configure Apryse / PDFTron Local Fonts in Explorer 708
Configure Third-Party Identity Provider: Meridian-to-Okta 709
Prerequisites 709
Meridian-to-Okta OIDC Configuration tool 709

Windows Installer Package Custom Actions **711**
SQL Azure Database Creation Script **713**
Prerequisites 713
Required script files 713
Configuration file settings 714
Script arguments 714
Procedures 715
Troubleshooting 716
SQL Server Database Creation Script **717**
Create a Meridian Explorer Repository Database on the Database Server 717
Oracle Database Creation Script **720**
Create a Meridian Explorer Repository Database 720
Windows Event Log IDs **721**
Service Account Usage **725**
Renditions Updater Tool **727**
Use the Tool 727
Use Command-Line Options 729
Glossary **732**
Index **748**

Meridian Enterprise Introduction

The Meridian Enterprise product suite is an on-premises engineering document management system (EDMS) and asset lifecycle information management (ALIM) Accruent solution. Meridian Enterprise streamlines engineering-related business processes in specific industries including chemicals, pharmaceuticals, oil and gas, metals and mining, and utilities. Meridian helps your organization manage technical documents and drawings throughout its lifecycle, providing a centralized repository to store, organize, and control engineering documentation.

Meridian Enterprise includes:

- **PowerWeb**: Create and modify engineering data.
- **Explorer**: Search and retrieve engineering information.
- **Configurator**: Customize document types, workflow, roles, and other organizational procedures.
- **Administrator**: Manage users, licenses, and vaults.
- **Administration Console**: Manage users, licenses, jobs, repositories, and other settings.
- **Application Integration**: Streamline working with file-based applications by utilizing site cache and managing local workspace.
- **Microsoft Office link**: Synchronize metadata and references with Microsoft Office applications.
- **Autodesk links**: Synchronize metadata and references with AutoCAD family, Revit, and Inventor.
- **MicroStation link**: Synchronize metadata and references with MicroStation.

Meridian Enterprise supports regulatory compliance. it includes an FDA module to help your organization maintain the integrity and traceability of its documentation. The Meridian Asset Management module enhances, automates, and streamlines asset operations throughout their lifecycle by linking them with engineering content such as drawings and technical specifications.

Meridian Enterprise can integrate with Meridian Portal, a web application for internal and external collaboration in engineering projects. Contact your Accruent account representative for further information.

What's In This Guide

This guide describes the system requirements, licensing, installation, and administration of Meridian Enterprise. Usage of the Meridian clients is documented in the *Meridian Enterprise User's Guide*. Configuration of Meridian vaults is documented in the *Meridian Enterprise Configuration Guide.*

This guide includes the following information:

- An introduction to this guide, who it is meant for, and how to use it.
- Instructions on surveying your computing environment to confirm that it can adequately support Meridian.
- Explanations of the purposes of the various services and other components that make up a Meridian system.
- Step-by-step instructions for the Meridian installation process on server and client computers, installing different options, and installing software upgrades.
- How Meridian licensing works, how to install licenses, and how to best manage licenses.
- Everything you need to create and maintain Meridian vaults.
- Your guide to emergency preparedness.
- How to create Meridian users and groups for configuring document workflow definitions and project workflow definitions.
- How Meridian security roles work together with vaults.
- How to configure document content indexing so users can search for text contained within documents.
- Guidelines for getting the best performance out of your Meridian system.
- Details of how Meridian works with Microsoft SQL Server as its vault database engine.
- Details of how Meridian works with Oracle as its vault database engine.
- How the Meridian local workspace improves client-side performance and how to optimize it.
- Networking topics relevant to Meridian operation and performance.
- Useful tips that can improve Meridian performance.
- Setup overview and installation steps for Meridian PowerWeb server administration.
- Important supplemental information.

Who Should Read This Guide

This guide is intended for Meridian server administrators. Readers should be familiar with, and have experience in:

- General computing concepts
- Microsoft Windows® server and workstation operating systems administration
- Microsoft Windows networks
- Microsoft Internet Information Services administration
- Microsoft SQL Server or Oracle database administration
- *the Meridian Enterprise User's Guide*

Technical Support

Technical support for Accruent products is available from a variety of sources if you have an active support contract. Your first source of support is the authorized contacts designated by your company to participate in the support contract. They are the persons that are responsible for resolving problems with Accruent software before contacting outside sources of support. If your company works with a Accruent Partner, that partner is your second source of support. Accruent Partners are responsible for providing technical support to their customers in order to maintain their status as Accruent Partners. Accruent will assist the partner company, if necessary, to help resolve your problem. If your company is a direct Accruent customer, your authorized contacts may communicate directly with Accruent to resolve your problem.

Accruent Partners and direct customers have access to all of these Accruent technical support resources:

- Support Cases: Around the clock support issue entry, update, and status
- Meridian knowledge base: Continuously updated problem solutions, minor releases, updates, and how-to articles about advanced techniques
- Email notifications: Immediate alerts to support issue status changes
- Telephone support: Direct access to highly qualified software support engineers with extensive experience in Accruent products

The available support contract options, terms, and other details are described in documents that are available from your Accruent Partner.

Meridian Architecture

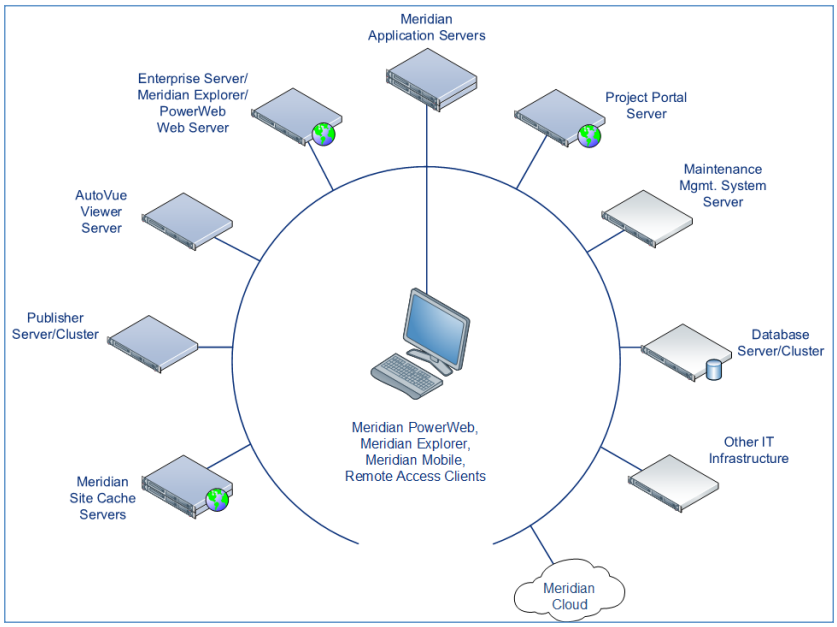
Meridian is primarily a client/server application, which means that some parts of the application run on a server and some parts run on client computers. A Meridian system can have several possible client processes and several server processes. The server processes are typically run on a single server. To see these server processes, use the **Manage** shortcut menu option of **My Computer** on the Meridian application server, or open **Services** from the **Control Panel**.

Below is a list of the Meridian server services that are available:

- AutoManager EDM Server
- Accruent License Server
- PowerWeb web server (Microsoft Internet Information Services)
- Meridian Document Content Service - provides document content to EDM server for indexing
- Meridian Content Indexing Service - hosts the IFilters. An IFilter takes a file and filters out what the readable text is in the file. This text is fed into Windows Search and indexed.

These services are managed with the Meridian Enterprise Administrator tool, although basic operations such as starting and stopping the services can be performed directly with the Services applet. The various client interfaces are described in the *Meridian Enterprise User's Guide*, which you should read as well as this *Administrator's Guide*. There is one other client-like interface, named Configurator, that is used to configure vaults for different requirements. The *Meridian Enterprise Configuration Guide*describes the usage of Configurator.

Although the deployment architecture of a basic Meridian-based system is fairly simple, Meridian can be the cornerstone of a enterprise content management system that is fully integrated with your existing infrastructure, similar to the following figure.



Additional configurations are possible as described in Deployment Strategies.

EDM Server Service

The main process of Meridian Enterprise is the EDM Server service. It appears as **AutoManager EDM Server** in the **Services** applet of your **Control Panel**. This service is responsible for all communication between the different clients with the available databases. All document management logic (including security) is built into this service, so any access to a vault will always have to go through the EDM Server service.

Meridian vaults may be stored in either Microsoft SQL Server or Oracle databases that reside on either the Meridian application server or another server.

The vaults may also be stored in the Accruent database format named Hypertrieve. This is a low-overhead, object-oriented database that is optimized for Meridian. This database engine runs in the same process as the EDM Server service and therefore the engine cannot run on a separate server.

Accruent License Server Service

The Accruent License Server service grants and reclaims licenses for all the Meridian clients, optional modules, and vaults on the same local area network. It manages licenses that have been assigned to specific users or on a concurrent user basis with first come, first served priority unless licenses have been reserved. The service can run on a non-dedicated computer separate from the EDM Server service, but because of its relatively low overhead, it is typically more convenient to run on the same computer. There should be only one instance of the License Server service running on a local area network. For organizations with multiple Meridian sites, each site requires one license server regardless of any wide area network connectivity between the sites.

The name of the computer running the Accruent License Server service is encoded in the transaction key of each Meridian license. Therefore, you should not rename the license server computer or move the service to another computer while Meridian is in production use. If the name of the license server changes, *you must re-register the license for installation.*

Meridian Content Indexing Service

The **Meridian Content Indexing Service** hosts the IFilters for the EDM server content indexing. An IFilter takes a file and filters out the readable text in the file. The text is then fed into Windows Search and indexed.

This service appears as **Meridian Content Indexing Service** in the **Services** applet of **Control Panel**. It should be configured to run automatically on startup of the machine.

Meridian Document Content Service

The **Meridian Document Content Service** provides the contents of your documents to the EDM for indexing. It appears as **Meridian Document Content Service** in the **Services** applet of **Control Panel**. It should be configured to run automatically on startup of the machine.

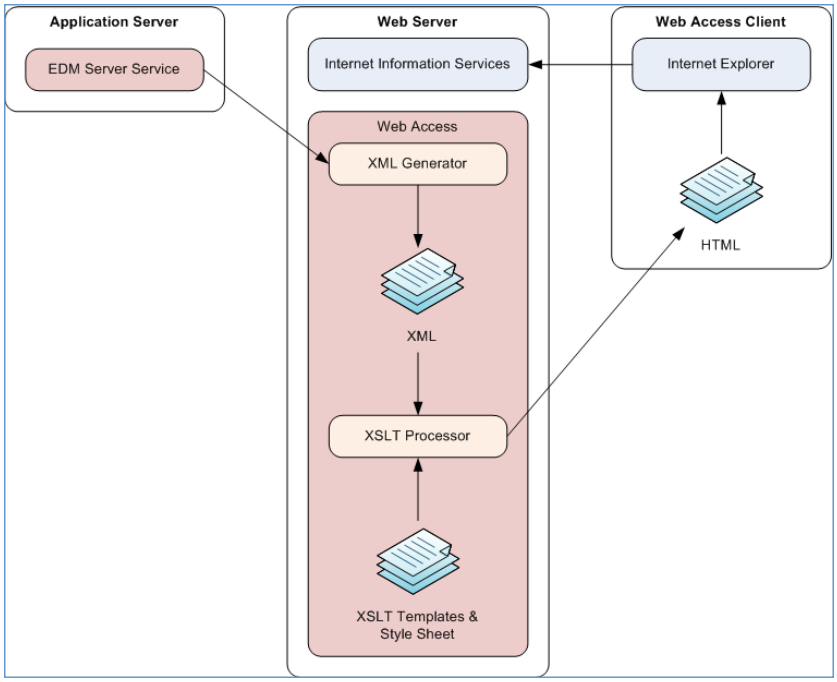
Meridian PowerWeb

Enterprise Server is required to run PowerWeb.

Meridian allows vaults to be accessed through its PowerWeb client using supported web browsers and Microsoft Internet Information Services (IIS). PowerWeb provides the web application hosted by IIS and the web browser acts as the client. A System Administrator publishes a vault as a website in IIS using the Meridian Enterprise Administrator tool.

Meridian PowerWeb is an Internet Server Application Programming Interface (ISAPI) application that runs as part of Microsoft Internet Information Services (IIS). PowerWeb processes requests from web browsers, retrieves data from the AutoManager EDM Server, and passes information back to the web browsers in the form of HTML pages.

Inside PowerWeb, HTML pages are created as illustrated in the following figure:



PowerWeb first creates XML files that contain pure data (no presentation) to be exposed by PowerWeb. The XML pages are then converted into HTML. During this step, information about the way the data should be presented on the screen is added. How the information is presented is determined by a set of templates (`*.xsl`), which are encoded in XSLT, and a style sheet named `amm.css`.

By default, the `.xsl` templates are located on the IIS server in the `\Inetpub\AMM\Templates` folder, and `amm.css` is located in the `\Inetpub\AMM\Src` folder. Due to the complexity of XSLT, we do not recommend customizing these templates. For

more information on customizing PowerWeb, see the *PowerWeb* section in the *Meridian Enterprise Configuration Guide*.

See our Document Synchronization Methods Overview to learn about the three methods you can use to synchronize document contents, title blocks, and references with PowerWeb.

The Meridian PowerWeb application includes PDFTron viewing technology that provides zero-install PDF viewing in PowerWeb and Meridian Explorer. To improve the viewing performance of PDF files that contain thousands of hyperlinks, see the RemoveLinkAnnotations registry value.

Optional Modules

The optional Meridian modules (Asset Management Module, Publisher, and so on) are implemented either as stand-alone server executables, Internet Information Services applications, built into the EDM Server service, or a combination. For example, the Meridian Explorer module is made up of a stand-alone server executable and an IIS application, which can each be installed on a different server and accessed by Internet Explorer clients.

For more information on the architecture of particular Meridian modules, refer to each module's documentation.

Interprocess Communication

The Microsoft Distributed Component Object Model (DCOM) protocol is used for all communication between the Meridian LAN clients and the AutoManager EDM Server service. All communication between the various server services also uses DCOM, which relies on the Transmission Control Protocol/Internet Protocol (TCP/IP) to run within a network environment. PowerWeb clients use the HyperText Transfer Protocol (HTTP or HTTPS), which runs on top of TCP/IP, to communicate with the Internet Information Services service.

Meridian Data Library

The Meridian Data Library is an optional component that can be installed with the Meridian server components. It provides a synchronized replica of the document metadata of one vault. The metadata can be stored in a SQL Server or Oracle database. The Data Library is a subset of the functionality that is provided by Publisher. Specifically, it is a publishing job template that omits the project folder and repository configuration features of the regular publishing job template.

The Data Library can be used in two scenarios:

- As a data source for your favorite reporting application or for more complex reports than can be configured in Meridian. You can configure reports against the Data Library using any application that supports SQL Server or Oracle as a data source, for example, Microsoft SQL Server Reporting Services or SAP Crystal Reports.
- For use with the Meridian Explorer client as a read-only alternative to PowerWeb. By installing Meridian Explorer client licenses, the Data Library can be accessed using all of the capabilities of Meridian Explorer from a web browser.

To add more flexibility to the configuration, you can install an Meridian Explorer Server license to unlock all of the potential of Meridian Explorer.

The primary differences between these three configurations are summarized in the following table.

Data Library feature comparison

Feature	Data Library	Data Library + Explorer Client	Explorer Server + Explorer Client
Database server	Must be the Meridian application server	Must be the Meridian application server	Any SQL Server or Oracle server
Source systems	One Meridian vault	One Meridian vault	Multiple sources of different types can be consolidated into each repository
Repositories	One	One	One or more
Repository contents	All documents, all properties, not configurable	All documents, all properties, not configurable	Configurable documents and properties

Feature	Data Library	Data Library + Explorer Client	Explorer Server + Explorer Client
Renditions	Not supported	Not supported	Supported by optional Publisher rendering modules
Client interface	None	All Explorer Client functionality	All Explorer Client functionality
Client Configuration	None	All Explorer Client options	All Explorer Client options
Document content access	Not supported	Read-only native document content accessible from vault only	Read-only native document and/or rendition content accessible from vault or Explorer repository
Project folders	Not supported	Not supported	Supported
Redlines and feedback properties	Not supported	Supported	Supported

The Data Library is an excellent introduction to other Accruent products:

- Meridian Explorer: The Data Library can be upgraded to all of the features and benefits of Meridian Explorer with the addition of Meridian Explorer server and client licenses. Meridian Explorer can provide engineering content to your entire enterprise. The Meridian Explorer client provides extensive search, viewing, and printing capabilities. For more information about the Meridian Explorer, see the *Meridian Enterprise Server Administrator's Guide* and the *Meridian Explorer User's Guide*.
- Meridian Publisher: The Data Library uses a subset of the Meridian Publisher components to synchronize data between the Meridian vault and the Data Library. Installing the entire Publisher solution and licenses allows you to publish metadata and documents (optionally rendered to other formats) to and from other destinations, such as other Meridian Enterprise vaults, a Windows file system, SharePoint, or other document management systems.

Meridian Data

Meridian stores information about the documents in a vault (metadata) in a database (Hypertrieve, SQL Server, or Oracle). The actual documents in a vault are stored in a secure folder structure that is completely managed by Meridian. This folder structure is called *streams* data, and is invisible to users and applications; it can be accessed only by the AutoManager EDM Server service. This service makes the files accessible for users and applications depending on the users' security privileges and the documents' workflow and revision status.

The vault database can be accessed only by Meridian and may be located on the same server as the AutoManager EDM Server service (using Hypertrieve) or on another server (using SQL Server and Oracle). The streams data can be located on the Meridian application server (the default), or on a file server or other storage device accessible by Windows via a URL.

To improve system performance for remote users who have a local web server, frequently used documents and data can be cached on the server.

Meridian Encrypted Data

Meridian Enterprise does not encrypt documents or their metadata in any way. That data is stored in secured databases. We do not recommend encrypting the database files as explained in Software Data Encryption.

However, Meridian Enterprise does use the Blowfish encryption algorithm with key lengths varying from 40 to 128 bits for small amounts of non-document related data:

Encrypted data

Data	Key Length (bits)	Description
Licenses	128	Copy protection
License registration return key	64	Used to generate license authorization keys
SQL Server and Oracle account passwords	40	User account protection
Site cache	128	Password protection

This encryption places Meridian Enterprise in Export Control Classification Number (ECCN) 5D992 for the United States by the Bureau of Industry and Security and for Europe by Regulation 428/2009. For more information, see the Wikipedia article Export Control Classification Number.

Document Synchronization Methods Overview

There are three different methods you can use to synchronize document contents, title blocks, and references with PowerWeb. You can use one or more of these methods in the same environment. The methods are listed below, from most desirable to least desirable.

Synchronize via IIS

Some file types can be synchronized directly through PowerWeb via IIS. Learn more about how PowerWeb uses IIS.

- **Benefits**: Synchronization is done immediately after a workflow transition is completed. Specialty software is not needed to update documents supported by this method.
- **Drawbacks**: Not all file extensions are supported.

Configuration

1. Navigate to the HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink registry key in the Windows Registry Editor.
2. Modify the **SynchronizeDirect** setting so that it contains the file extensions you want to synchronize via IIS.

   The file extensions must be entered as a semicolon-delimited list. The supported extensions are as follows: dst; dgn; dwg; doc; docx; docm; xls; xlsx; xlsm; ppt; pptx; pptm; vsdx; vsdm. If you remove one of the extensions from this list, it will no longer synchronize immediately via PowerWeb after a workflow transition is completed.

   A use case for when a System Administrator may want to remove a file extension from this setting is if they wanted to run a Macro in Microsoft Office. In that scenario, they would remove the appropriate file extension from the **SynchronizeDirect** setting and create a publishing job for that file type.

End-User Procedures

The following end-user procedures are impacted by this configuration:

- *Run a Workflow Transition on a Project*
- *Route a Document In a Workflow*

To read these procedures, see the *Meridian Enterprise User's Guide*.

Synchronize via Publisher

Publisher provides links to the most common engineering document management systems. Publisher also includes rendering modules for the most popular engineering content authoring applications. See the *Rendering Modules* article in the *Meridian Enterprise Supported Software* document for a list of file extensions and the modules that support them.

- **Benefits**: Some file extensions require specialty software for editing. This method allows users to edit documents without needing the software installed on their workstation.
- **Drawbacks**: Synchronization is NOT immediate, but instead is asynchronous. While Publisher is processing the synchronization, the affected document will be locked.

Configuration

For cluster node scanning to work when using SQL Server, the Publisher nodes need to have the SQL driver installed, and they need to be able to connect to the SQL Server configuration database. This is a requirement for the *Create And Edit a Rendering Profile* procedures in step 2.

To configure synchronization via Publisher:

1. Configure a Vault For Publisher.

   The **Publisher Jobs** settings cannot be configured until after you have created publishing jobs in step 3 below.
2. Create a rendering profile for the rendering module you want to use for your publishing job.

   To learn how to create a rendering profile, see *Create And Edit a Rendering Profile* in the *Meridian Enterprise Server Administrator's Guide*.

   See the *Rendering Modules* article in the *Meridian Enterprise Supported Software* document for a list of file extensions and the modules that support them.
3. Create publishing jobs for your rendering profiles.

   To learn how to create a publishing job, see *Create a Publishing Job* in the *Meridian Enterprise Server Administrator's Guide*.

   At least one rendering profile must be specified for each publishing job that will generate renditions.
4. Configure any applicable options for your publishing jobs.

   To learn how to configure these options, see the articles in the *Configure a Publishing Job* section in the *Meridian Enterprise Server Administrator's Guide*.
5. Configure the synchronize content options for your publishing jobs.

   To learn how to configure these options, see *Configure the Synchronize Content Options* in the *Meridian Enterprise Server Administrator's Guide*.

6. If you want to link a publishing job to a specific command in PowerWeb, configure the Publisher Jobs settings in the Administrator.

End-User Procedures

The following end-user procedures are impacted by this configuration:

- *Update Renditions*
- *Synchronize File Properties*
- *Synchronize References*

To read these procedures, see the *Meridian Enterprise User's Guide*.

Synchronize via Application Integration

Meridian includes application links for the most popular applications used for engineering. The links provide specific Meridian functionality within each application for working with that application's data. This functionality is in addition to the functionality provided by Meridian Application Integration described in the *Application Links* section of the *Meridian Enterprise User's Guide*.

Application Integrations are application-independent and configurable by each user so that they can conveniently work with vault documents. Because the links work with application data, the application links can be configured by a System Administrator so that the data is managed in the same way for all Meridian users in the organization.

To learn more about the supported application integrations, see the *Application Integration* section of the *Meridian Enterprise Configuration Guide*.

- **Benefits**: Some file extensions require specialty software for editing. This method supports specialty software.
- **Drawbacks**: Users must have specialty software installed on their workstation. Updates are only made when the user triggers the update from within the application.

Configuration

To configure an application integration, see the relevant section in the *Application Integration* section of the *Meridian Enterprise Configuration Guide*.

End-User Procedures

The following sections in the *Meridian Enterprise User's Guide* are impacted by this configuration:

- *AutoCAD Link*
- *MicroStation Link*
- *Autodesk Inventor Link*
- *SolidWorks Link*
- *Revit Link*
- *Office Link*
- *Lotus Notes Link*

To read these procedures, see the *Meridian Enterprise User's Guide*.

Installation Requirements

To install Meridian successfully, you must be familiar with the different components of the system. To ensure that each component can be successfully installed and will perform at its intended level, specific system requirements apply to every component.

Meridian 2026 requires .NET Core version 8 or higher on machines where you install either the Meridian Server or Meridian client components.

Meridian Servers

There are numerous hardware configurations possible for the Meridian server, depending on how it will be used and the database engine that is used. A server on which Meridian is running should be a dedicated server that is not used for any other purposes, such as a print server or running other applications.

The following components can also be run on the Meridian application server together with the AutoManager EDM Server service or they can be run on one or more separate servers, if required to improve scalability or performance.

- Optional SQL Server or Oracle database management systems.

  See the *Database Management Systems* section of the *Supported Software* document for this release of Meridian.
- Optional Windows Search Service (for full-text searching)
- Optional PowerWeb (Internet Information Services)
- The Accruent License Server service

The optional SQL Server or Oracle database server can be either an existing server or a new installation on the Meridian server (with adequate hardware resources). If a separate Oracle database server will be used, the Oracle client software must be installed on the Meridian application server as described in Install the Server Components.

Servers with multiple processors can manage multiple vaults more efficiently, to reduce overall CPU loading as described in CPU and Configure the CopyDLL Setting.

Meridian Application Server Requirements

These requirements are recommended for the following example environments:

- **Workgroup**: 50,000 documents and 15 users, or for demonstration computers
- **Department**: 100,000 documents and 30 users, or for demonstration computers
- **Enterprise**: 500,000 documents and 150 users. Vaults stored in SQL Server or Oracle should not exceed 2 million documents. Vaults stored in Hypertrieve can accommodate many more documents and several hundreds of users.

The preceding examples are general guidelines *only*. Capacity and performance depend on the specific server configuration and are not guaranteed.

These specifications pertain to Meridian Enterprise only. Meridian can be one system within a larger computing environment that also includes Meridian Explorer, which can serve many times more users than Meridian Enterprise. For information about Meridian Explorer system requirements and deployment, see the *Meridian Enterprise Server System Requirements* chapter of the *Meridian Enterprise Server Administrator's Guide*. For the best possible performance, see Hypercache. This specification is recommended for SQL Server or Oracle installations on the same computer with Meridian.

Hardware Specifications table

Lesser specifications might be insufficient to configure HyperCache. For more information, see Hypercache.

Hardware specifications

Requirement	Workgroup	Department	Enterprise
CPU	Intel® Xeon® E3 or E5	Intel® Xeon® E3, E5, or E7 with 4 to 8 cores	Multiple Intel® Xeon® E5 or E7 CPUs with 8 or more cores
Memory	2 GB or higher depending on the total of all database sizes	16 GB or higher depending on the total of all database sizes	32 GB or higher depending on the total of all database sizes
Storage	1 GB + document storage space on high performance drives. Non-system partition volumes recommended. To calculate the document storage space and to prevent out of disk space errors, see Document Storage Space Requirements.		

Basic Server Requirements and Usage

- Dedicated server that is not used for anything other than Meridian and its database engine, SQL Server or Oracle.

  We recommend only the Enterprise hardware specifications when Oracle or SQL Server are used on the same computer or with multiple active vaults.
- One of the Windows Server operating systems (with latest Service Pack) listed in the *Operating Systems* section of the *Supported Software* document for this release of Meridian.

  The operating system should be installed with the roles and services described in Server Role Requirements.
- Microsoft .NET Framework 4.7.1 Full Profile (the Client Profile is insufficient)
- Any additional requirements for specific operating systems or Meridian releases that are documented in the *2026 Release Notes*.

Database Management Systems

- If the vaults will not be hosted on the Meridian application server with the Hypertrieve database engine, a connection to one of the database management systems listed in the *Database Management Systems* section of the *Supported Software* document for this release of Meridian.
  - If any vaults will use a Meridian Enterprise **MS SQL Server 5** (or later) database engine to connect to either a local or remote SQL Server instance, the Microsoft OLE DB Driver for SQL Server (MSOLEDBSQL) must be installed on the Meridian server.
  - If any vaults will use the Meridian Enterprise **Oracle 5** database engine (not **Oracle 3**) to connect to either a local or remote Oracle instance:
    - The 64-bit Oracle Data Access Components (ODAC) and Oracle Data Provider for .NET (ODP.NET) version 11.2 or higher must be installed on the Meridian server.

      For more information about database engine selection during vault creation, see Create a New Vault.
    - A default installation of Oracle is limited to 150 processes.

      If the database server has more than one CPU, that limit may be reached and cause vault errors, especially during large imports. We recommend that you configure Oracle to allow up to 500 processes.
- The vault audit trail feature of the Meridian FDA Module and the subscriptions feature of Meridian Enterprise require a connection to one of the database management systems listed in the *Database Management Systems* section of the *Supported Software* document

for this release of Meridian.

- Microsoft Access installed in advance.

  Microsoft Access is the default storage for external lookup tables. We install SQLite as the default for storing local workspace data. Microsoft Access is not used for vault data and is not installed by the Meridian setup programs. You can use Enterprise Server or Microsoft Access for your user database.

  The lookup tables (but not the user account database or local workspace databases) can also be stored in a server edition of SQL Server. The supported versions of SQL Server are listed in the *Database Management Systems* section of the *Supported Software* document for this release of Meridian. Storage in a server edition has the following limitations:

  - Lookup table entries will not be included in the vault configuration export (`.met`) file. Therefore, they cannot be imported for use in another vault unless that vault is also connected to the same database server.
  - Lookup tables will not be included in the vault backup snapshots and must be backed up separately.
  - Retrieving lookup table entries and using them in custom property pages requires VBScript programming. The database connection strings will be encoded in the scripting, which may pose a security risk for your organization and will require updating if the database server name is changed.

  The data contained in lookup tables created in the Configurator can be stored in Microsoft Access tables instead if the following requirements are met:

  - An OLE DB driver is installed. Microsoft Office includes a 64-bit OLEDB driver named the Office System Driver that can be used to connect to Access, Excel, and text files. The provider name is Microsoft.ACE.OLEDB.*<VersionNumber>*.

    If Office is not installed, the driver is available as a separate download from the Microsoft Download Center by the name of Microsoft Access Database Engine Redistributable.

    For additional information, see Jet for Access, Excel and Txt on 64-bit systems at ConnectionStrings.com.
  - The **ConnectionString** registry setting is configured as described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server\UserDatabase
  - The **TablesDb** registry setting is configured as described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server
  - The **WorkspaceDB** registry setting is configured as described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client

To learn more about lookup tables, see the *Create And Edit Tables* article in the *Meridian Enterprise Configuration Guide*.

> **Note:**
> Depending on how much additional data is stored in Microsoft Access (for example: document subscriptions, audit log), the database can grow to where performance is degraded considerably. For that reason, we do not recommend using Microsoft Access for more than external lookup tables, the user account database, and local workspace data. Store all additional data in SQL Server instead.

Browsers and the Internet

- One of the Internet Information Services versions listed in the *Web Servers and Browsers* section of the *Supported Software* document for this release of Meridian. The minimum IIS components that must be installed for proper operation are described in Server Role Requirements.
  - If the **Request Filtering** feature option **Allow unlisted file name extensions** is disabled in IIS Manager, the following file extensions must be added to the **File Name Extensions** list and allowed: `.dll,.gif,.png,.js,.css`.
  - If Meridian Mobile will be deployed, additional requirements must be met as described in Install the Meridian API Service.
  - Transport Layer Security (TLS) 1.2 is supported by Meridian 2018 R2 Update 1 and higher.
- One of the web browsers listed in the *Web Servers and Browsers* section of the *Supported Software*document for this release of Meridian (some components are used by Meridian).

Server Role Requirements

Windows Server 2003 and higher allow you to select the operating system components that are installed on the server to match the functions that you expect the server to perform. This reduces system administration and the amount of disk space used. Certain components of Meridian Enterprise require that some operating system components be installed in order to function correctly.

The following table lists the minimum server roles and role services that are required for particular Meridian Enterprise components. These roles and services must be installed on the computer that will host the Meridian components, whether on the same server with other roles and services or on a different server. Additional roles and services may be installed but are not required. Not all of these roles and services are available in all versions of Windows Server. If a listed role or service is unavailable, it is not required by Meridian Enterprise.

Server role requirements

Meridian Component	Server Components
EDM Server service	Features: • Windows Process Activation Service • HTTP Activation • Windows Search Service (required for full-text search)
Web server	Web Server (IIS) role services: • Static Content • Static Content Compression • IIS Management Console • ISAPI Extensions • ISAPI Filters • Basic Authentication or Windows Authentication per your organization's security requirements • URL Rewrite module

Meridian Component	Server Components
Data Library web server	Web Server (IIS) role services: • Static Content • ASP.NET 4.6 • IIS Management Console • Basic Authentication or Windows Authentication per your organization's security requirements

Document Storage Space Requirements

When estimating the disk space needed for a Meridian application server or file server, there are many variables involved:

- The number of vaults that will reside on the server
- The number of documents that will reside in each vault
- The size of the documents that will be stored in each vault (2 GB maximum each)
- The number of revisions of each document
- The type of database engine used (Hypertrieve, SQL Server, or Oracle)
- The number of properties that will be used in each vault
- The amount of data stored in each property

With all of these variables, an accurate disk space calculation is nearly impossible. But you can make a rough estimate with these formulas:

- Stream storage space for each vault is the sum of all of the following:
  - Number of documents X average document size (current revisions)
  - Number of revisions per document X average document size (prior revisions)
  - Number of documents X average document size X 2 (renditions & viewer intermediate files)
  - 30% for future growth
- Database storage space = 0.6 to 1.0 GB per 100,000 documents. Triple the storage space if Hypertrieve is used, to allow for backup snapshot files. Double the storage space if SQL Server or Oracle is used (allow additional space for database replicas, if required).

These are rough estimates only, but should give you a good start on estimating server disk space requirements.

We strongly recommend that vaults be located on a different drive on the same server from the Meridian program files. The streams can be stored on any local or network storage device accessible by Windows via a UNC address and the account under which the EDM Server service is run. Vaults cannot be located on mapped drives, which require an interactive logon session. However, local disk storage typically provides the best performance and reliability. Database files should be located on the fastest possible drives. For information about using different disk subsystem types, see Disk Subsystems.

Note:
Windows normally uses extended memory to cache data before writing it to virtual memory on disk. However, Windows does not do this if a Hypertrieve database is stored on a network device accessed by a UNC location. In that case, Windows assumes that the data could be modified by other users since it does not reside on the local computer.

Serious errors can occur and services may stop working if a server runs out of free disk space. For this reason, we recommend that you:

- Maintain a minimum amount of free disk space on the Meridian application server that is equal to three times the combined sizes of all vault databases (`.HDB` files in the `BC-Meridian Vaults` folder described in Meridian Folder Structure).
- Schedule a task to periodically clean the Windows temporary file folders:
  - `C:\Users\<ServiceAccount>\AppData\Local\Temp`
  - `C:\Windows\Temp`
- If rendering is performed by a Meridian Enterprise Server node, schedule periodic cleaning of the computer's local workspace as described in the *Clean the local workspace* article in the *Meridian Enterprise Server Administrator's Guide*.
- Consider deploying a program on the Meridian application server to monitor and generate System Administrator alerts when the free disk space falls below 15%.

Server Time Requirements

Meridian safely manages changes made to documents by multiple users, even those located in different time zones by storing dates and times in an absolute, locale-independent format. However, minor differences in system time between computers can have unexpected and critical implications. Therefore, it is very important that all computers running Meridian software keep correct time. Ensure that the computers' time is set correctly before installing Meridian, for example, by synchronizing the time on all servers and client computers with an atomic clock or a trusted Network Time Protocol (NTP) server.

Time settings are particularly important because date-based properties are an integral part of every vault's configuration. For maximum compatibility with related VBScript customization and application data exchange, it is important that all users use the same date format, for example, dd/mm/yyyy or mm/dd/yyyy, but not some using one and some another. If your organization must use different date or time formats, be sure that all aspects of the system are compatible with all formats that are used.

To synchronize the time of a client computer with that of the server running Meridian, you can use the **NET TIME** command. The syntax is:

```
NET TIME \\<ServerName> /SET
```

> **Important!**
> When Meridian is running, do not change the time of the server.

The AutoManager EDM Server service saves the last moment (date and time) it was used. You cannot open a vault at any moment that is earlier than this, or you risk data corruption. If you set back the server clock, you cannot open the vault again until the server clock reaches the last moment it was used. You will have to wait until that time. To protect against this situation, the server requires that you confirm any change to the server clock that is seven days or more.

> **Note:**
> Meridian will display a warning if the AutoManager EDM Server service has not been active for more than seven days. To enable the service again, use the **Acknowledge Current Server Time** command on the Meridian Enterprise Administrator toolbar.

The number of days used by this feature can be configured by creating the following **DWORD** key in the server's registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager Meridian\
CurrentVersion\Server\DaysSinceLastOpen
```

Set it to the number of days (decimal) you would like as the limit.

Network Requirements

Because Meridian data is stored on a server, Meridian relies heavily on network performance. Therefore, the local area network bandwidth between all Meridian client and server computers must be 100 Mbps or higher to ensure adequate performance. The bandwidth between Meridian servers (application servers, database servers, web servers, and other servers used by Meridian) should be 1 Gbps or higher (preferably optical links and very reliable). There should be no switches, routers, hubs, or network cards slower than 100 Mbps at any point between Meridian computers. Just as important as speed is the latency (delay) of the network, which should be under 5 milliseconds between all LAN client computers and the Meridian application server. A latency of less than 300 ms is required when using application links in Remote mode over wide area networks. If the latency is higher, we recommend using Offline mode instead.

Real-time bandwidth, latency, and Meridian application server responsiveness can be measured with the Diagnostics command in PowerUser.

If you use more than one Windows server or more than a few Windows workstations, we recommend implementing a Windows domain structure. We highly recommend installing Meridian only on a member server, not a domain controller. You might also need to configure security delegation as described in Security Delegation.

Meridian relies heavily on the DCOM protocol. By default, DCOM communicates over a very wide port range (1024 to 65535). The Meridian desktop clients always start a DCOM session with a request on the TCP port 135 of the Meridian application server. If a response is received, DCOM handles further communications and determines which port will be used. It's essential to ensure that DCOM is running with TCP/IP only. If possible, delete all other protocols except TCP/IP if you are not using them. If you only have a restricted number of ports to use, refer to the Microsoft MSDN site for the current recommendation for the minimum number of ports to allocate. Additional information about Windows port requirements can be found at Service overview and network port requirements for Windows.

The following table lists the default TCP port numbers that Meridian relies upon. Some of the ports are configurable as described elsewhere in this guide. Other ports may be used by some third-party applications.

TCP port numbers

Port	Description	Remarks
25	SMTP email notifications	Used by EDM Server and Enterprise Server to send notification emails.
80	HTTP (PowerWeb)	Used by the PowerWeb and Explorer clients for HTTP connections.

Port	Description	Remarks
135	DCOM port negotiation	Used by PowerUser, WebAccess, and Enterprise Server to connect to EDM Server and License Server.
443	HTTPS (PowerWeb)	Used by the PowerWeb and Explorer clients for HTTPS connections.
445	Server Message Block (SMB)	Used by EDM Server and Enterprise Server to exchange files.
587	SMTP SSL email notifications	Used by EDM Server and Enterprise Server to send notification emails.
1024 to 65535	DCOM communication	Used by PowerUser, WebAccess, and Enterprise Server to connect to EDM Server and License Server.
8080	Meridian Enterprise	Used by EDM Server to connect to Enterprise Server.
8450	BlueCielo Connector SSL	Used by PowerUser.
8686	Meridian Enterprise	Used by EDM Server to connect to Enterprise Server.
8900	BlueCielo Connector	Used by PowerUser.

System Requirements For Meridian Clients

For successful installation and acceptable performance on a client computer, the Meridian client applications require the following minimum specifications.

Hardware Requirements

The hardware requirements for Meridian clients are listed in the table below.

Hardware specifications

Requirement	Minimum
CPU	Intel® Pentium® 4 3 GHz with SSE2
Memory	2 GB (4 GB recommended and for 64-bit) or higher depending on the other applications used with Meridian
Storage	Up to 750 MB depending on the options chosen.
Display	1024 x 768 resolution with true color

Software Requirements

The software requirements include:

- One of the Windows desktop operating systems (with latest Service Pack) listed in the *Operating Systems* section of the *Supported Software* document for this release of Meridian.

  We recommend the 64-bit editions of Windows and Meridian.
- Microsoft Access for Local Workspace data management.

  It can also be managed by SQLite (included) by setting the **WorksSpaceDB** registry value described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client.
- Microsoft .NET Framework 4.7.1 Full Profile (the Client Profile is insufficient)
- Some of the optional Meridian modules require the .NET Framework and other software to be installed.

  See the system requirements in the module's *Administrator's Guide*.
- TCP/IP protocol and DCOM access to the Meridian Enterprise server.

- Sufficient access rights for installation of Meridian (that is, a member of the **Administrators** group of the computer).
- Any additional requirements for specific operating systems or Meridian releases that are documented in the Release Notes.

Client computer specifications should be determined by the most demanding application that is installed on them. This is particularly true for heavy duty 3D CAD applications such as Autodesk AutoCAD, Autodesk Inventor, or SolidWorks. In such cases, you should always use a computer that meets at least the software manufacturer's recommended specification, not the minimum.

Internet / Intranet Requirements

To use PowerWeb over the Internet or an intranet requires:

- A web browser capable of rendering HTML 5 markup and of running JavaScript components.

  The supported web browsers and additional requirements specific to each browser are listed in the *Web Servers and Browsers* article in the *Supported Software* document for this release of Meridian.
- For integration with authoring applications installed on the client PC and to manage downloaded documents in the local workspace, the Application Integration component must be installed on the client PC. Application Integration communicates with web servers independent of the web browser and must be set to **Remote** mode as described in the *Application Links In Remote Mode* article in the *Meridian Enterprise User's Guide*. The local workspace location must be set to the same path in both PowerWeb and in Application Integration options as described in the *Application Integration Options* article in *Meridian Enterprise User's Guide*.

Additional Notes

- To use site cache on client computers without MS SQL CE Compact 3.5 or 4.0, create the **WorkSpaceDB** registry key with a value of 1 and add the Meridian URL to the trusted sites in Internet Options > Security > Trusted Sites. If you don't create the registry key, you might receive the **LocalDB updade failed** error.
- By default, PowerWeb versions prior to 2017 use ActiveX controls that must be installed on the client PCs to transfer documents and perform batch operations. Newer versions of Meridian use built-in, server-side component by default. The ActiveX controls can be enabled in the newer versions for backward compatibility by enabling the **Enable PowerWeb client components** option in the user's preferences.

In particular, the **UseHTMLProgressComponent** should be set to **0** and the **DownloadDocumentWithRefs** option set to **1** in each user's PowerWeb profile file for compatibility with Windows 7 when Windows authentication is enabled for the Meridian website. Importing documents by drag-and-drop does not work correctly with **UseHTMLProgressComponent** set to **0**.

Editing the PowerWeb user profile files (preferences) is described in general for other settings in *Deploy Standard Preferences* and *Edit PowerWeb User Profiles* in the *Meridian Enterprise Configuration Guide*. Also, the following options must be configured on the **Security** tab of **Internet Options** in **Control Panel** for each user:

For either the **Internet** or **Local intranet** zone (as applicable for your environment), set all options under **ActiveX controls and plug-ins** to either **Enable** (recommended) or **Prompt** (and ensure the user always clicks **Yes** when prompted to use a control related to Meridian).

- On Windows 64-bit operating systems, Internet Explorer 10 and 11 open web pages in 32-bit processes only. This is for backward compatibility with ActiveX components. Therefore, Meridian Enterprise installs and runs 32-bit components when necessary, particularly for viewing documents.

System Requirements For Optional Modules

The hardware and software specifications listed elsewhere in this document support the basic engineering content management functionality provided by Meridian Enterprise, the centerpiece of the Meridian Enterprise product suite. The entire suite includes optional modules that integrate with Meridian Enterprise to extend its functionality to other enterprise departments and information systems. Some of the optional modules impose additional requirements that should also be considered. A brief overview of the modules and their requirements are listed below.

Optional module resource requirements

Module	Function	Resource Requirements
Asset Management Module	Integrates Meridian with computerized maintenance management systems (CMMS).	Additional vault database storage space, high-speed ODBC connectivity to the CMMS server, web server, synchronization processing time, additional client component installation may be necessary.
FDA Module	U.S. Food and Drug Administration 21 CFR Part 11 compliant functionality.	Meridian server configured to Meridian Application Server Requirements specifications, additional vault database storage space, rendering storage space, SMTP server, audit log database server, rendering server, database client installed on Meridian server and clients (Oracle only).
Meridian Explorer	Easy to use, web browser-based, read-only views of Meridian vaults for information consumers on a large scale.	Repository database server, web server, additional Windows components.
Publisher	Automated rendering of vault documents to alternative formats and publishing to other vaults or information systems.	Rendering storage space, rendering server, additional Windows components.

Several of the modules listed above perform tasks under the control of the Windows Scheduler. If the tasks take too long to complete when run on the Meridian server, or if they need to be executed on a more frequent basis, an additional application server may be necessary.

Language Requirements

Meridian Enterprise and Meridian Enterprise Server have language limitations when installed in the same organization for access by users in multiple locales. The limitations are summarized as follows to help you decide which languages to install and configure for each product.

- Meridian Enterprise, PowerWeb, and Meridian Explorer server components may only be installed in one language. Server-based messages that appear in the client applications such as status, progress. and error messages are shown in the server language. Configuration data and vault or repository data is stored in one language.
- Meridian Enterprise Configurator and Meridian Enterprise Server Administration Console may only be installed in one language.
- Meridian Explorer client language is selected by the user.
- PowerWeb language is determined by the web server.

Installation

A Meridian installation can be as simple as a minimally configured, stand-alone installation for testing or demonstration purposes or as complex as a fully configured, complex global network of many vaults, optional modules, and integration with other information systems. Meridian may be distributed as either a full installation, or an update to an existing installation, depending on each particular release.

In all instances you should first completely read the release notes that are included with each release, as they contain particular information about, and instructions for, the new release. Before you begin installation, you should consider the different installation configurations and the preparation that is required.

- **Stand-alone configuration**: A stand-alone configuration will act as server and client at the same time, for example, on a single computer for evaluation purposes. All functionality is available in this configuration.
- **Client/server configuration**: At least two computers are needed for a client/server configuration. One will act as server and all other computers will be clients. Various options in this configuration are described in Deployment Models.

There is only one way to obtain the release files, from the Accruent website. The download location and archive file password are communicated to Accruent Partners by email.

The setup programs detect previously installed versions and install the appropriate upgrade.

> **Important!**
> We do not define your content security policy. It is up to you, the customer, to configure your security settings and add a corresponding HTTP header. For more information, see the following resources:
>
> - OWASP - Content Security Policy
> - Mozilla - Content Security Policy
> - Google - CSP Evaluator Tool

Deployment Strategies

The architecture of Meridian Enterprise is flexible so that it can be deployed in various configurations to meet a wide range of organization sizes and requirements from small workgroups to large enterprises. Each configuration has inherent advantages and disadvantages in terms of:

- **Load**: from a small departmental productivity tool to a mission-critical enterprise system with many users and documents.
- **Reliability**: whether all components are hosted on a single server or some components are hosted by dedicated, fail-safe systems.
- **Systems management**: distributing components to other servers distributes administrative responsibilities correspondingly.
- **Geography**: whether data resides in a single vault or many vaults distributed globally.
- **Functionality**: from out-of-the-box basic tools to custom data structures and unique functionality.

Single-Server Strategy

The single-server strategy is best suited to smaller Meridian configurations for use in workgroups or small departments. This strategy is based on deploying all Meridian components on a single server, which has the following notable advantages and disadvantages.

Single-server strategy overview

Advantage	Disadvantage
Lower hardware cost	
Less complicated configuration	
Single point of administration	Not well suited to centralized IT management
Performs well with modest loads	Maximum performance is limited by hardware

Under this strategy, Meridian is installed on a single server that can be upgraded with additional processors and memory to serve the growing needs of more users and documents. An organization may deploy their initial configuration based on this strategy and then transition to a multi-server strategy later.

In particular, a single processor server can be upgraded with an additional processor in those cases where the Meridian application uses a third-party DBMS hosted on the same server. Then, each application can use its own processor assigned by Windows.

More important is the available free memory of the server. Meridian can take advantage of all of the physical memory installed on a server that is accessible by the Windows operating system. For more information on memory configuration options, refer to Optimize the Server Operating System. Vault documents and metadata are both stored directly on the server in this strategy.

When a Meridian application server has been scaled up under this strategy as much as possible, if the organization's needs continue to grow, the replacement strategy is to scale the configuration up to multiple servers as described in the following section.

Multiple-Server Strategy

To accommodate the users, workloads, and document quantities of large departments and the enterprise, the best results can be obtained by scaling Meridian up to additional servers for more processing and storage capacity, which has the following notable advantages and disadvantages.

Multiple-server strategy overview

Advantage	Disadvantage
	Higher hardware cost
	More complicated configuration
Better suited to centralized IT management	Multiple points of administration require coordination
Required to obtain maximum performance for heavy loads	More complicated security administration

Each of the major components of a Meridian-based system can be hosted on its own server, thereby making the maximum processor power and physical memory available to the primary process, the EDM Server service. For example, the Meridian database server, web server, and document content can each be deployed on separate server computers with their own inherent benefits.

Under this strategy, vault data can be distributed between metadata residing on a database server and documents stored on the Meridian application server, on a file server, or even stored on network attached storage (NAS) or storage area network (SAN) devices.

For configuration recommendations for specific system sizes under this strategy, refer to Deployment Models.

Deploy For High Availability

Meridian Enterprise can be deployed in virtualized, high availability infrastructures like VMware or Microsoft Hyper-V in a Windows Server failover cluster or similar environment. By doing so, the underlying IT architecture provides high availability for Meridian Enterprise. Other scenarios for partial high availability or switchover are also possible.

For example, using VMware vSphere Replication, a production Meridian Enterprise server running on a virtual machine can be replicated to one or more copies in real time. If the production server fails, services can be switched over to a shadow server with minimal effort and time loss.

Meridian Explorer runs on Microsoft and Oracle systems for storing, managing, and serving documents and their metadata. It can thereby claim high availability when the Microsoft SQL Server or Oracle database is run in a high availability cluster.

If a virtualized environment is not an option, certain components of Meridian Enterprise can achieve high availability with the aid of other infrastructure or 3rd party tools.

- **Database**: The Microsoft SQL Server or Oracle database can be deployed on a high availability cluster
- **Rendering**: Multiple Meridian Enterprise Server computers can be configured as a cluster to improve rendering performance
- **Data storage**: The documents stored in Meridian Enterprise can be hosted on a RAID 6 disk subsystem to provide a high level of protection against hard disk failures

Deployment Models

The following topics describe deployment models for Meridian Enterprise to provide adequate performance and stability for several typical organization sizes. These models and the corresponding system requirements contained in this document pertain to Meridian Enterprise only. Meridian can be one system within a larger computing environment that also includes Meridian Explorer, which can serve many times more users than Meridian Enterprise. For information about Meridian Explorer system requirements and deployment, see *System Requirements For Optional Modules* in the *Meridian Enterprise System Requirements* document.

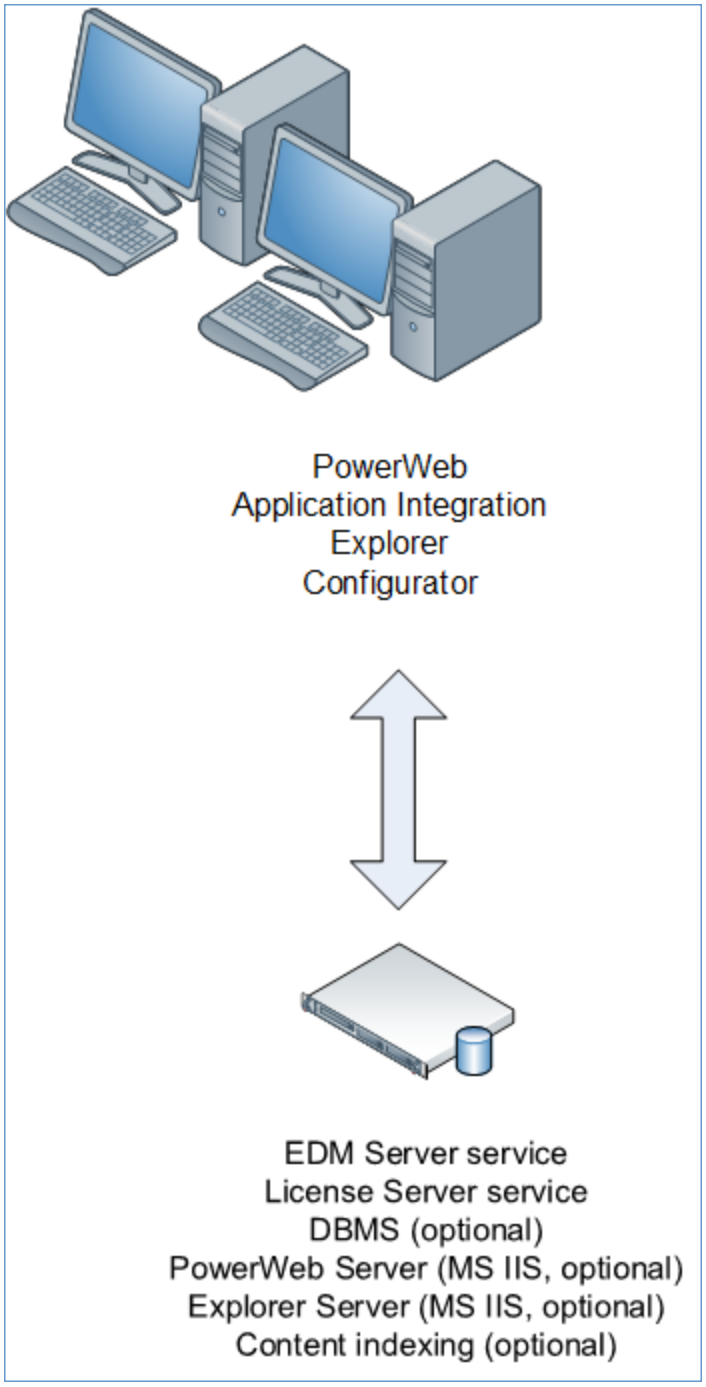
The configurations that follow are general in nature and intended as a starting point for your own performance and stability tuning. The actual performance that can be expected for any particular number of concurrent users and documents is dependent on many factors. These configurations do not guarantee a particular level of performance or stability, and additional optimization may be necessary as described in Optimizing performance. Consultation is available from Accruent Services or one of our Partners.

Workgroup Model

In the workgroup model, Meridian is configured to meet the following needs:

- Less than 50 Meridian vault users, excluding Meridian Explorer repository users, which can be many more.
- One site.
- Modules such as the Meridian Asset Management Module or Publisher are not used.
- Minor or no customization is implemented.

A typical configuration to meet the needs of a workgroup would look similar to the following figure.



Since all components are installed on a single server, that server should be dedicated to Meridian and host no other significant applications or services. The DBMS in this configuration can be either the Hypertrieve database engine (preferred), or SQL Server or Oracle if standards conformance is required and a separate database server is not available (see Department Model). However, if all components are installed on a single server, special attention must be specified to memory management, as described in Physical Memory.

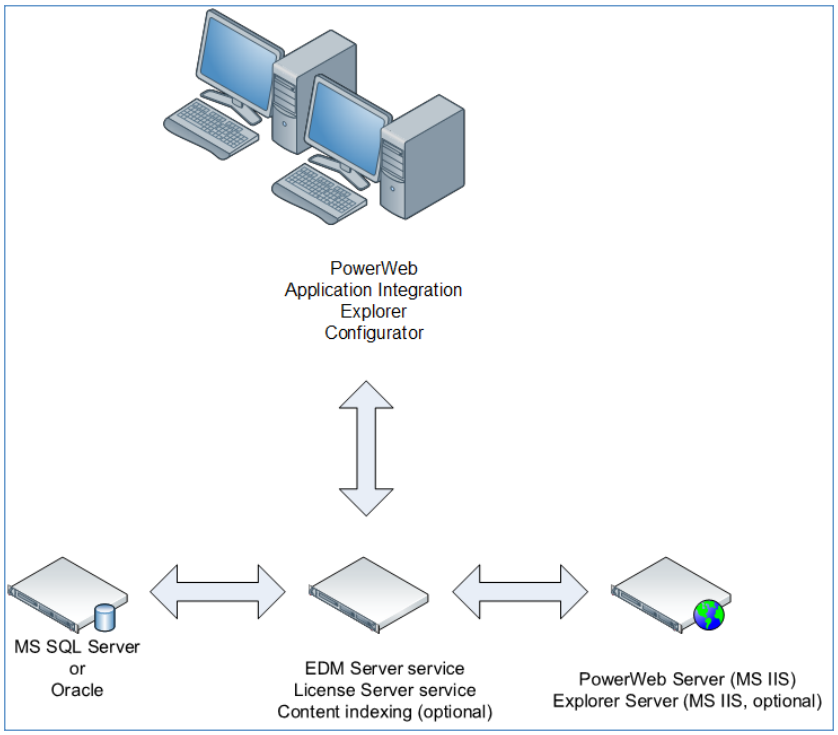
The maximum cache size of each vault should be 1 GB or less. The combined sizes of all vault database caches plus user session memory must not exceed the amount of application virtual memory provided by the operating system.

Department Model

The department model represents an organization with the following needs:

- Between 50 and 75 Meridian vault users, excluding Meridian Explorer repository users, which can be many more.
- One site.
- Modules such as the Meridian Asset Management Module and Publisher may be required.
- Minor to moderate customization is implemented.
- Oracle or SQL Server is the organization's standard DBMS.
- An existing suitable web server is available

A typical configuration to meet the needs of a department would look similar to the following figure.



In this configuration, Meridian uses existing DBMS and web servers, and all remaining components are installed on a single dedicated application server.

Configuration of the Meridian application server should include the following items.

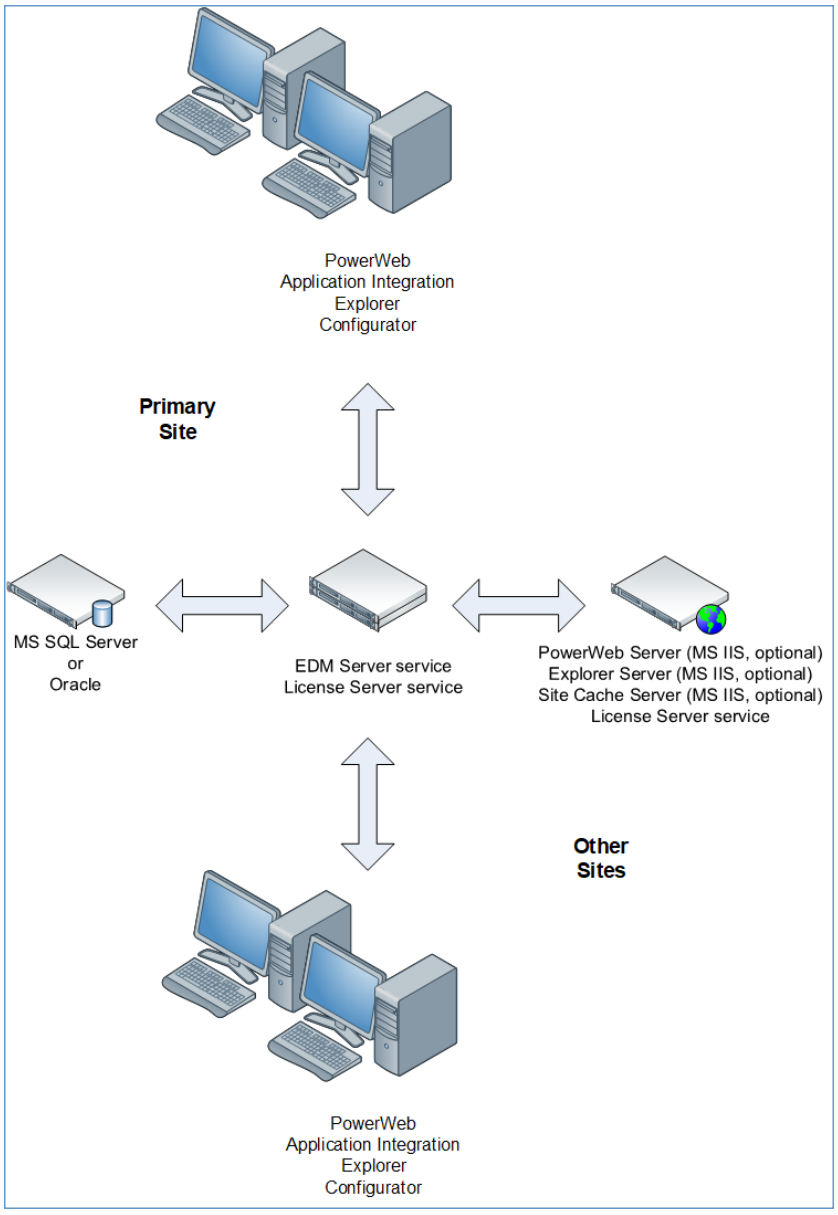
- The maximum cache size of each vault should be 1 GB or less. The combined sizes of all vault database caches plus user session memory must not exceed the amount of application virtual memory provided by the operating system.
- A separate database server should be used only if there is a minimum 1 Gbps (fiber optic preferred) and very reliable connection to the Meridian application server. Otherwise, the application and database should be hosted on the same computer and 64-bit editions of Windows and Meridian installed.

Enterprise Model

The enterprise model represents an organization with the following needs:

- Over 75 Meridian vault users, excluding Meridian Explorer repository users, which can be many more.
- One or more sites.
- Modules such as the Meridian Asset Management Module and Publishermay be required.
- Moderate to heavy customization is implemented.
- Oracle or SQL Server is the organization's standard DBMS.
- An existing suitable web server is available.

A typical configuration to meet the needs of an enterprise would look similar to the following figure.



In this configuration, Meridian uses existing DBMS and web servers, and all remaining components are installed on one or more dedicated application servers at each of the organization's sites. Each site hosts its own vaults from which users may work only on documents relative to that site.

Configuration of the Meridian application servers should include the following items.

- The maximum cache size of each vault should be 1 GB or less. The combined sizes of all vault database caches plus user session memory must not exceed the amount of application virtual memory provided by the operating system.

- A separate database server should be used only if there is a minimum 1 Gbps (fiber optic preferred) and very reliable connection to the Meridian application server. Otherwise, the application and database should be hosted on the same computer.
- If more than 75 concurrent users per server, a dedicated server.

Server Installation Checklist

Installing Meridian Enterprise on a server computer is a complex procedure that involves the installation and configuration of many different components and configuring the security of those components so that they can communicate with one another.

The following table is a checklist for confirming that the critical related tasks of installing a Meridian Enterprise application server have been performed. The table indicates those tasks that should be performed when:

- Installing a Meridian Enterprise server for the first time
- Migrating Meridian Enterprise from an existing server to a new server
- Upgrading Meridian Enterprise on an existing server

The tasks are listed in the order in which they should be performed. Use the hyperlinks in the checklist to find the installation information for each task. Track your installation progress by printing this checklist and placing a check mark in the box in the applicable column as you finish each task.

This checklist is not necessarily complete for every deployment scenario. Additional tasks may be required depending on your requirements and system configuration.

Server installation checklist

Done?	First	Migration	Upgrade	Task	Topic References
	Required	Required	Required	Confirm all system requirements have been met	Meridian Servers
	Required	Required	Required	Prepare for installation	Prepare For Installation
	Required	Required	Required	Create an account with Administrator rights on the server computer to perform the installation (if necessary)	See the Windows product documentation.

Done?	First	Migration	Upgrade	Task	Topic References
	Required	Required		If multiple domains or multiple servers will be used, create a domain account to run the Meridian services (EDM Server, Task Server, License Server)	Grant Domain Privileges With a Service Account
	Required	Required		Create an account to use as a rescue account	Create a Rescue Account For Security Administration
		Required	Required	Disable DCOM remote connections to the server to prevent users from opening existing vaults until the installation is complete	Enable DCOM
	Required	Required		If vaults will be stored in Oracle, install the Oracle client software on the Meridian server	See the Oracle product documentation.
	Required	Required		If vaults will be stored in Oracle, create the Meridian service account with the required privileges	EDM Server Service Account Requirements For Oracle Configure the Oracle Account Used By Meridian
	Required	Required		If vaults will be stored in SQL Server, create the required vault database folders (if absent)	Integrate With a Separate SQL Server Computer

Done?	First	Migration	Upgrade	Task	Topic References
	Required	Required		If vaults will be stored in SQL Server, create the Meridian service account with the required privileges	Configure the Windows Account Used By Meridian Create a SQL Server Account For Use By Meridian Configure the SQL Server Account Used By Meridian
	Required	Required		Confirm that all vault users have adequate privileges on the server	Meridian Server Privileges
	Required	Required	Required	Install any other software on the server that is required for content indexing (IFilters), default 64-bit external table support (Microsoft Access), optional Meridian modules, and so on.	See corresponding chapters in this document and appropriate chapters in the module's Administrator's Guide.
	Required	Required	Required	Install Meridian server components (latest service pack, if applicable) and necessary updates	Download Installation Files Install the Server Components Upgrade Meridian

Done?	First	Migration	Upgrade	Task	Topic References
	Required	Required		If multiple domains or multiple servers will be used, configure the Meridian services (EDM Server, Task Server, License Server) to use the domain account created above	Grant Domain Privileges With a Service Account
	Required	Required	Required	Obtain and register license keys for all products that will be installed	Register Licenses - Administrator
	Required	Required		Create local Active Directory and/or Meridian Enterprise user groups	Meridian User Administration
		Required		Restore existing vaults on the new server from backups made on the old server	Restore Backups
		Required		Copy the existing BC-Meridian Extensions share to the new server, if necessary	Move the BC-Meridian Extensions Folder
		Required		Copy any customized registry keys from the old server to the new server	HKEY_LOCAL_MACHINE

Done?	First	Migration	Upgrade	Task	Topic References
		Required		If the operating system on the new server is different from the old server, run the `icosnlsver.exe` vault upgrade tool described in the Meridian Enterprise knowledge base, if required.	Change Operating System Versions
		Required	Required	Upgrade vaults with Meridian Enterprise Administrator	Upgrade Meridian Vaults
		Required		Correct the security roles assigned in the vaults to refer to the new server name. This can be done by either deleting all role assignments and recreating them or with the ACL Rename tool described in the Meridian Enterprise knowledge base.	
	Required	Required	Required	Configure the server to automatically deploy client upgrades (Optional)	Install the Client Components Silently
	Required	Required		Configure PowerWeb (Optional)	Create a PowerWeb Location Configure a PowerWeb Location

Done?	First	Migration	Upgrade	Task	Topic References
	Required	Required		Create scheduled tasks for vault backups and recovery logs	Prepare For Backups Create a Recovery Log
	Required	Required		Configure content indexing (Optional)	Content Indexing
	Required	Required		Configure reserved licenses (Optional)	Reserve Licenses Reserve Licenses For Remote Access
	Required	Required	Required	Create the subscriptions and audit log databases (FDA Module only). (Optional)	See corresponding chapters in this document and appropriate chapters in the module's Administrator's Guide.
		Required	Required	Remove unused data in vaults (Optional)	
		Required	Required	Run Vault Consistency Toolkit tools	Vault Consistency Toolkit
		Required	Required	Configure any planned vault modifications (Optional)	
	Required			Create Accruent users and groups and configure vault security.	Meridian User Administration
		Required	Required	Enable DCOM remote connections to the server to allow users to open the upgraded vaults	Enable DCOM

Done?	First	Migration	Upgrade	Task	Topic References
	Required	Required	Required	Perform user acceptance testing	

Prepare For Installation

Before you start installing any components, complete the following tasks:

1. Review the *Supported Software* for this version of Meridian to determine if the configuration that you are about to create is fully supported.

   It is available from your Accruent Partner or the Accruent Technical Library.

2. If you are installing the server components, create a verified back up of all existing vaults as described in Prepare For Backups.
3. Network connections between all involved computers must be working and active.
4. DCOM communications must be possible between all involved computers.

   For information on enabling DCOM, see Enable DCOM.

5. If you are installing PowerWeb, know the computer name of the server on which IIS and Meridian PowerWeb is installed.

   During the client installation process, you will be prompted to type the Meridian web server location in this form:

   `http://<ServerName>/Meridian/Start`

6. If you are installing only Meridian client software, know the name of the Meridian application server, as you will be prompted for it during installation.
7. If you are installing PowerWeb on a separate IIS server, you must have already installed the AutoManager EDM Server service on another computer and you must know its name.

   During PowerWeb installation, you will be prompted for this name.

8. Any web server that will be used for PowerWeb must be running before PowerWeb installation.

   If you do not want to enable PowerWeb during the initial setup of Meridian, you can install it later.

9. You must have Administrator rights on the computer before you begin installation.
10. All client computers should be time-synchronized with the Meridian application server.
11. Always disable any real-time virus scanning software before attempting to install Meridian.

    Some virus scanners have been found to interrupt the creation of Meridian registry items. You can re-enable them after installing Meridian, although we do not recommend it. For more information on the effects of antivirus software on Meridian, see Optimize Antivirus Applications.

12. The accounts under which Meridian services will run may need additional permissions as described in Active Directory Security Problems.

Install the Server Components

To install the Meridian Enterprise server components, start the appropriate installation package described in Download Installation Files. To install the components in silent mode, see Install the Server Components Silently. After you have installed and correctly licensed the Meridian application server, you can then install Meridian on client computers or additional servers. For information on the Windows Installer Package, see Control Windows Installer Packages.

Change License Server Type

If you already have Meridian installed, and you want to change your license server type:

1. Navigate to **Control Panel** > **Programs and Features**.
2. Select **Meridian Enterprise**.
3. Click **Change** > **Modify**.

   The installation wizard opens.
4. Deselect the license server role.
5. Wait until the license server file is uninstalled.
6. Navigate to **Control Panel** > **Programs and Features**.
7. Select **Meridian Enterprise**.
8. Click **Change** > **Modify**.

   The installation wizard opens.
9. Select the license server role.
10. Click **Next**.
11. Select the license server type you want.

Requirements for Oracle and SQL Server

- The Oracle client components must be installed on the Meridian application server and the server rebooted before installing Meridian in order for the **Oracle Driver** to appear as an option when creating new vaults in the Meridian Enterprise Administrator. A **Minimal** installation of Oracle on the Oracle server is sufficient to create and maintain Meridian vaults.

On the computer running the EDM Server service, an **Oracle Instant Client Basic** installation is required. Meridian and the **Oracle Instant Client Basic** components can be installed in any order. After a correct installation on the computer running the EDM Server, the Oracle Listener should be able to connect with the Oracle database. You can verify that by using the command **tnsping <*OracleInstanceName*>** at the command prompt.

- The Oracle database driver is only a driver; it does not install the Oracle database management system software. You must have an existing Oracle installation and licenses on this or another server, and have the **Oracle Instant Client Basic** installed and functional on the Meridian application server.
- The SQL Server database driver is only a driver; it does not install the SQL Server database management system software. You must have an existing SQL Server installation and licenses on this or a separate server.

  If a separate SQL Server computer will be used, you must install the SQL Server **Workstation components** option on the Meridian server. You must also enable remote connections to SQL Server on the separate server with either the SQL Server Surface Area Configuration program or the **Connections** options of SQL Server.

Installation

To install the Meridian on a server computer:

1. Perform the tasks described in Prepare For Installation.
2. Run the Meridian installation package.

   The Meridian setup wizard starts and searches for a previous installation. If one is found, you will be prompted to perform an upgrade as described in Upgrade Meridian.

   To start Meridian server installation on Windows Server Core, run the appropriate setup program listed in Download Installation Files from a command line window. The setup program will show the graphical setup wizard with which you can complete installation.

   The Meridian services can then be managed with Meridian Enterprise Administrator from a remote computer as described in Administer Meridian Enterprise Remotely. Rerun the program to change, repair, or uninstall the software.
3. If you are installing Meridian for the first time on a computer, the language selection page appears.

   Otherwise, the **Welcome** page appears.
4. Choose a language in which to install the software.
5. Click **OK**.

   The **Preparing to Install** page appears while the setup files are decompressed and then the **Welcome** page appears.

6. Click **Next**.

   The **License Agreement** page appears.

7. Read the license agreement.
8. Accept or reject the agreement.
9. Click **Next**.

   If you do not accept the license agreement, the installation will stop. If you accept the license agreement, the **Specify Program Folder** page shows the default location for 64-bit program files.

10. If you want to place most of Meridian's files on a non-system partition, click **Browse** and specify the destination for the 64-bit program files.

    The default folder is usually adequate.

11. Click **Next**.

    The **Specify Program Folder** page shows the default location for 32-bit program files.

12. If you want to place most of Meridian's files on a non-system partition, click **Browse** and specify the destination for the 32-bit program files.

    Again, the default folder is usually adequate.

13. Click **Next**.

    The **Select Server Roles** page lists the available server roles.

14. Select the roles that you want this server to perform.
15. Click **Next**.

    You can install other products on other servers. The **Select Features** page shows a tree view of the available server components. The required components and the components that comprise the server roles that you selected are selected by default.

16. Select the components that you want to install on this server.
    - The minimum configuration for a functional Meridian application server is the **EDM Server service** and **License Server** components.
    - If you want to run the License Server service on a different computer than the EDM Server service, **do not** choose the **License Server** option at this time. Run the setup program on the other computer and choose *only* the **License Server** option.

      See Run Accruent License Server On a Different Computer for additional configuration that may be necessary.
    - Select the **Microsoft SQL Server Driver** or **Oracle Driver** option if you will be using either of those systems regardless of the server where the database management system will be located.

The correct driver is required on the Meridian server.

- If the Meridian application server will also host PowerWeb, choose the **PowerWeb** option.

  Internet Information Services must already be installed or installation of this component will fail. The minimum IIS components that must be installed for proper operation of PowerWeb are listed in Meridian Application Server Requirements.

- You should choose the **Task Server** option *only* if you plan to implement custom server-based processes.

  For more information about Task Server, see Meridian Task Server.

- We recommend that you install all of the **System administration** components.

17. Click **Next**.

    If you selected the **License Server** role in step 14, the **Specify License Server Type** page appears. Otherwise, the **Logon Information** page appears; skip to step 19.

18. Choose between three options:

    - On the **Specify License Server Type** page, if you have not received term licenses or you do not want your licenses to be managed by Meridian Cloud:

      a. Accept the default of **On-premises license server for named and concurrent licenses**.

      b. Click **Next**.

         The **Logon Information** page appears; skip to step 19.

    - If you have received term licenses or you do want your licenses to be managed by Meridian Cloud:

      a. Select **Connection to Meridian Cloud license server for subscription licenses**.

      b. Click **Next**.

         The **Meridian Cloud Connection** page appears.

      c. Enter the information in the **URL**, **User name**, and **Password** fields that was provided to you when you received your Meridian Cloud tenant registration information.

      d. Click **Next**.

         The **Logon Information** page appears.

         The account under which the Meridian Enterprise License Server service is run must be able to connect to the Internet to use the Meridian Cloud license server.

If this is not permitted by your organization's security policy, limited time licenses that do not require a connection can be provided upon request. A utility program is installed with Meridian Enterprise for this purpose as described in Test Cloud License Server Connectivity.

- If you want to use an on-premises server for subscription licenses:
  a. Select **On-premises license server for subscription licenses**.
  b. Click **Next**.

19. Type the user name (or click **Browse** to find one) and password for one existing account to use for all the Meridian services and application pools that will be installed.

    If the account is in a complex domain, you can prepend the domain name like <*DOMAIN*>\<*User*>. This account must meet the security requirements described in Grant Domain Privileges With a Service Account. For a list of the other resources that can use the same account, see Service Account Usage.

20. If you are installing additional products to work with an existing Meridian Enterprise installation and you want this account to be assigned to those services too, enable the **Use this account for EDM and License services** option.

21. Click **Next**.

    The **Computer Browser** service must be running to be able to select a user. The service is disabled by default in some versions of Windows and must be started manually.

    The **Choose Computer** page appears.

22. Type the name of the server where Meridian License Server is installed.

23. Click **Next**.

    If you did not select to install the **Meridian Enterprise Server** component, the **Choose Computer** page appears.

24. Type the name of the server where Meridian Enterprise Server is installed.

25. Click **Next**.

    The **Specify Local Workspace Folder** page appears. This folder is used to cache documents on a local hard disk for maximum performance.

26. Accept the default folder or click **Browse** and select a different location.

27. Click **Next**.

    If you selected to install the **Site Cache** component, the **Specify Site Cache Location** page appears.

28. Accept the default folder or click **Browse** and select a different location.

29. Click **Next**.

    The **Select Vaults Folder** page appears.

30. Accept the default folder or click **Browse** and select a different location.
31. Click **Next**.

    For information about the amount space required and location options, see Document Storage Space Requirements. The **System Time** dialog box appears. It is extremely important that the correct date, time, time zone, and regional settings are made on both the server and all client computers, and that all client computers are time-synchronized with the server.
32. Click **OK**.

    The **Shared Extensions Folder** page appears. If any client extensions are registered in a vault, they will be copied to this location where they can be downloaded by the client PCs when the vault is opened. The setup program will create a hidden share for this folder. All users require read access to this location. Usually the default folder is acceptable.
33. Accept the default folder or click **Browse** and select a different location.
34. Click **Next**.

    The **Start Copying Files** page appears.
35. Review all your choices.
36. Click **Next**.

    The installation begins and the progress is shown on the **Setup Status** page.
37. When installation is completed, you will be prompted to click **Finish**.
38. If any other server computers will be used with Meridian, configure a service account as described in Grant Domain Privileges With a Service Account.
39. Upgrade any existing vaults as described in Upgrade Meridian Vaults.

Install the Server Components Silently

In some situations it can be convenient to automate the installation of server components to save time or to ensure identical installations. This can be done by running the Meridian executable setup program in silent mode with a response file that provides the setup program with all of the desired setup choices.

To perform silent installation of the server components:

1. Run the setup program to completion with the optional record mode command switch: `BC-Meridian Server (x64).exe -r`.

   The setup program runs interactively so that you can choose installation options. The setup program stores your installation options in a response file named `Setup.iss` that is created in the `Windows` folder.

   To specify an alternative response file name and location, also use the option `/f1<Path>\<FileName>`.

2. Run the setup program again with the optional silent mode command switch: `BC-Meridian Server (x64).exe -s`.

   The setup program runs silently with the installation options provided by the response file that you created in step 2.

3. Test the installation for the expected results.

   If you encounter problems, first read the `AMM-Setup<BuildNumber>.log` file located in the `Windows` folder for errors.

   If necessary, uninstall the components, edit the `Setup.iss` file, and repeat the installation until you obtain the correct results.

Although the principle remains the same for each Meridian release, some response file options may be discontinued over time and some new options may be introduced.

Test Cloud License Server Connectivity

When Meridian is configured to use the Meridian Cloud license server as described in Install the Server Components, it can be helpful to test the connectivity with your network, server computer, and service account before requesting assistance from Accruent Support. A graphical testing program is installed with Meridian for that purpose if **Connection to Meridian Cloud license server** is enabled during setup.

> **Important!**
> For the connection to work, you must have TLS 1.2 installed. Additionally, you must also set the **SchUseStrongCrypto** registry key value to **00000001** in the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\` registry key.
>
> To learn more about these requirements, see How to enable TLS 1.2 on clients on the Microsoft website.

To test connectivity:

1. On the Meridian Enterprise application server, open `DAWebServiceTest.exe`.

   By default, it is installed in the `C:\Program Files\BC-Meridian\Program\ACLicense` folder. The **Cloud Licensing Test Utility** window opens.
2. Type values using the descriptions in the following table.
3. Choose between three options:
   - **Claim** to claim subscription licenses for the specified users
   - **Update** to check the state of subscription licenses for the specified users
   - **Get Token** to get an access token for the cloud license service

   The full address of the operation (based on the **Base URL**) is shown in **Full URL**. The result of the operation is shown in **Result**.

Program options

Option	Description
Base URL	URL of the Meridian Cloud tenancy to test, for example, `https://my-org.meridian360.com`.
User IDs	Comma separated list of user names with which to test license claims, for example, **bjohnson, tjones**.

Install the Client Components

The following instructions describe how to install the client software for Meridian on-premises deployments using the installation package that accompanies the Meridian server installation package.

To install Meridian on a client computer from a command line or batch file with the Windows Installer package, see Control Windows Installer Packages.

Installation

To install the Meridian client components on your computer:

1. Run the Meridian client installation package.

   The Meridian setup wizard starts and searches for a previous installation. If one is found, you will be prompted to perform an upgrade as described in Upgrade Meridian.

   > **Note:**
   > To start Meridian server installation on Windows Server Core, run the appropriate installation package listed in Download Installation Files from a command line window. The installation package will show the graphical setup wizard with which you can complete installation.
   >
   > The Meridian services can then be managed with Meridian Enterprise Administrator from a remote computer as described in Administer Meridian Enterprise Remotely. Rerun the installation package to change, repair, or uninstall the software.

   The setup files are decompressed and then the **Welcome** page appears.

2. Click **Next**.

   The **License Agreement** page appears.

3. Read the license agreement.

4. Accept or reject the agreement.

5. Click **Next**.

   If you do not accept the license agreement, the installation will stop. If you accept the license agreement, the **Destination Folder** page shows the default location for the program files.

6. Click **Change** and specify the destination for the program files if you want to place most of Meridian's files on a non-system partition.

   The default folders are usually adequate.

7. Click **Next**.

   The **Setup Type** page appears.
8. Select one of the following options depending on the required client components:
   - **Complete** installs all of the client components including application links using the default options.
   - **Custom** installs only the components that you select on the **Custom Setup** page.
9. Repeat step 8 until you have finished selecting components.
10. Click **Next**.

    The **Choose Computer** page appears.
11. Type the name of the Meridian application server (provided by a System Administrator).
12. Click **Next**.

    If you selected the **PowerWeb** component, the **Specify PowerWeb URL** page appears.
13. Type the URL of the Meridian web server (provided by a System Administrator).
14. Click **Next**.

    If you selected the **PowerWeb** component, the **Specify Site Cache URL** page appears.
15. Type the URL of the Meridian site cache server (in most cases, the same URL as the Meridian web server).
16. If you will use the same single sign-on authentication provider to log on as your Meridian Portal tenancy, enable **Use External Authentication** and then type the name of your Meridian Portal tenancy in **M360 Tenant Name**.
17. Click **Next**.

    The **Specify Local Workspace Folder** page appears. This folder is used to cache documents on a local hard disk for maximum performance.
18. Accept the default folder or click **Change** and select a different location on your PC.
19. Click **Next**.

    The **Ready to Install the Program** page appears.
20. Click **Install** to complete installation.

Add Components to an Existing Installation

1. In the Windows **Control Panel**, in the **Programs and Features** folder, select **Meridian Enterprise** and then click **Change** in the toolbar.

   The Meridian setup program starts.
2. Click **Next**.

The **Program Maintenance** page appears.

3. Select **Modify**.
4. Click **Next**.

   The **Custom Setup** page appears.
5. Select the components that you want to add to the installation.
6. Click **Next**.

   The **Ready to Modify the Program** page appears.
7. Click **Install**.

   The existing installation is modified with your component selections.

Install the Client Components Silently

In some situations it can be convenient to automate the installation of client computers to save time and ensure identical installations. This can be done by running the Meridian setup program in silent mode with a response file that provides the setup program with all of the desired setup choices.

1. Copy all of the Meridian installation files to a shared disk accessible by all of the client computers.
2. Run the setup program to completion with the optional record mode command switch: `setup.exe -r`.

   The setup program runs interactively so that you can choose installation options. The setup program stores your installation options in a response file named `Setup.iss` that is created in the `Windows` folder.

   To specify an alternative response file name and location, also use the option `/f1<Path>\<FileName>`.
3. Run the setup program from a test computer with the optional silent mode command switch: `setup.exe -s`
4. Test the installation for the expected results.

   If you encounter problems, first read the `AMM-Setup<BuildNumber>.log` file located in the Windows system folder for errors.
5. Run the same command line on the remaining computers to repeat the installation.

Although the principle remains the same for each Meridian release, some response file options may be discontinued over time and some new options may be introduced.

Control Windows Installer Packages

In addition to the Meridian server setup program, the Meridian distribution package includes Windows Installer (MSI) packages for the Meridian client programs, which can be run from a command line.

The Meridian client installation packages install only client components and cannot be used to install server components or developer components. Use the server setup program to install the server components as described in Install the Server Components and Install the Developer Components.

To install a package with the default options, double-click the file to open it with the Windows Installer program. The program will present an installation wizard for manually choosing available installation options.

If you want to install a package on many computers with Active Directory or another automated deployment method, run the Windows Installer program in a command window with the optional command-line arguments and switches to specify the installation options you need.

The command-line arguments supported by the Meridian installation packages are listed in the following table:

Windows Installer package command-line arguments

Argument	Description
ADDLOCAL	Comma-separated list of product components to install.
EDMSERVERNAME	Default Meridian application server name. Not applicable for PowerWeb installation.
INSTALLDIR	Optional path of the destination application folder. If omitted, the default folder will be used.
LWSFOLDER	Path of the local workspace folder.
OPENID	If set to **1**, connect this PC to the site cache server specified by SCURL using the OpenId authentication credentials specified in the configuration of the tenant specified by TENANTNAME. If this value is **0** (default), connect to the site cache server via the logged on Windows account.
OFFLINEMODE	If set to **1** (default if the PowerUser client component is not selected during interactive installation) or omitted, Application Integration (local workspace synchronization) is set to Remote mode. If set to **0**, it is set to Online mode. Use this setting in combination with WEBSERVICESMODE.

Argument	Description
PUC_ICON	If set to **1** (default) or omitted, creates a PowerUser shortcut on the Windows desktop. If set to **0**, the shortcut is not created.
SCURL	URL of the site cache server for use by the client.
TENANTNAME	Name of the Meridian Portal tenancy configuration where the OpenId credentials are specified with which to connect to the site cache server specified by SCURL. Use this setting in combination with OPENID.
TRANSFORMS	Optional language support file name. If omitted, the English language is installed.
WEBACCESSURL	URL of the web server where the PowerWeb components are installed.
WEBSERVICESMODE	If set to **1** (default) or omitted, Application Integration (local workspace synchronization) connects to the vault through the PowerWeb server (Remote mode). If set to **0**, it is set to Online (LAN) mode. Use this setting in combination with OFFLINEMODE.
WEB_ICON	If set to **1**, creates a PowerWeb shortcut on the Windows desktop. If set to **0** (default) or omitted, the shortcut is not created. • If set to **1**, the WEBACCESSURL argument must be specified. • This argument must be specified as /VWEB_ICON=1 (no spaces) for use with the executable version of the PowerWeb setup package. No special syntax is necessary if the setup package is unpacked as described in Install the Client Components Silently.

Command-Line Switches

The Windows Installer program's command-line switches can be used together with the Meridian package arguments to further control the installation, such as for display, restart, logging, and repair options. For example, use the `/quiet` switch to install a product without user interaction. Refer to the Windows Installer help (`msiexec /help` or `/?`) for the additional command-line switches supported. For a list of the values supported by the **ADDLOCAL** property, refer to Install Or Remove Optional Components.

The install options and properties (following `/i`) must be followed by the display options (`/quiet` above), restart options (`/norestart` above), and log options (`/log` above) for the installation to work.

Example PowerWeb installation

The following example uses some of the Meridian options provided in the Windows Installer Packages:

```
msiexec /i "BlueCielo Meridian Enterprise (x64).msi"
LWSFOLDER="C:\BC-WorkSpace\"
INSTALLDIR="C:\Program Files\BC-Meridian" INSTALLDIR32="C:\Program
Files (x86)\BC-Meridian"
WEBACCESSURL="http://Rainier/Meridian/Start"
SCURL="http://SCServer/BCSiteCache"
ADDLOCAL="Common,AMHook,Download,Viewer,DBX,NETInterops" /quiet
/norestart
/log "C:\Temp\BCME2017-Setup.log"
```

This example will result in the following:

- The Meridian PowerWeb client will be installed
- The local workspace folder will be set to `C:\BC-WorkSpace\`
- The 64-bit program files will be installed in folder `C:\Program Files\BC-Meridian`
- The 32-bit program files will be installed in folder `C:\Program Files (x86)\BC-Meridian`
- The PowerWeb shortcut will be set to `http://Rainier/Meridian/Start`
- The site cache URL will be set to `http://Rainier/BCSiteCache`

- The following components will be installed:
  - Common client components
  - Application Integration
  - Viewer
  - Autodesk ObjectDBX viewer support
  - .NET interop assemblies
- The installation will run in Quiet mode with no user interaction (including progress bar)
- The computer will not be restarted upon completion
- All setup output will be logged to the file `C:\Temp\BCME2018-Setup.log`

Install Or Remove Optional Components

The Meridian client installation packages support installing individual components in a command-line installation by using the **ADDLOCAL** property. To remove individual components using a command line, specify them with the **REMOVE** property. The package supports the following values for these properties. The values are case-sensitive. Spaces are not allowed. Misspelled values will cause the entire command line to fail.

For example, to remove the application links for a subset of users, run the following command line:

```
msiexec /i "C:\Temp\BlueCielo Meridian Enterprise.msi"
INSTALLDIR="C:\Program Files\BC-Meridian"
REMOVE="Acad2018,Inventor" TRANSFORMS="1053.mst"
/quiet /norestart /log "C:\Temp\BCME2018-Setup.log"
```

PowerWeb

Component property values

Value	Component	Required	Required for document viewing	Optional	Optional, requires NetInterops	Optional, requires DBX	Notes
Common	Common client components	**Yes**	No	No	No	No	
Download	PowerWeb functionality	No	No	**Yes**	No	No	
Viewer	Accruent viewer	No	**Yes**	No	No	No	

Value	Component	Required	Required for document viewing	Optional	Optional, requires NetInterops	Optional, requires DBX	Notes
DBX	Autodesk RealDWG library support	No	**Yes**	No	No	No	Also required for DWG title block data exchange and asset tag extraction.
AMHook	Application Integration	No	No	No	**Yes**	No	Required when any component other than PowerWeb is installed and required to use a site cache.
NETInterops	Accruent .NET interop assemblies	No	No	No	**Yes**	No	

Install Second Language Support

Meridian user interface support for the English language is built in. The PowerWeb, Meridian Explorer, and Meridian Enterprise Server support a user-selected language. The Meridian Windows applications (PowerUser, Configurator, and Administrator) support a second language in addition to English.

You can install a second language in one of two ways:

- Select the language from the setup program during installation (`setup.exe` only)
- Use the **TRANSFORMS** argument with the command line (`.msi` files only) to specify the support file that corresponds to the language that you want to install. You may only install support for one language other than English.

  See the following table for the filenames of the language support files. For more information about using the command line, see Command-Line Switches.

You may not install a second language after the initial installation. After you have installed support for a non-English language, you can switch between that language and English and vice versa. Support for the English language does not require separate installation.

- Language support only affects the Meridian software user interface and how dates are shown. It does not affect vault configuration or customization text (property names, for example) or document content and its metadata, which remain in the original language.
- Dates can be displayed in formats other than that of the selected Windows locale by setting the **LCID** value of this registry key, which also affects PowerWeb:

  HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion

  If the default date format for the selected locale does not meet your needs, you can create a custom locale as described in Custom Locales.

Supported Languages

These language versions are only available through special channels. Contact Accruent Sales for more information.

Meridian currently supports the following languages:

Language strings and filenames

Language	String	Filename
Brazilian	Bra	1046.mst
English	Eng	1033.mst
Finnish	Fin	1035.mst
French	Fre	1036.mst
German	Ger	1031.mst
Italian	Ita	1040.mst
Japanese	Jap	1041.mst
Korean	Han	1042.mst
Polish	Plk	1045.mst
Russian	Rus	1049.mst
Spanish	Esp	1034.mst
Swedish	Sve	1053.mst

Switch from Non-English Language to English

To switch from a non-English language to English:

1. Install support for the non-English language using one of the methods at the beginning of this topic.
2. Modify the default **Language** value in the following registry keys:

   `HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion`
   `HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager View Control2`

   The default is the language that was selected during installation. Set the value to **Eng**. You may then switch back to the non-English language by setting the value back to the default (the corresponding language string in the following table). This sets the language the current user of the PC.
3. Restart Application Integration (`AMHookTray.exe`) for the change to take effect there.

Switch from Non-English Language to Non-English Language

To switch from one non-English language to another non-English language:

1. Install support for the first non-English language using one of the methods at the beginning of this topic
2. Install support for the second non-English language on a different computer using one of the methods at the beginning of this topic.
3. Copy the support files for the second language to the computer where you want to switch languages.

   The files are those with names that begin with the language string in the following table (for example, `FRE*.*` for French). Copy the files from the 32-bit program folder (by default, `C:\Program Files (x86)\BC-Meridian\Program`) and from the `Cyco Shared` folder (by default, `C:\Program Files (x86)\Common Files\Cyco Shared`). Do this for either the 32-bit or the 64-bit versions. The 64-bit version does not have its own language support files, but uses the 32-bit files.
4. Modify the registry value as described in the preceding task.
5. Restart Application Integration (`AMHookTray.exe`) for the change to take effect there.

Set Language for All Users of a Computer

To set the language for all users of the same computer (for example, a remote session host):

- Modify the default **Language** value in the following registry key:

  `HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion`

  This value overrides the value in the `HKEY_CURRENT_USER` hive.

  Installation files for language support can be found in the same folder as the setup package (`.msi`) file. The language support files are named according to the Windows locale codes.

Switch Language in Viewer

To manually switch the language that is shown in the viewer:

1. Right-click anywhere within the viewer window.

   The shortcut menu appears.

2. Click **Viewer Options**.

   The **Accruent View Control** dialog box appears.

3. On the **General Options** tab, in the **Common settings** branch, select the language string in the **Language** list.
4. Click **OK**.

Upgrade An Existing Installation

If a previous product version is already installed, the existing product components can be upgraded by omitting the command-line arguments. For example:

```
msiexec /i /quiet "C:\Temp\Accruent Meridian Enterprise.msi"
```

Deploy Standard Viewer Settings

Meridian provides a feature for updating client computers that can be used to deploy standard viewer settings for all users. The feature can be used similar to how client computers can be automatically upgraded as described in Upgrade Meridian Client Computers Automatically.

When a Meridian client computer starts, the program `AMUpdateU.exe` runs and reads the file `AMUpdate.ini`, if found on the Meridian Server. The file does not exist by default. For each item found in `AMUpdate.ini`, the program looks for a corresponding registry value in the following key on the client computer to determine if the item has been installed already or if the installation failed:

`HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\Update`

By default, `AMUpdateU.exe` first looks for `AMUpdate.ini` in the location specified by the **SharedFolder** registry value in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server as described in the *Meridian Enterprise Administrator's Guide*. If that location does not exist, `AMUpdateU.exe` then looks for the file on the server where the vault resides that was last opened.

If the item is new or failed, its corresponding command line is executed to update the client computer. The command line that is executed should create or update the DWORD value named **ExitCode** in the preceding registry key and set it to **0**, indicating success. The next time that the client computer is started, `AMUpdateU.exe` will find the **ExitCode** value and not run the same command line. If the value is missing or is set to a value greater than 0, `AMUpdateU.exe` interprets the value as failure of the command line and executes it again, for example, in case the user did not have sufficient privileges or an intermediate error occurred.

Notes about Functionality

- For the process to succeed, the client computer's user must have privileges to copy the file and to modify the computer's registry. For example, they must be a member of the computer's **Administrators** group. If this does not comply with your security policy, consider providing the users the privilege on a temporary basis or deploying the file using a different program.
- Additional viewer settings are stored in the Windows registry in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager View Control2 (64-bit key. The 32-bit key is located in the **Wow6432Node** parent branch), as described in the *Meridian Enterprise Administrator's Guide*. For example, the available viewers are registered in the **DocViewPlugin** child branch.

To remove user access to a particular viewer, rename or delete the entire child key that contains the viewer name in its default value (for example, **Acrobat**). If the user is not a member of the **Administrators** group of the PC, they will not have sufficient privileges to recreate the key and it must be done by an administrator or a Meridian Enterprise setup program.

To deploy these settings, the batch file that you create can add the desired settings to the client computer registry using Registry Editor and an export of a preconfigured registry key.

- To prevent users from changing the priority of the viewers as described in the *Change Viewers* article in the *Meridian Enterprise User's Guide*, see the **DisableChangeViewerPriority** registry value in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager View Control2\Settings, as described in the *Meridian Enterprise Administrator's Guide*.

Deploy Standard Settings

1. In Meridian running on any client computer, configure the viewer settings that you want to deploy as standard settings.

   The viewer settings are stored in the file `C:\Users\<UserName>\AppData\Roaming\Cyco\AutoManager View Control2\avx.ini`.

2. Copy the settings files to the Meridian extensions folder on the server.

   By default, this folder is located at `C:\BC-Meridian Extensions`.

3. In the Meridian extensions folder on the Meridian application server, create a batch file to copy the settings files to the client computers as in the following example:

   ```
   COPY avx.ini
   C:\Users\%USERPROFILE%\AppData\Roaming\Cyco\AutoManager View Control2
   ```

4. In the Meridian extensions folder on the Meridian application server, edit the text file named `AMUpdate.ini`.

   If the file does not exist already, create it with a text editor.

5. Add a line to the file similar to the following in the **AutoManager Meridian** section where <BatchFileName> is the name of the batch file that you created.

   The name on the left side of the expression can be anything that you want. If you are creating the file anew, add the section name as shown in the example:

   ```
   [AutoManager Meridian]

   ViewerSettingsUpdate=<BatchFileName>
   ```

Configure Default PowerWeb User Settings

PowerWeb users can configure personal preferences as described in the *Personal Preferences* article in the *Meridian Enterprise User's Guide*. These settings are stored on the PowerWeb server in a profile file for each user. The settings can be overridden by editing their profile file, as described in *Edit PowerWeb User Profiles* in the *Meridian Enterprise Configuration Guide*. The default settings are created as registry values on the PowerWeb server during setup and are copied to new profile files. The settings correspond directly to the options on the **Preferences** page of PowerWeb.

To configure the default PowerWeb user settings, create or modify the registry values described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\UserPreferences\Default.

Install the Developer Components

The Meridian Enterprise COM API was originally developed for use with Visual Basic 6. With the emergence of .NET as its replacement, Accruent provides the Accruent .NET Software Development Kit (SDK) for those customers who want to migrate existing Visual Basic 6 user interface extension projects to .NET (using Visual Basic .NET or other .NET-compatible languages) or to develop new extensions. Another key reason for providing the Accruent .NET SDK is to make it possible to create 64-bit standalone applications, supplementary ActiveX objects, and extensions that work with 64-bit applications such as 64-bit Inventor, Solidworks, or MS Office, which cannot be done with Visual Basic 6.

The Accruent .NET SDK includes a single library (.NET assembly `BlueCieloECM.InnoCielo.Meridian.dll`) and a set of Primary Interop Assemblies (PIAs). The library provides a .NET alternative for commonly used classes of the Meridian Enterprise COM API. All of these assemblies are installed in the `BIN` sub-folder where the SDK is installed and registered in the Global Assembly Cache (GAC). The Global Assembly Cache is a computer-wide code cache provided by the .NET Framework that is used to store assemblies that need to be shared by several applications on the computer.

The library is compliant with the Common Language Specification (CLS). It provides a guarantee of interoperability with a wide range of .NET programming languages (like VB.NET and C#).

What To Expect After Meridian Installation

After a successful Meridian client installation, you can expect to see the PowerUser client shortcut on the Windows desktop:



You should also see a corresponding Meridian Application Integration icon added to the Windows system tray:



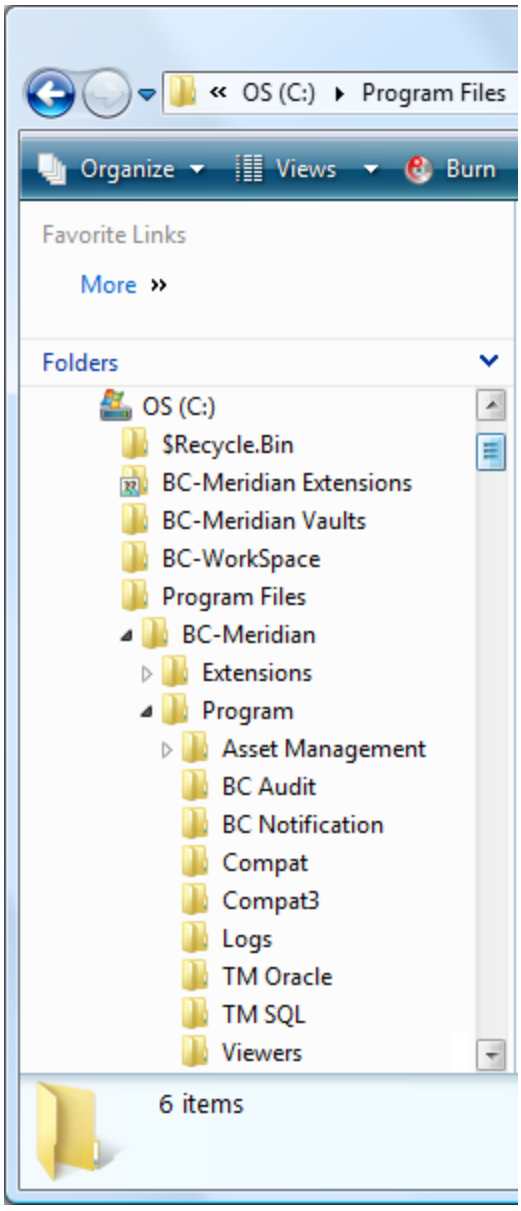
And a new Windows **Start** menu program folder should be present that includes shortcuts to all of the programs you chose to install as well as a **Help** folder containing shortcuts to electronic Help versions of related guides.

A log file named `BCME<Version>-Setup<BuildNumber>.log` is created by default in `C:\Program Files\Common Files\Cyco Shared`. This log file is a complete record of the actions that were taken by the setup program, and may be useful for support purposes. This file is not removed if Meridian is uninstalled.

> **Note:**
> If you installed a Meridian upgrade, your vaults will need to be manually upgraded as described in Upgrade Vaults To a Newer Database Engine before they can be seen by the Meridian clients.

Meridian Folder Structure

The Meridian setup program creates a number of folders as shown below:



These folders contain the files for various purposes as described in the following table:

Meridian folder structure

Folder	Description
`BC-Meridian Extensions`	Deployment folder for PowerUser custom extensions (shared as AMM3EXT$)
`BC-Meridian Vaults`	Root folder for all vaults managed by this server
`BC-WorkSpace`	Local Workspace folder
`BC-Meridian`	Root folder for program files
`Program`	Server and/or client executables depending on installation type
`Compat`	Class type libraries for backward compatibility
`Compat3`	Class type libraries for backward compatibility
`Viewers`	Registry files for third-party viewer support

Move the BC-Meridian Extensions Folder

During installation, the `BC-Meridian Extensions` folder is created on the C: drive of the server by default. You can change this location manually, if necessary, by performing the following steps:

> **Note:**
> Perform this task only when no users are accessing vaults hosted by the Meridian application server where the folder is located.

To move the BC-Meridian Extensions folder:

1. Open the **Sharing** tab of the `BC-Meridian Extensions` folder's properties and disable sharing temporarily.
2. Copy or move the existing folder to a new location.
3. Open the **Sharing** tab of the new location and share the folder as AMM3EXT$.

   The dollar sign ($) at the end of the name will make the share hidden to users to discourage abuse.
4. Open the server's registry and locate the following key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
   Meridian\CurrentVersion\Server
   ```
5. Change the value of the **SharedFolder** key to the new folder location.
6. Restart the AutoManager EDM Server service.

Upgrade Meridian

When run in interactive mode, the Meridian setup program will detect a previous version of Meridian, and offer to upgrade the previous installation.

Before proceeding with any upgrade, carefully consider the following points.

- You must install the upgrade first and at least on the Meridian application server and eventually all client computers.
- Older versions of the client applications will continue to work with the upgraded server, but this should be considered only a temporary measure until all client computers can be properly upgraded. Upgrade the client computers as soon as practical.

  Accruent does not provide technical support for production environments in which different versions of Meridian Enterprise software are used on server and client computers.
- The software will be installed in the existing folder structure. If the default folder names for the new software are different from the existing folders, the default folder names will not be used, which could make troubleshooting more difficult.
- After the upgrade process has completed, the setup program might prompt to restart the computer so that files that are in use can be deleted. If you choose to upgrade Meridian client computers automatically and configure the setup so that an automatic restart is not executed, the software will not function correctly until the computer has been restarted. After the computer has restarted, always log on to Windows with an account that has at least the same security privileges as the account that started the upgrade.

We highly recommend that you:

- Use the Server Installation Checklist to guide you through the upgrade process and complete all of the items in the **Upgrade** column that apply to your environment.
- Perform and troubleshoot the upgrade on a test server with a current copy of your production environment first before attempting to upgrade the production environment.
- Perform comprehensive user acceptance testing in a test environment before deploying the upgrade to the production environment.

Upgrade Meridian Vaults

When you install a Meridian upgrade, you must manually upgrade the vaults to the new version before they can be opened by the Meridian clients.

> **Note:**
> This will maintain the current database engine of the vault. To upgrade the vault to a newer database engine, see Upgrade Vaults To a Newer Database Engine.

To upgrade vaults:

1. Confirm that a verified backup of the vaults exists.
2. Open the Administrator tool from the **Start** menu.
3. Click **EDM Server** in the left pane.
4. On the **Action** menu, point to **All Tasks**, and then click **Upgrade Vault Wizard**.

   The **Vault Upgrade Wizard** appears.
5. Click **Next**.
6. Select the vaults to upgrade.
7. Click **Next**.
8. Confirm that you want to upgrade the vaults that are listed, and click **Finish**.

   The upgrade process begins and displays the results when complete.
9. Run the **Vault Consistency Wizard** tool as described in Vault Consistency Toolkit.

   If any serious errors are found, contact your Accruent Partner or Accruent Technical Support. If no serious errors are found, you may proceed with the server software upgrade.

Upgrade External Tables to Microsoft Access

With SQL Compact reaching End of Life status, Microsoft Access is now used as the default provider to store Table Data as of the Meridian 2022 release. Since many of our customers use SQL Compact, we have provided a tool that can be used to convert your tables to Microsoft Access.

To learn more about how this change affects Meridian, see our KnowledgeBase article about this topic.

> **Note:**
> You must first install Microsoft SQL Server Compact Edition 4.0 before using the conversion tool. Edition 3.5 is still required for installation. Both may be installed simultaneously.

To convert a lookup tables database:

1. Stop the **AutoManager EDM Server** service.
2. Navigate to the `C:\Meridian Extensions\<VaultName>` folder.
3. Run the following command in a Windows command prompt:

   ```
   "C:\Program Files\BC-
   Meridian\Program\BlueCieloECM.SdfToMdbConvertor.exe"
   <VaultName>$LL.sdf -TTAB
   ```

   The Microsoft Access database file (.mdb) is generated.
4. Navigate to HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server.
5. Set the **TablesDB** registry setting to **0**.

   If you are upgrading Meridian from a previous version, this step is required.
6. Restart the **AutoManager EDM Server** service.

   Your changes take effect.
7. Verify that the correct data is available in Meridian Enterprise and then remove the SQL Compact database files.

   The existence of lookup list databases can cause errors if queries exist in the vault script.

Upgrade Vaults To a Newer Database Engine

Occasionally, Accruent releases a newer generation of its database engines. Newer versions of Meridian might include small fixes to the database engines and upgrading is normally done as described in Upgrade Meridian Vaults. But large-scale optimizations take longer to develop and test and result in a new generation of engines. When this happens, you might want to upgrade a vault to take advantage of its new features and performance. Upgrading a vault to a new generation of database engine is typically not done during the normal vault upgrade process but must be performed manually.

> **Note:**
> An exception is when a vault that uses an older database engine (`ObjectSet*.dll`, `ht3*.dll`) is restored onto a 64-bit computer, the database engine is automatically upgraded to the latest database engine (`ht5*.dll`).

Manually upgrading a vault to a newer database engine can be done by either restoring the vault from a backup or by editing the Windows registry. In both cases, you specify a different database engine for the vault.

The filenames and descriptions of the different database engines are listed in the following table.

Database engine filenames

Database Engine	Filename	Description
First generation	ObjectSet.dll	Hypertrieve 32-bit
First generation	ObjectSQL.dll	SQL Server 32-bit
First generation	ObjectORA.dll	Oracle 32-bit
Second generation	ht3.dll	Optimized Hypertrieve
Second generation	ht3sql.dll	Optimized SQL Server
Second generation	ht3ora.dll	Optimized Oracle
Third generation (64-bit only)	ht5.dll	Multi-threaded Hypertrieve
Third generation (64-bit only)	ht5sql.dll	Multi-threaded SQL Server
Third generation (64-bit only)	ht5ora.dll	Multi-threaded Oracle

> **Note:**
> This task should only be performed during non-production hours and after a verified backup of the existing vault is made.

Upgrade during Restore from Backup

To upgrade a vault to a newer database engine during a restore from backup:

- Follow the procedure for restoring the vault from backup as described in Restore Backups except before running the **Restart After Restore From Backup Wizard**, edit the `datastore.ini` file in any text editor and change the value of the **DLLName** setting to the filename of the database engine that you want the restored vault to use.

Upgrade by Editing Windows Registry

To upgrade a vault by editing the Windows registry:

1. Disable and stop the EDM Server service with one of the following methods:
    - The **EDM Server** properties in the Meridian Enterprise Administrator
    - Microsoft Management Console (MMC)
2. Open the Windows registry and change the value of the **DLLName** setting described in the following topic to the filename of the database engine that you want the restored vault to use.

    HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<vaultname>\CompoundItemService
3. Re-enable and restart the EDM Server service.

Upgrade Meridian Client Computers Automatically

Meridian client computers can be upgraded automatically with new Meridian software. This can be particularly convenient if your organization has many Meridian client computers or the computers are remote from your location.

Automatic upgrades are executed by the program `AMUpdateU.exe`, which resides in the folder `C:\Program Files\Common Files\Cyco Shared`. This program is executed automatically each time the computer reboots. AMUpdateU looks for the following registry key for software updates that should be installed on the client:

`HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\Update`

The values found in this key are used to find corresponding sections in an AMUpdate.ini file located in the BC-Meridian Extensions folder on the Meridian application server. The file does not exist by default. AMUpdateU executes the upgrade packages listed in the file and updates the **ExitCode** value of the preceding key. This prevents the same upgrade from being installed more than once.

For the upgrade to succeed, the client computer's user must have privileges to modify the computer's registry and to install software components. For example, it must be a member of the computer's **Administrators** group. If this does not comply with your security policy, consider providing the users the privilege on a temporary basis only until the upgrade is installed on all client computers.

AMUpdateU can be used to deploy more than just software updates, as described in Deploy Standard Viewer Settings.

Automatic update is disabled on Meridian application servers when a rescue account is specified as described in Create a Rescue Account For Security Administration. Updates will still occur on the client computers.

Add Components To An Existing Installation

To add components to an existing installation, whether a server installation or a client installation, use the same installation package as the original installation. Do not run more than one installation package on the same computer.

For example, to add client components to a server for testing, reuse the server installation package. Or to add the PowerWeb to a PowerUser installation, reuse the client installation package.

Only use a different installation package if you want to add components that are not included in the original installation package. In that case, first uninstall the original installation first, then start the other installation package. For information about the components included in each installation package, refer to Download Installation Files.

To add components to an existing installation:

1. In the Windows **Control Panel**, in the **Programs and Features** folder, select **Accruent Meridian Enterprise** and then click **Change** in the toolbar.

   The Meridian installation package starts.
2. Click **Next**.

   The **Program Maintenance** page appears.
3. Select **Modify**.
4. Click **Next**.

   The **Custom Setup** page appears.
5. Select the components that you want to add to the installation.
6. Click **Next**.

   The **Ready to Modify the Program** page appears.
7. Click **Install**.

   The existing installation is modified with your component selections.

Install PowerWeb On a Different Server

In many situations, a different server already running IIS is available for hosting Meridian PowerWeb. This is a valid configuration so long as DCOM access is possible between the PowerWeb server and the Meridian server. For help installing PowerWeb with a firewall, see Allow PowerWeb Access Through a Firewall. The minimum IIS components that must be installed for proper operation of PowerWeb are listed in Meridian Application Server Requirements.

To install the PowerWeb server components on a server other than the Meridian application server:

1. Start the Meridian setup program on the PowerWeb server.
2. From the **Server** components list, select *only* **PowerWeb**. Do not install the **License Server** component.

   The **Administrator** components will be installed with PowerWeb because they are needed to create web locations of the vaults.
3. If prompted, type the name of the computer running the AutoManager EDM Server service.

In this configuration, user logon credentials will be required to authenticate the PowerWeb server to the Meridian application server. For more information, see Security Delegation.

Install Supplemental Documentation

Meridian is designed to show supplemental documentation that can be configured for each organization's unique needs. This documentation can be in the form of video tutorials (for example, those that are included with Meridian) or PDF files for any purpose. Some examples are:

- Optional Meridian module documentation
- Standard operating procedures
- Instructions for using vault customization

The file names of the documents will automatically appear in **Printable Documentation** and **Video Tutorials** sub-menus of the **Help** menu in the PowerUser client application.

To install supplemental documentation:

1. On the Meridian application server, create sub-folders named **Printable Documentation** and **Video Tutorials** in the folder specified for the user interface extensions share.

   By default, this folder is located at `C:\BC-Meridian Extensions`.

   Only these sub-folder names may be used.

2. Create at least one additional level of sub-folders to organize the supplemental documentation into different types, for example, **Administrator's Guide**, **Configuration Guide**, and so on as shown in the following figure.

   The sub-folder names may be anything you choose.

3. Place copies of the supplemental documentation files in these sub-folders.

   The folder and file names will appear in the **Help** menu the next time the users open the client applications.

   The file names in the **Printable Documentation** folder may be anything you want as long as they have the `.pdf` extension.

   For example, you might want to rename the Meridian documentation PDF files with names to match the documents' titles (`Meridian2017_UG_LTR.pdf` to `Accruent Meridian Enterprise User's Guide .pdf`), shorter names (`Meridian2017_UG_LTR.pdf` to `Meridian User's Guide.pdf`), or names in your native language (`Meridian 2017_UG_LTR.pdf` to `Guía del usuario de Meridian.pdf`).

Upon startup, the Meridian client applications will scan the **Printable Documentation** sub-folder structure for PDF files and scan the **Video Tutorials** sub-folder structure for HTML files. No other file types are supported.

Install the Webhelp Documentation

The documentation for Meridian Enterprise is available in several formats:

- **Printable PDF (`.pdf`) files**
- **Online webhelp (`.htm`) files**

  Displayed in all Meridian applications when the user presses **F1** on their keyboard AND:

  - The user has enabled the **I prefer online help** option in PowerUser, OR
  - The UseWebHelp registry key value is set to **1** on the Client PC.
- **Locally-hosted webhelp (`.htm`) files**

  Displayed in all Meridian applications when the user presses **F1** on their keyboard AND:

  - The user has enabled the **I prefer local help** option in PowerUser, OR
  - The UseWebHelp registry key value is set to **0** on the Client PC.

To learn more about PowerUser configuration options, see the *General Options* article in the *PowerUser* section of the *Meridian Enterprise User's Guide*.

As of the 2022 release, we no longer provide Microsoft HTML Help (`.chm`) files. To get a .zip file of the webhelp files, contact your Accruent representative or click the link on the Meridian software downloads page in your Customer or Partner Portal.

The help documentation is hosted by Accruent at the URL **https://help.meridian360.com**. The documentation can also be hosted on your web server to place it inside of your organization's firewall if Internet access is not permitted, for example. In that case, you are responsible for installing and maintaining the documentation.

Update locally-hosted webhelp

You can see when your local help was last updated by comparing the **Documentation Updates** page of your locally hosted help with the page in the Online Help.

1. Choose between two options:
   - Request the zip file from your Accruent representative.
   - Download the zip file from the Software Downloads page in your Customer or Partner Portal.
2. Extract the contents of the zip file.
3. Copy the contents from the unzipped file.

4. Navigate to **C:\Program Files\BC-Meridian\Help** on the machine where you want to update the help files.
5. Paste the contents of the unzipped file into the **C:\Program Files\BC-Meridian\Help** folder.
6. Click **Yes** to replace outdated files with updated versions.

Install the Subscriptions Viewer

Document subscriptions are enabled by creating the subscriptions database as described in Create a Subscriptions Database. The database contains the names of documents to which each user has subscribed. The subscriptions viewer allows users to view and remove their subscriptions and, with the **Allow Management of Subscriptions of Others** privileges, to do the same for other users.

The subscriptions viewer can be opened in PowerUser if the following conditions are met:

- The vault extension `BlueCieloECM.Extensible.UI.dll` is registered in Windows by a setup program.
- The option **Enable BlueCielo Publisher extension** is enabled on the **Advanced Features** page of the vault properties in the Meridian Enterprise Administrator.
- The subscriptions database connection string is configured as described in Create a Subscriptions Database and is valid.
- To also view the audit log (it uses the same extension), the audit log database connection string must be entered and **BC FDA Server** (M--FDS) and **BC FDA Client Extension** (M--FDE) licenses must be registered in Meridian Enterprise Administrator.
- The Publisher extension module must be installed when installing Meridian on a client machine.

The subscriptions viewer is a web application that is installed with the Meridian Enterprise PowerWeb components but the installation must be completed manually on the web server that will run the application. We recommend installing it on the PowerWeb server.

By default, the subscriptions viewer can only be opened from within PowerUser as described in the *View and Remove Subscriptions* article in the *Meridian Enterprise User's Guide*. The database connection string, user name, and user privileges are passed in the URL to the web application as encrypted data.

To open the subscriptions viewer outside of PowerUser, type a connection string (without the **Provider** keyword) in the **connectionString** attribute of the **BCNotesDBConnectionString** setting in the **appSettings** section of the `web.config` file of the web application.

Installation

1. On the web server, in Internet Information Services Manager, in the default website, locate the web application **WebExtensibilityDBViewer**.
2. Disable all authentication types except **Windows Authentication**.
3. Set user permissions to the viewer to meet your organization's requirements.
4. If necessary, set the identity of the DCOM service used by the viewer as described in Configure the DCOM Identity Of Remote Services.

Test the Viewer

1. Subscribe to one or more documents as described in the *Subscribe To Changes* article in the *Meridian Enterprise User's Guide*.
2. View your subscriptions as described in the *View And Remove Subscriptions* article in the *Meridian Enterprise User's Guide*.

Install the Meridian API Service

The Meridian API Service is the key to enabling the Meridian Mobile app. With it, users can find, view, and participate in document workflows from anywhere on your LAN with mobile devices.

To use the Meridian Mobile app, the Meridian API Service must be installed on the Meridian Enterprise server.

The Meridian API Service can be installed on a Meridian Enterprise 2019 R1 or higher server with the Meridian Enterprise server installation package described in Install the Server Components. The service can also be installed on Meridian Enterprise 2018 R2 or higher servers with a separate Windows Installer package as described below.

Prerequisites

Complete the following tasks prior to installation:

1. For Meridian Enterprise versions prior to 2019 R1, download the Meridian API Service installation package from the Accruent Customer Portal.
2. Uninstall any previous version of the API service.
3. Verify that the following are installed on the Meridian Enterprise server:
    - These components can be installed in advance:
        - Microsoft .NET Framework 4.6.1
        - Microsoft Internet Information Services
        - **BC Enterprise website** component
    - For use with HTTPS, the SSL certificate should be issued to the domain where the Meridian API is installed. Use a validated SSL certificate signed by a certificate authority (CA).
    - The Meridian Enterprise vault registered in the Meridian Enterprise Server configuration as described in the *Register a Meridian Enterprise* vault article in the *Meridian Enterprise Server Administrator's Guide*.
    - A Meridian Explorer repository created in the Meridian Enterprise Server configuration as described in Create a Meridian Explorer repository.
    - A Meridian Explorer view configured for use by Meridian Mobile as described in the *Create and edit repository views* article in the *Meridian Enterprise Server Administrator's Guide*. The following options must be enabled:

    - **Accessible by the Meridian Explorer app for mobile devices** option as described in the *Create and edit repository views* article in the *Meridian Enterprise Server Administrator's Guide*.
    - **Enable relational searches** option as described in the *Configure miscellaneous search options* article in the *Meridian Enterprise Server Administrator's Guide*.
    - For document and tag views, full-text search must configured as described in the *Configure miscellaneous search options* article in the *Meridian Enterprise Server Administrator's Guide*.
  - A Meridian Explorer repository synchronization job configured and running without errors as described in the *Create a publishing job* article in the *Meridian Enterprise Server Administrator's Guide*.

- The service will be installed under the **Default Web Site** in a virtual folder `M360.Meridian\api` as an application with the name of the current version being installed (for example, v2, v3, and so on). The files will be installed at `C:\Inetpub\wwwroot\M360.Meridian` by default.
- Only the default API path of `https://<ServerName>/m360.meridian/<api_version>/` is supported.
- Users of Meridian Mobile must enter their user name as either:
    - *<UserName>* (local computer account)
    - *<DomainName>**<UserName>* (Active Directory account)

  UPN format (*<UserName>*@*<DomainName>*, for example) is not supported.

  They must enter the server name as either:
    - *<ServerName>*
    - *<ServerName>*.*<DomainName>*
- Service logs for troubleshooting are located in the folder `C:\Inetpub\wwwroot\M360.Meridian\api\<api_version>\Logs` by default.
- Meridian Mobile requires Meridian Explorer Standard or Meridian Explorer Plus licenses be registered on the Meridian Enterprise License Server.
- To allow access by Meridian Mobile users outside your organization's firewall, implement one of the following solutions:
    - Install the Meridian API Service on a web server running IIS in your DMZ. The web server will communicate via DCOM with the Meridian application server inside the firewall.
    - Configure a VPN on the mobile devices to provide a secure connection through the firewall to the Meridian API Service installed on an internal web server running IIS.

Interactive Installation

1. On the Meridian EDM server, start `M360MeridianApiServiceSetup.msi`.

   The setup wizard welcome page appears.
2. Click **Next**.

   The **IIS Application Pool** page appears.
3. Click options or type values using the descriptions in the following table.
4. Click **Next**.

   A progress page appears while the service is installed. When the installation is complete, the final page appears.
5. Click **Finish**.

   The setup wizard closes.

IIS Application Pool options

Option	Description
User name	Type the name of a domain account to assign to the application pool **M360.Meridian** under which the service will run. This account must be the same account under which the Meridian EDM Server service runs. For more information about the requirements of this account, see Grant Domain Privileges With a Service Account.
Password	Type the password for the account

Unattended Installation

To install the Meridian API Service unattended:

- Run the following command line with the correct values for your environment:

```
msiexec /passive /i "M360MeridianApiServiceSetup.msi"
    APPPOOL_IDENTITY_NAME="<AccountName>"
    APPPOOL_IDENTITY_DOMAIN="<DomainName>"
    APPPOOL_IDENTITY_PWD="<Password>"
    INSTALLLOCATION="<Path>"
```

Test Installation

Open the following URL in a browser:

`https://<ServerName>/m360.meridian/api/<api_version>/checks/health`

If the service is installed and working correctly, the service will return **status: "Healthy"**

The following table lists the available settings that can be configured by editing the application's `web.config` file.

Meridian API Service settings

Option	Description
Authorization.Issuer	Case-sensitive StringOrURI value that identifies the principal that issued the access token. Must be unique per on-premise installation.
Authorization.TokenTimeout	Access token timeout formatted as *<Hours>:<Minutes>:<Seconds>*. The default is 00:30:00 (30 minutes).
Authorization.Key	Key with which to sign the access token. Must be unique per on-premise installation. The length should be more than 16 characters.
PageMaxLimit	The maximum number of items to return per page when a call is made and the limit parameter specified is greater than 1000. The default is **1000**.
PageDefaultLimit	The default number of items to return per page when a call is made with the offset parameter specified. The default is **100**.
UseAdvancedSearchProperties	By default, this setting is set to **false**. When set to **false**, the mobile app uses Property Navigation for document filtering. When set to **true**, the mobile app uses Advanced Search for document filtering.

Install Apryse BIM Server

The Apryse IFC Viewer provides visualization of 3D models contained in Industry Foundation Classes (IFC) files.

This viewer is a fully web-based component in which a user can view and navigate a 3D model and inspect metadata contained in the IFC file. The viewer is integrated in the PowerWeb and Explorer clients.

To function, IFC files need conversion to an intermediate (.vsfx) format, which requires a server component, the BIM Server. The BIM Server runs as a Window service. We recommend deploying the BIM Server on the machine hosting the Publisher. When the rendition of a document has the IFC format, updating the rendition triggers the BIM Server to convert the IFC file.

In addition to the BIM Server, a BIM Proxy IIS application is needed to provide secure access to the .vsfx files.

This article describes the installation procedure of these components.

> **Important!**
> The .vsfx files are stored in the folder `C:\MM\BIM\server\sys\data\output` on the machine hosting the BIM Server. In Meridian 2023, this location cannot be changed. The .vsfx files need to be preserved because they are required by the IFC viewer. Make sure the content of this folder is included in the procedure to back up the Meridian streams files.

Prerequisites

Complete the following tasks before installation:

1. Make sure the IFC rendering module is installed during Meridian installation.
2. Download the BIM Server files from this link.

   The `BIMFiles.zip` archive contains all files related to the BIM server. You can find the following files in the archive:

   a. `Bimserver.zip`
   b. `BimProxy.8.3.14.zip`
   c. `BimProxySettings.dat`
3. Extract the `Bimserver.zip` file and move the extracted file to an appropriate directory, such as `C:\program files\BC-Meridian\Program\BcBimServer`.
4. In the **Command Prompt**, execute the following command: `set GIN_MODE=release`.
5. Copy the `BimProxySettings.dat` file to the following folder: `C:\ProgramData\BlueCieloECM\BimProxy`.

6. Edit the `BimProxySettings.dat` file. Add the `UploadFolder` property to include the path of the folder to which the files will be uploaded.

   The upload folder must be in the same directory where the Apryse BIM server (`wv-3d-bim.exe`) is placed, in the following format: `\sys\data\source\uploaded`.

   For example: `C:\program files\BC-Meridian\Program\BcBimServer\sys\data\source\uploaded`.

7. Add the `BimServerUrl` property to the Apryse BIM Server URL.

   A typical value would be `http://localhost:8085`.

8. Add a registry key in `HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager Meridian\CurrentVersion\WebLink`.

9. Create a string property with the name `BimServerURL`. Provide the URL of the `BcBimProxy` web application you created in the IIS.

   A typical value would be `http://localhost/BcBimProxy`.

Create application pool and BcBimProxy website

Follow these procedures on the Enterprise Server machine:

1. Install the `BCBimProxy` website in IIS.
2. To add an application pool, in IIS, right click **Application Pools**and click **Add Application Pool**.

   Name it as appropriate. For example `BimProxyPool`.

3. Make sure the login is set to the Windows username and password that are used to log into the system.
4. Create a `BcBimProxy` folder under `inetpub\wwwroot`.
5. Copy the content of the BcBimProxy.8.3.14..zip file to the `BcBimProxy` folder.
6. To add a website (`BcBimProxy`), right click **Sites**, click **Default Website**, and click **Add Application**.
7. Change the **Application Pool** to the `BimProxy` pool that you just created. Set the physical path to the `BcBimProxy` folder that you created in step 4.
8. Make sure the Windows username and password are configured in **Connect as...**, under **Basic Settings**. Use **Test Settings** to make sure the provided credentials are valid.
9. Make sure **Windows Authentication** is set to **Enabled**.
10. Perform this step in the same directory where `BIMService` is present. To install the Windows service , in the **Command Prompt** in administrator mode, execute the commands below. Replace `[pathto]` with the actual path to the service in your system.

```
sc create "Meridian BIM Service" binpath= "
[pathto]\BIMService.exe” .
sc description "Meridian BIM Service" "Provides data
conversion for the 3D IFC Viewer”
```

11. Open Windows **Services** (services.msc). Find and start the **Meridian BIM Service**.
12. Access `https://[machinename]/BCBIMProxy/ping`.

    The URL should result in a `pong` output.
13. In the Meridian Enterprise Server Administration Console, under **Options**, click **Viewer**.
14. In **Viewer Options**, add the `BcBimProxy` URL in **BIM Server URL**.
15. In IIS, click **Request Filtering**.
16. Click **Allow Verb** and add an "`OPTIONS`" verb .
17. Restart IIS.
18. In Enterprise Server, create a rendering job and try rendering an IFC file from PowerWeb.

Run the BIM Server without a service

You can also run a BIM server without a service.

In the directory where the BIM Server executable and `config.json` are present, open the **Command Prompt** and execute the following command: `wv-3d-bim.exe -c “config.json”`.

Additional information

- A time out error might occur while converting an IFC file. This is a known issue. Normally, the conversion works in a second attempt.
- If you get a 500 internal server error, make sure the service is configured and running properly.
- To uninstall the service, execute the following command: `sc delete "Meridian BIM Service"`.

Uninstall Meridian

Removing Meridian from either a server or client computer is an easy process performed by following these steps:

1. In Windows Control Panel, click **Programs and Features**.

   A list of the installed programs appears.

2. Select the Meridian product to be removed and click **Uninstall**.

   The Setup wizard for the selected product appears.

3. Select **Remove** and click **Next**.

   The program will prompt for confirmation before starting the uninstall process.

4. Click **OK**.

   If the program finds that Meridian server components are installed on the computer, it will prompt for confirmation to remove all vault-related registry data.

   > **Important!**
   > This registry data is necessary to make vault data accessible by Meridian.

   Registry information for reserved licenses and PowerWeb **Find** form customization are also not removed in case Meridian is reinstalled on the same computer. This information is retained only if Meridian 2010 or higher was newly installed on the computer. If Meridian was upgraded from an earlier release, this information will be removed if the product is uninstalled.

5. Choose between two options:

   - Click **No** if Meridian will be reinstalled on the computer.
   - Click **Yes** if the vault data will not be used again on the same computer.

     A progress dialog will display the progress of uninstalling Meridian.

     The program may prompt for confirmation before removing shared DLLs that can safely be removed. This prompt will only appear for those DLLs that are not in use by any other application.

     In most situations, click **Yes**.

6. Enable the **Don't display this message again** option to prevent the prompt from appearing before deleting other shared DLLs.

   After the process has completed, the program might prompt to restart the computer so that files that are in use can be deleted.

7. Select **Yes, I want to restart my computer now** and click **Finish**.

   The computer restarts and Meridian has been completely removed from the computer.

Licenses

You will not be able to use Meridian until licenses have been correctly registered. For Meridian on-premises deployments, the Accruent License Server service grants and reclaims licenses for all Meridian clients, vault connections, and optional modules on the same local area network. It manages either licenses that are assigned to specific users (named) or floating (concurrent) licenses. Meridian Cloud users are granted subscription licenses that do not require any registration or management by the customer.

- **Concurrent licenses** are granted to users dynamically on a first-come, first-served basis unless licenses have been reserved. Concurrent licenses are released immediately when the client application is closed.
- **Named licenses** are assigned to specific users upon first use. A license remains assigned to the user unless it is re-assigned by a System Administrator.
- **Subscription licenses** are a pool of concurrent users (each with a user pass) that are allowed within the organization's subscription level.

The following topics describe the types of licenses and how to register, authorize, merge, reserve, view, and re-assign licenses.

Concurrent Licenses

Following are the basic Meridian concurrent licenses. Client licenses are assigned on either a first-come, first-served basis or are automatically assigned to specific users (named licenses). For information about how named licenses work, see Named Licenses.

For more information about the features supported by each Meridian license, consult a Accruent sales representative or your Accruent Partner.

Optional Module Licenses

Optional module licenses are claimed whenever a vault is opened in which the optional module is enabled, such as the Asset Management Module, Advanced Project Workflow Module, and so on. Some modules require client licenses, other modules only require server licenses. If the server license of a module is claimed by a client application as the result of opening a vault that uses that module, the license will continue to be claimed even after a different vault is opened in the same client session that doesn't use the module. To release the server license, the client application must be restarted.

For information on the license requirements of a particular module, consult a Accruent sales representative or your AccruentPartner.

Shared Workspace Support server License

The **Shared Workspace Support** server license is required for any Meridian application server that hosts vaults that have folder types defined with the **Can be used as a shared workspace** option enabled. The license is claimed regardless of whether the folder type is actually used or shared workspaces are defined. If the license is absent, the vault cannot be opened by the client applications and documents cannot be opened or saved in the vault from other applications. For information about configuring folder types and shared workspaces, see the *Configure Shared Workspaces* article in the *Meridian Enterprise Configuration Guide*.

Special Licenses

Special licenses are available for use only in development and test environments. The licenses are provided so that such environments can be isolated from computers that are used for production purposes and so that licenses that are needed for production are not claimed by other users. These Not For Production licenses have product codes that include the letters NFP, for example, 010.MN-PUR**NFP**I001.

Special ways that these licenses behave as opposed to production licenses are that they:

- Do not expire.
- Do not need to be authorized by Accruent. The licenses are available immediately after registering in the Accruent License Server.
- Display a message when they are used.
- Cannot be registered together with production licenses on the same Accruent License Server.

Named Licenses

Named licenses work the same as concurrent licenses as described in Concurrent Licenses with the following exceptions:

- Named licenses cannot be mixed with concurrent licenses for the same license type.
- Each license type can be assigned to a different Microsoft Active Directory group as described in Reserve Licenses.
- When named licenses are registered, an encrypted cache file (`AM-Meridian.clic`) is created in the program folder and updated frequently. If this file is deleted, renamed, or restored from backup, the license manager service will not start and the licenses must be re-registered and re-authorized.
- Named licenses are assigned to specific users upon first use.
- Named licenses that have not been used for a period of 30 days can be re-assigned to a different user as described in Reassign Named Licenses - Administrator.
- Separate license servers cannot pool named licenses. If a user opens vaults on separate servers that connect to separate license servers, that user will claim a named license from each license server.
- All license activity can be logged for troubleshooting by setting the **AuditLicenseRequests** registry value as described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server\Licensing. The logged data can be viewed in the Windows **Application** event log.
- Special licenses are available for use only in development and test environments. The licenses are provided so that such environments can be isolated from computers that are used for production purposes and so that licenses that are needed for production are not claimed by other users. These Not For Production licenses have product codes that include the letters NFP, for example, 010.MN-PUR**NFP**I001.

  Special ways that these licenses behave as opposed to production licenses are that they:

  - Do not expire.
  - Do not need to be authorized by Accruent. The licenses are available immediately after registering in the Accruent License Server.
  - Display a message when they are used.
  - Cannot be registered together with production licenses on the same Accruent License Server.

Subscription Licenses

Compared to concurrent and named licenses, *subscription licenses* are simpler to understand, more flexible to use, level in cost, and easier to administer.

Subscription licenses have the benefits of both concurrent and named licenses combined in two license Stock Keeping Units (SKUs), the Meridian Enterprise Subscription license and the Meridian User Pass license.

The Meridian Enterprise Subscription licenses are assigned to users upon login to the Meridian system. The Enterprise Subscription license grants access to all Meridian applications and server modules. User Passes are assigned to active named users if SAML authentication or Meridian Portal is used.

For on-premise deployments of Meridian, the Meridian Enterprise Subscription license is the only relevant license. There are two options for deploying your licenses, which can be selected during setup:

1. A Meridian License Tenant

   Enterprise Subscription licenses and User Pass licenses are registered by the License Tenant in the Cloud. The Meridian License Tenant does not require any registration of license keys on the Meridian On-Premises License Server.

2. An On-Premises License Server

   Enterprise Subscription and User Pass licenses are registered on the Meridian Enterprise Server. The license keys are provided by licensing@accruent.com.

Meridian Enterprise Subscription Licenses can be combined with Meridian Cloud Project Licenses. In this scenario, the client always connects to the Meridian Cloud License Tenant.

For specific benefits, requirements, limitations, and prices of subscription licenses, contact a Accruent Partner or Accruent Account Executive.

You do not need to reassign a license for a User Pass. Unlike named licenses, a User Pass automatically becomes available 30 days after use. As your user community changes, new users can access available User Passes without any manual steps.

If you try to reassign a User Pass, the system returns an error.

For more information about the setup, refer to *Install the Server Components* in the *Meridian Enterprise Administrator's Guide*.

You can manually reassign a PAS license once every 30 days after the system automatically releases it due to 30 days of user inactivity (based on the user’s last logoff). The system does not allow manual release of licenses.

Comparison Between Subscription Licensing Options

The following table compares the two subscription licensing options described above.

Comparison between subscription licensing options

Requirement	Cloud License Tenant	On-Premises License Server
Authentication	Azure AD and OAuth 2 compatible authentication.	Windows AD.
Usage limits	Permissive usage is applied. Limited overage is possible, as specified in the license agreement.	The maximum number of subscriptions and user passes is strictly enforced.
License keys	No need to enter registry keys. Entitlements are managed by Accruent in the cloud.	License keys need to be requested from Accruent and entered into the on-premises system.
Internet connection	An internet connection from the machine hosting the Enterprise Server is required. If the connection is not available, users currently logged into a Meridian client can continue to work for 24 hours; however, users cannot log in to a Meridian client.	A local internet connection is required for the Meridian clients.
Multi-site deployment	Licenses can be shared between sites.	Licenses must be allocated to specific sites, unless a DCOM connection between sites is available.

License Usage Example

Consider an example in which your tenancy has 35 Subscription Licenses (SUB) and 50 User Passes (PAS).

Maximum Number of Licenses

This model is similar to Named Licenses if the number of PAS users is 50. In this case, up to 50 users can hold any license for 30 days, but only up to 35 SUB users can work simultaneously.

Users will not be able to access Meridian if one of the licenses gets to its maximum number.

License Release

- If one of the active users has been logged out for more than one hour (SUB timeout), one SUB license is released, and the user can be replaced by another of the 50 PAS users.
- If one of the active users has been logged out for more than 30 days (PAS timeout), one PAS license is released. This user can be replaced by a different new user, who does not have any license yet.

  The group of active users (PAS=50) will be updated with the new user who acquired SUB/PAS Named Licenses, replacing the previous one.

Obtain Licenses and Authorization Keys

Codes for the licenses that you have purchased and authorization keys for those licenses can be downloaded from the Accruent Self Service Center. You receive logon credentials for the site from Accruent after your purchase.

To obtain license keys and authorization keys:

1. Log on to the Accruent Self Service Center.
2. On the **Customers** menu, click **Agreements**.

   The **Agreements** page appears and lists your license agreements.
3. Click the name of the appropriate license agreement.

   The **Agreement Details** page appears.
4. Click **Download License Keys**.

   Your browser downloads a MS Excel file that contains your license keys.
5. Open the file to copy the keys to the clipboard and paste them into the Meridian license server as described in Register Licenses - Administrator and Enter Authorization Keys.

Register Licenses - Administrator

After successfully installing the Meridian Enterprise application server components, you must register licenses before creating or opening any vaults. The default method to register licenses is in the Meridian Enterprise Server Administration Console as described in the *Register Licenses* article in the *Meridian Enterprise Server Administrator's Guide*.

If necessary, licenses may be registered in the Meridian Enterprise Administrator program run on the Meridian application server. The **License Server** branch in the Meridian Enterprise Administrator is hidden by default. To reveal it, set the **NodesMask** registry value as described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMAdmin.

Note:

- Download your license keys from the Accruent Self Service Center as described in Obtain Licenses and Authorization Keys.
- All licenses must be entered at the same time.
- When you purchase additional licenses for Meridian for which you have already authorized licenses, the existing license quantity is combined with the new licenses when you register and authorize the new licenses.

To register licenses in the Meridian Enterprise Administrator:

1. On the Meridian application server, open **Meridian Enterprise Administrator** from the Windows **Start** menu.
2. Click **License Server** in the left pane.

   Property page tabs appear in the right pane.
3. Click the **Licenses** tab.

   If the **Registration Wizard** does not appear automatically, click the **Start Wizard** button. The **Registration Wizard** appears.
4. Type the requested information on each page and click **Next** until the **Transaction Keys** page appears.
5. Copy and paste or type the **Transaction Key** elements from the file that you downloaded from the Accruent Self Service Center and click the **Add** button to register each license.
6. To remove an expired license:
   a. Select the license.
   b. Click **Delete**.
7. Accept the default value for **Site ID/Agreement** or type your license agreement number.
8. Click **Next**.

9. Click **Finish**.
10. Click the **Registration** tab in the right pane.

    The **Registration** page appears listing all of the information that you have typed.
11. Confirm that the information is correct or click **Edit** to reopen the **Registration Wizard** and correct the information.
12. Click the **Save as File** button.

    Save the file to a secure location accessible from a computer where you can send an email message.
13. Open the file from a computer where you can send an email message, scroll to the bottom of the file, and click the hyperlink that corresponds to your geographic region.

    A new email message should appear addressed to Accruent.
14. Attach the file that you saved to the email message.

    Entering additional information is optional.
15. Send the message.

    The licenses are now registered but not yet authorized. You or your Accruent Partner can expect to retrieve the authorization keys within three business days.

Each time a vault is opened by a Meridian Enterprise client until the licenses are authorized, a reminder dialog that the licenses have not been authorized will appear. The system may be used with full functionality for up to 30 days to allow time for you to obtain the authorization keys from Accruent and register them as described in Enter Authorization Keys.

Enter Authorization Keys

After you have registered your licenses as described in Register Licenses - Administrator and retrieved authorization keys in return, you must enter the keys to authorize the licenses.

The default method to enter authorization keys is in the Meridian Enterprise Server Administration Console as described in the *Register Licenses* article in the *Meridian Enterprise Server Administrator's Guide*. If necessary, keys may be entered in the Meridian Enterprise Administrator program run on the Meridian application server.

The **License Server** branch in the Meridian Enterprise Administrator is hidden by default. To reveal it, set the **NodesMask** registry value as described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMAdmin.

Download your license and authorization keys from the Accruent Self Service Center as described in Obtain Licenses and Authorization Keys.

1. Open **Meridian Enterprise Administrator** from the Windows **Start** menu.
2. Click **License Server** in the left pane.

   Property page tabs appear in the right pane.
3. Click the **Licenses** tab.

   The list of registered licenses appears.
4. Select a license from the list that corresponds to an authorization key that you have received.

   The license's transaction keys appear at the top of the page.
5. Copy and paste or type the corresponding authorization key in **Authorization key** from the file that you downloaded from the Accruent Self Service Center.
6. Click **Add**.

   The authorization key appears in the license list indicating that the license has been authorized.
7. Repeat steps 4–6 for each license.

   When all licenses have been authorized, the license reminder dialog will stop appearing when the vault is opened by a Meridian Enterprise client.

Reserve Licenses

In many situations, certain users should always receive Meridian Enterprise licenses. Because of the first-come, first-served claiming of Meridian licenses, it is possible that a critical user may not receive a license because all available licenses have already been claimed by other users. Meridian allows you to reserve licenses for certain users who always need access to Meridian vaults.

> **Note:**
> The users of reserved licenses must be members of a local or domain user group.

Reserved licenses are configured in the Windows registry of the computer where the Accruent License Server is installed. You specify pairs of user group names and corresponding Meridian Enterprise product codes. The Accruent License Server service will then reserve enough licenses to grant each member of the specified group a license for the specified product code.

To reserve licenses:

1. Open the Windows registry on the license server computer and locate the following key:

   `HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server\Licensing`

2. Create new values as necessary with the names described in the following table.

Reserved license registry values

Value Name	Value
LicMgrRefresh	The DWORD interval (in minutes) to refresh the reserved licenses. We recommend a value of 60 minutes. The maximum value is 24 hours.

Value Name	Value

LicMgrGroup*n*	The names of local or domain user groups to reserve licenses for. You can reserve licenses for multiple groups by creating one key for each group or by entering multiple group names separated by commas. The key names should be numbered from 1 to *n* (**LicMgrGroup1**, **LicMgrGroup2**, and so on). The license server will reserve one license of the product specified by the corresponding key **LicMgrProduct***n* for each member of the specified groups. Each user group should be specified with the format:
	`<DomainName>\<DomainUserGroupName>`
	or
	`<LocalUserGroupName>`
	Note:
	If a domain group is specified, the Accruent License Server service must be run under an account that has permission to query the domain group memberships. By default, the service runs under the local SYSTEM account, which does not have the necessary privilege. For more information on granting the necessary privileges, see Grant Membership Query Access and Grant Domain Privileges With a Service Account.

LicMgrProduct*n*	The product code of the Meridian product for which to reserve licenses. This value can contain multiple entries separated by semicolons. The key names should be numbered from 1 to *n* (**LicMgrProduct1**, **LicMgrProduct2**, and so on). The license server will reserve one license of the specified product for each member of the group specified by the corresponding key **LicMgrGroup***n*.

These registry values are ignored if they do not contain valid values or if valid corresponding keys do not exist for each pair. The license server automatically ensures that only a single license of each type is claimed per user.

The product codes to type for the **LicMgrProduct***n* values are the first six characters of the part number portion of each license transaction key. They can be found on the **Licenses** page of the **License Server** in the Meridian Enterprise Administrator tool or on your license certificate. For example, for database connection licenses with part number M--DBLNFS001-XEE94, the product code is M--DBL.

The following figure illustrates an example of a reserved licenses configuration for Meridian Enterprise (product codes M--DBL, M--PUR).

Name	Type	Data
(Default)	REG_SZ	(value not set)
LicMgrGroup1	REG_SZ	Administrators
LicMgrGroup2	REG_SZ	Engineers
LicMgrProduct1	REG_SZ	M--PUR;M--DBL
LicMgrProduct2	REG_SZ	M--PUR;M--DBL
LicMgrRefresh	REG_DWORD	0x0000003c (60)

In this example, the license server refresh rate is set to 60 minutes. Each member of the user groups **Administrators** and **Engineers** has reserved a client license and a database connection license.

Note:

- Reserved licenses are indicated on the **Users** page of the **License Server** in the Meridian Enterprise Administrator with the text **(Reserved)** following the user's name for whom the license has been claimed, for example, **John Doe (Reserved).**
- Nested groups (for example, domain groups as members of local groups) are not supported for reserving licenses.

Restrict Licenses

In some environments, users should only receive Meridian Enterprise licenses if a user is a member of a specific Active Directory group. Restricted licenses can be configured in the following Windows key on the computer where the Accruent License Server is installed.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server\Licensing

You specify pairs of user group names and corresponding Meridian Enterprise product codes. The Accruent License Server service will then only grant licenses to the members of the specified group for the specified product code. If a user attempts to use one of the specified products but is not a member of the matching group, the user will be denied a license. You may also restrict licenses in the Meridian Enterprise Administrator as described in the following task.

Notes about functionality

- Restricting licenses overrides reserved licenses.

  You can restrict licenses without reserving them and you can reserve licenses without restricted them. But if you want to use both license reservations and license restrictions, the users for which you want to reserve licenses must also be members of groups to which licenses have been restricted. Users without reserved licenses only need to be members of groups to which licenses have been restricted.
- Restricted licenses can also be configured in Meridian Enterprise Server if the **Use Enterprise Server for user management** option is enabled as described in Configure the Connection To Meridian Enterprise Server.
- The available group names are retrieved from the Active Directory server that has been synchronized. This synchronization can be done in two ways:
  - Using the `ADSyncUsers.exe` program as described in Synchronize User Groups With Active Directory.
  - Using the AD Sync tool in the Meridian Enterprise Server Administration Console, as described in *Synchronize Users And Groups From Active Directory* in the *Meridian Enterprise Server Administrator's Guide*.
- Users must be members of a local or domain group.

Administrator Procedures

To restrict licenses:

1. In the Meridian Enterprise Administrator, select **License Server** in the left pane.

   Property page tabs appear in the right pane.
2. Click the **Users** tab.

   The current quantity of each registered license type is shown in the **Licenses** list.
3. Right-click the name of the licenses that you want to restrict and then click **Restrictions**.

   The **License Restrictions** dialog box appears and lists all of the registered licenses. By default, the **Select user group** list is empty until you specify at least one group to which to restrict licenses.
4. Select an existing group from **User group** that has already been assigned product codes.

   If the group you want to select is not listed:

   a. Click **Add**.

      The **Select User Group** dialog box appears.

   b. Type the name of a group in **User group** and press **Enter**.

      The group name appears in the **User group** list.
5. Select the license codes that you want to allow for the specified group.
6. Repeat steps 3-4 for each group to which you want to restrict licenses.
7. Click **OK**.

Enterprise Server Administration Console Procedures

To restrict licenses:

1. In the **System Management** group, click **Settings**.

   The **Application Settings** page appears.
2. In the menu, click **Licenses**.

   The **Licenses** page appears.
3. Click **Restrictions**.

   The **License Restrictions** dialog box appears and lists all of the registered licenses. By default, the **Select user group** list is empty until you specify at least one group to which to restrict licenses.

4. Select an existing group from **Select user group** that has already been assigned product codes.

   If the group you want to select is not listed:

   a. Click **Add group**.

      The **Select User Group** dialog box appears.

   b. Type a search criterion in **Search filter** and press **Enter**.

      The matching groups appear in the **User group** list.

   c. Select a group.

   d. Click **OK**.

      The group appears in the **Select user group** list where you can select it to assign product codes.

5. Select the license codes that you want to allow for the specified group.
6. Repeat steps 3-4 for each group to which you want to restrict licenses.
7. Click **OK**.

View Current License Usage

At times, it can be helpful to know how many users are currently connected to a Meridian Enterprise system:

- When preparing to perform vault or server maintenance
- If performance problems occur
- To forecast future growth needs

The default method to view license usage is in the Meridian Enterprise Server Administration Console as described in the *Manage Licenses* article in the *Meridian Enterprise Server Administrator's Guide*. If necessary, usage may be viewed in the Meridian Enterprise Administrator program run on the Meridian application server. The **License Server** branch in the Meridian Enterprise Administrator is hidden by default. To reveal it, set the **NodesMask** registry value as described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMAdmin.

To view the current license usage:

1. In the Meridian Enterprise Administrator, select **License Server** in the left pane.

   Property page tabs appear in the right pane.
2. Click the **Users** tab.

   The current quantity of each registered license type is shown in the **Licenses** list.
3. Select a license type in the **Licenses** list.

   The names of users currently claiming that license type are shown in the right-hand list.

> **Note:**
> You cannot release claimed licenses or disconnect users from the Meridian application server in the Meridian Enterprise Administrator.
>
> You can also log Meridian license usage with the **AutoManager Licenses** counter in Windows Performance Monitor as described in Configuring the Windows Performance Monitor.

Monitor License Usage

Monitoring license usage over time can be useful to determine:

- Average license usage to gauge whether users are taking advantage of the tools as much as expected.
- Peak total license usage in order to forecast the need for more licenses.
- Usage during different days of the week and hours of the day for troubleshooting performance issues or scheduling maintenance tasks.

See the User Guide in Performance Monitor for information about the more advanced features of Performance Monitor, including:

- Changing how the graph is displayed
- Saving sets of performance counters as data collectors that can be reused
- Scheduling data collection on a periodic basis
- Logging the data to a file that can be sent to Accruent Support or to a database for advanced reporting
- Viewing historical performance reports

Monitor License Usage

To monitor license usage in real time with Performance Monitor:

1. Open Windows Performance Monitor.
2. In the navigation tree, expand **Monitoring Tools**, and then click **Performance Monitor**.

   The **Performance Monitor** graph appears with the default performance counters loaded.
3. In the graph pane toolbar, click **Add** button .

   The **Add Counters** dialog box appears.
4. Click options or type values using the descriptions in the following table.

Performance counter options

Option	Description
Select counters from computer	If you are logged on to the Meridian Enterprise application server, accept the default of **<Local computer>**. If you are logged on to a different computer and want to monitor the licenses of a remote computer, click **Browse** and then select the computer that you want to monitor.
Available counters	Expand **AutoManager Licenses** and select **Licenses in use**.
Instances of selected object	To monitor all installed licenses, select **<All instances>**. To monitor only specific licenses, select them in the list.

5. Click **Add**.

   The selected counters appear in the **Added counters** list.

6. Click **OK**.

   The performance graph refreshes to show the added counters.

Enable License Server Activity Logging

To enable license server activity logging:

1. Set the **AuditLicenseRequests** value described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server\Licensing.
2. To also log events when licenses are reclaimed by the same user, set the **PostEventOnLicenseReclaim** value as described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server\Licensing.
3. Use the Windows Event Viewer to view, filter, and export the license server activity from the **Admin**, **Operational**, and **Debug** channels of the **Accruent-LicenseServer** log in the **Applications and Services Logs** folder.

   To see the **Debug** channel, enable the **Show Analytic and Debug Logs** option be enabled on the **View** menu.

Reassign Named Licenses - Administrator

Named licenses are assigned to specific users when an unassigned license is claimed for the first time. The user will then retain exclusive use of that license until they have not used it for 30 days, at which time the license is released and may be claimed by another user. You may exchange the user of a claimed license and assign it to another user instead of waiting for the 30 days to elapse, such as for an extended absence. Such a license may not be exchanged again for 30 days.

Following is an example scenario:

John claims an unused license on March 1 (effective until the end of May). John takes a leave of absence on March 20. Joe is hired on April 1 and a System Administrator reassigns John's license to Joe. The license is then locked to Joe for 30 days. It cannot be claimed by another user or exchanged by a System Administrator until May 1.

The default method to reassign named licenses is in the Meridian Enterprise Server Administration Console as described the *Reassign Named Licenses* article in the *Meridian Enterprise Server Administrator's Guide*. If necessary, licenses may be reassigned in the Meridian Enterprise Administrator program run on the Meridian application server. The **License Server** branch in the Meridian Enterprise Administrator is hidden by default. To reveal it, set the **NodesMask** registry value as described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMAdmin.

To reassign a named license:

1. In the Meridian Enterprise Administrator, select **License Server** in the left pane.

   Property page tabs appear in the right pane.

2. Click the **Users** tab.

   The current quantity of each registered license type is shown in the **Licenses** list.

3. Select a license type in the **Licenses** list.

   The names of users currently claiming that license type are shown in the right-hand list.

4. Right-click the name of the user who is assigned a license that you want to reassign and then click **Exchange user** on the context menu that appears.

   The **Select user to exchange with <*CurrentUser*>** dialog box appears.

5. Click the name of the user to which you want to assign the license.

   If that user name has multiple accounts assigned to it, select the desired account in the **Accounts** list.

6. Click **Select**.

   The license is assigned to the selected user.

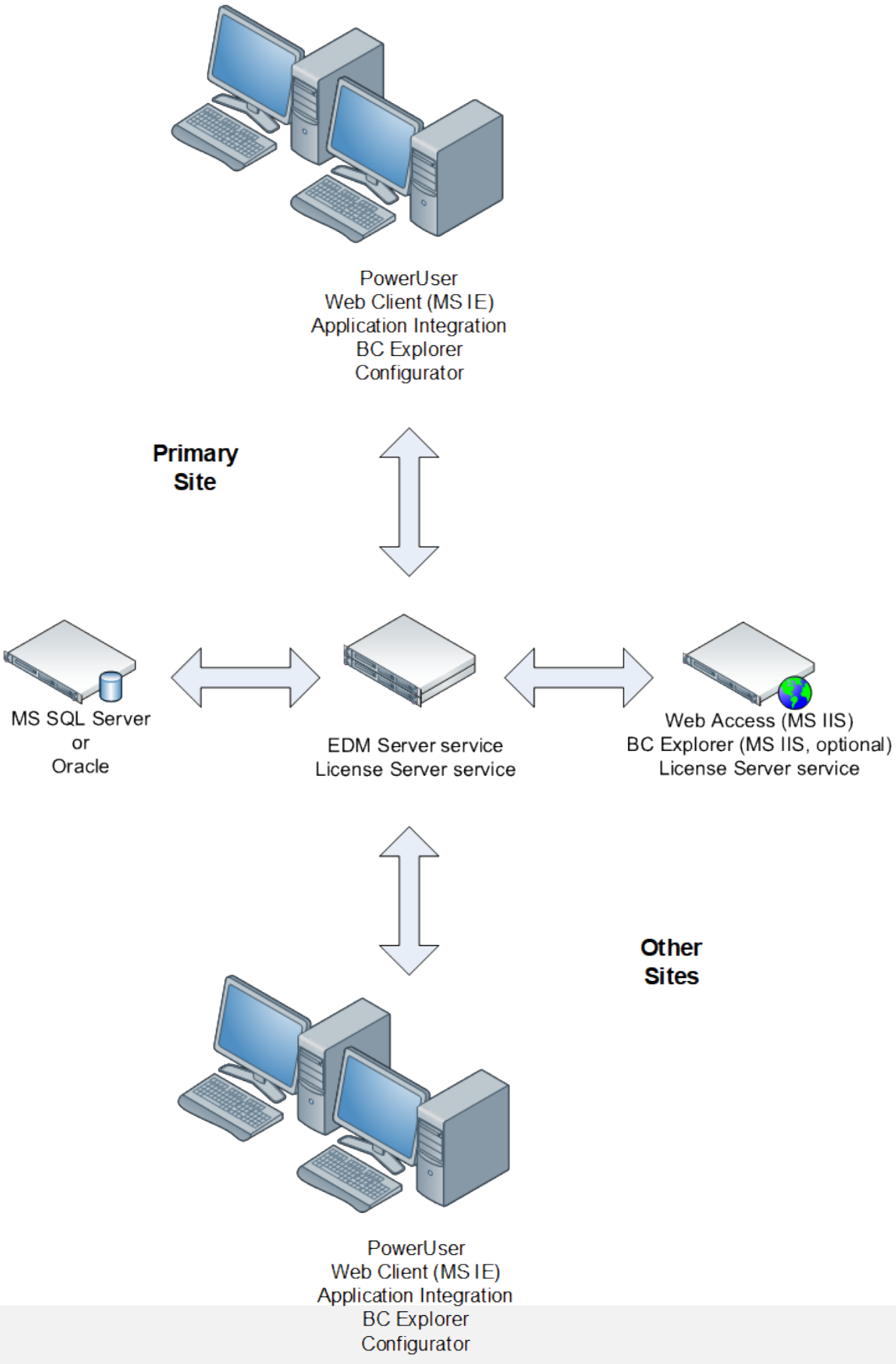
Deploy Multiple License Servers

In the workgroup and department deployment models described in Deployment Models, a single Meridian license server is sufficient for most environments. The license server can be installed either on the Meridian EDM Server computer or on the Meridian Enterprise Server computer at the same site. Enterprise-level deployments, however, often present more complicated environments in which multiple Meridian license servers are necessary. This can be done to ensure that specific types of licenses are available at each site.

The following are approved deployments of multiple license servers.

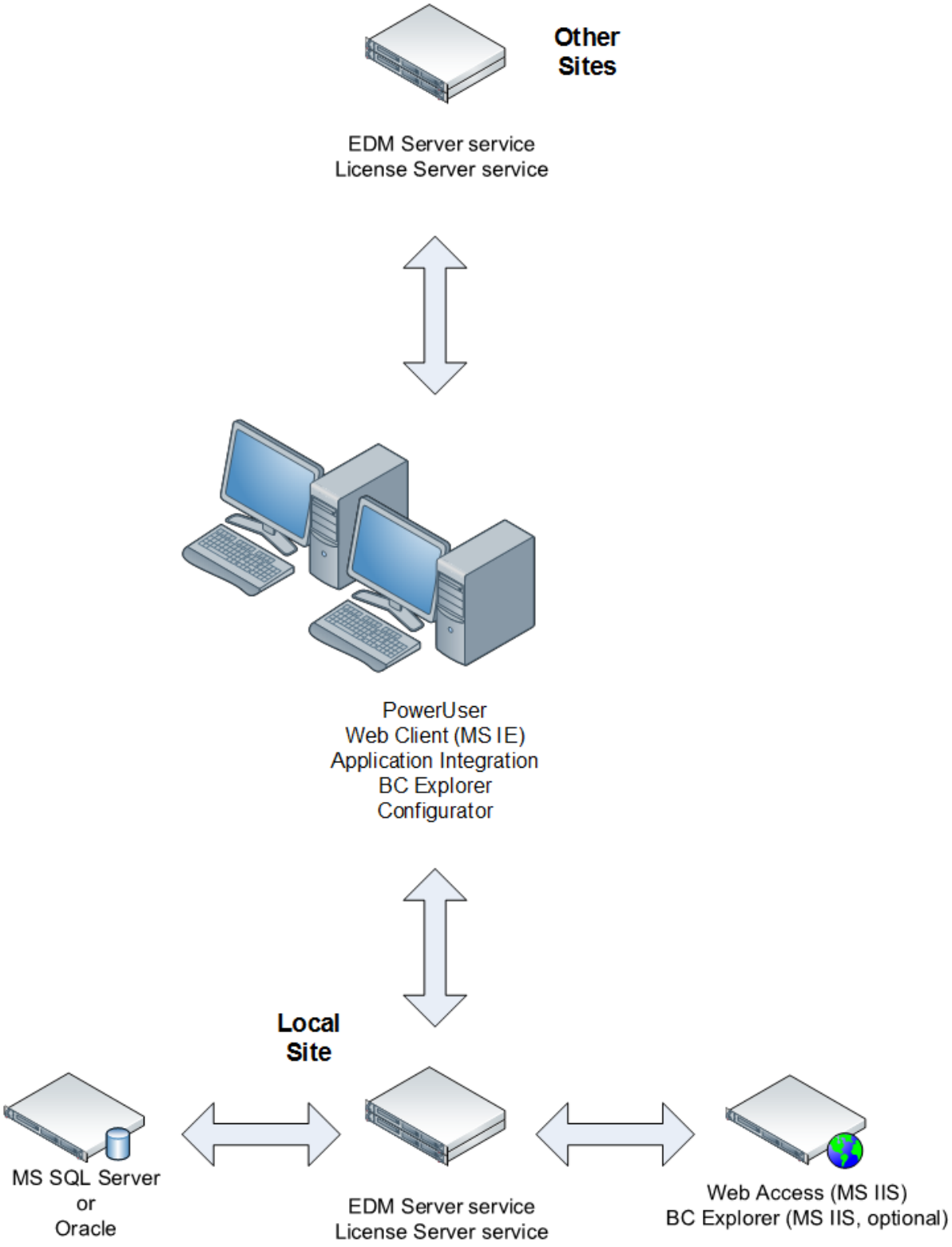
One License Server For All Sites

In this deployment, all users draw from the same set of named or concurrent licenses regardless of the user's location. The license server is installed on a central Meridian Enterprise Server computer in order to maximize the Meridian EDM Server performance. This is the default for all installations. No special configuration is necessary.


PowerUser
Web Client (MS IE)
Application Integration
BC Explorer
Configurator
Primary Site
MS SQL Server
or
Oracle
EDM Server service
License Server service
Web Access (MS IIS)
BC Explorer (MS IIS, optional)
License Server service
Other Sites
PowerUser
Web Client (MS IE)
Application Integration
BC Explorer
Configurator

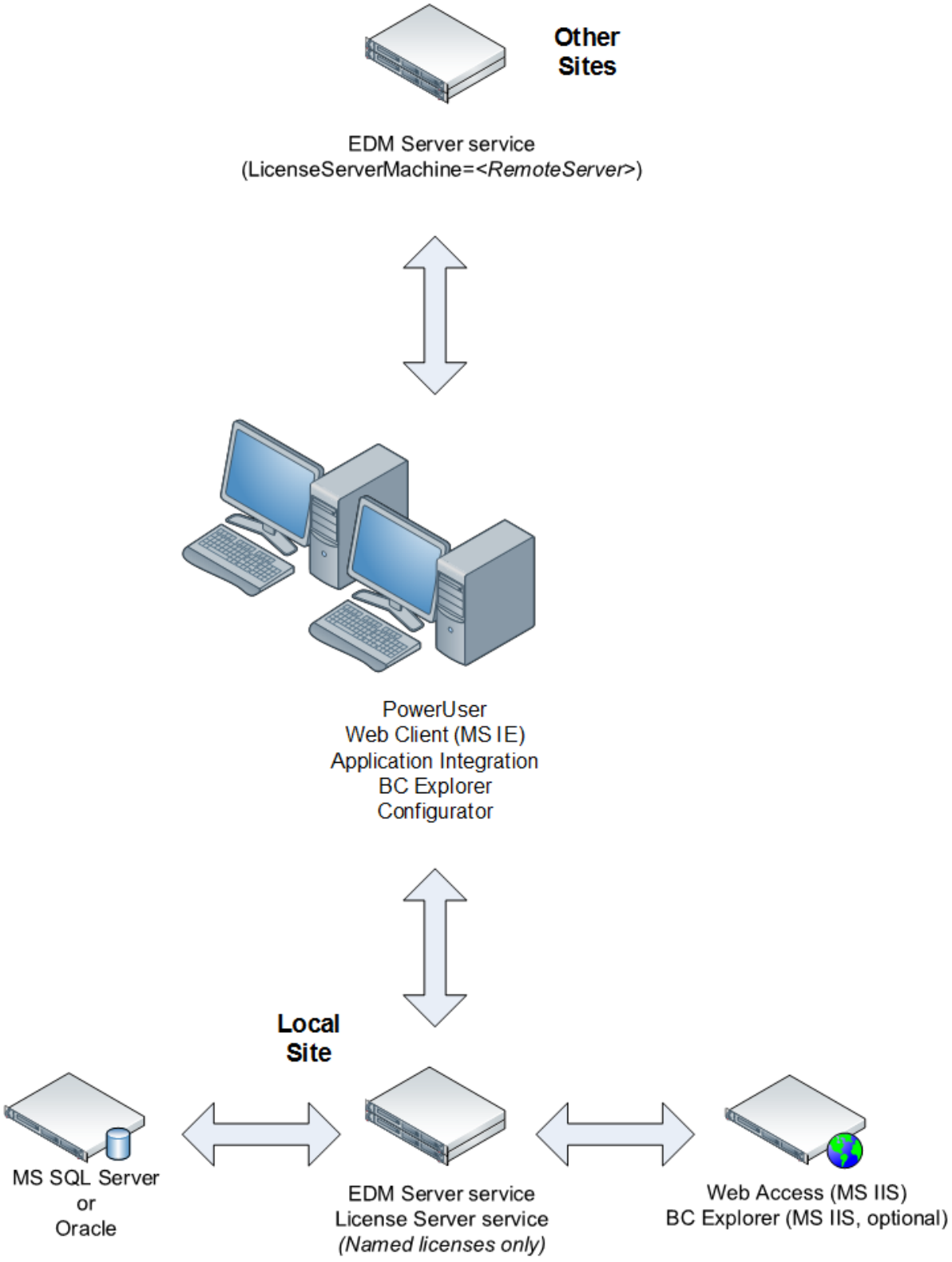
One License Server For Each Site

In this deployment, users draw from a specific set of named or concurrent licenses that are installed on a local license server that is dedicated to the user's location. The license server is installed on a local Meridian EDM Server that hosts the vaults that are used by the users at that location. This is the same as the preceding deployment scenario except that besides the local vaults, the users can also work in vaults hosted at the other sites. When they do so, they draw from the licenses that are installed on the license server at the remote site instead of from their local server.


Other Sites
EDM Server service
License Server service
PowerUser
Web Client (MS IE)
Application Integration
BC Explorer
Configurator
Local Site
MS SQL Server
or
Oracle
EDM Server service
License Server service
Web Access (MS IIS)
BC Explorer (MS IIS, optional)

One License Server For All Sites With Local Edm Servers

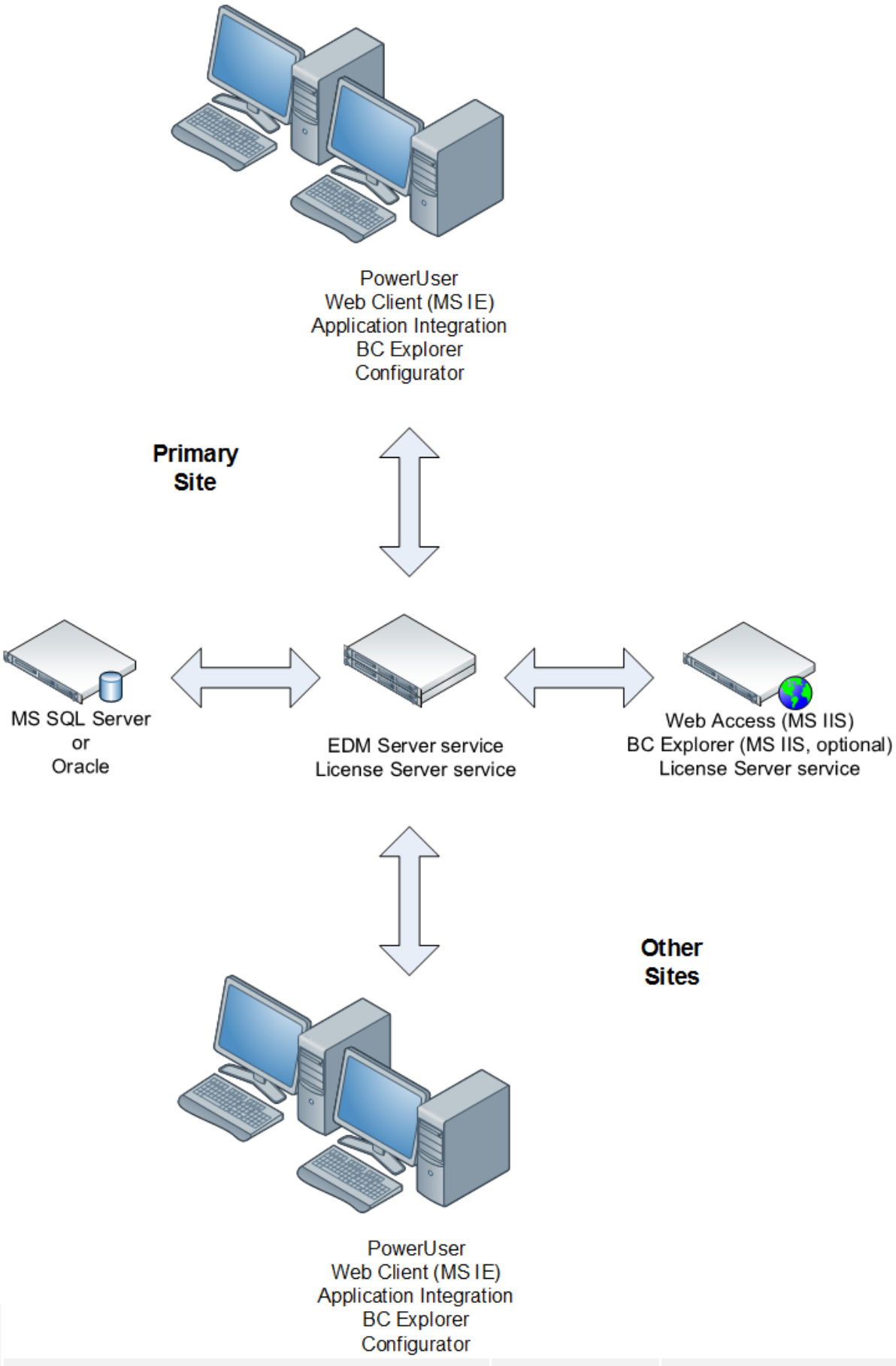
In this deployment, all users draw from a central, shared set of named (not concurrent) licenses regardless of the user's location. The license server is installed on a central Meridian Enterprise Server computer. This can be configured by setting the **LicenseServerMachine** registry setting on each EDM Server to the computer name where the license server is installed. For more information about this setting, see HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server .


Other Sites
EDM Server service
(LicenseServerMachine=<RemoteServer>)
PowerUser
Web Client (MS IE)
Application Integration
BC Explorer
Configurator
Local Site
MS SQL Server
or
Oracle
EDM Server service
License Server service
(Named licenses only)
Web Access (MS IIS)
BC Explorer (MS IIS, optional)

More Than One License Server At the Same Site

The following is NOT an approved or supported deployment of multiple license servers.

Only one license server may be installed at the same site.


PowerUser
Web Client (MS IE)
Application Integration
BC Explorer
Configurator
Primary Site
MS SQL Server
or
Oracle
EDM Server service
License Server service
Web Access (MS IIS)
BC Explorer (MS IIS, optional)
License Server service
Other Sites
PowerUser
Web Client (MS IE)
Application Integration
BC Explorer
Configurator

Create and Maintain Vaults

The Meridian Enterprise database format is invisible to the user. The vault looks and behaves the same no matter whether it uses the Hypertrieve, SQL Server, or Oracle database engines. Meridian allows for multiple active vaults so that, for example, different departments can have their own vaults to store documents. This can be more efficient than using a single large vault because it allows each vault to have different document naming conventions, folder structures, and workflows that may be unique to each department.

By using multiple vaults, each department can retain its own standards and procedures, rather than conforming to a single vault configuration that attempts to meet the needs of all departments. In general, one folder structure (Field-Path definition) applies to each vault. See *Field-Path Definition* in the *Meridian Enterprise Configuration Guide* for information on configuring folder storage structures.

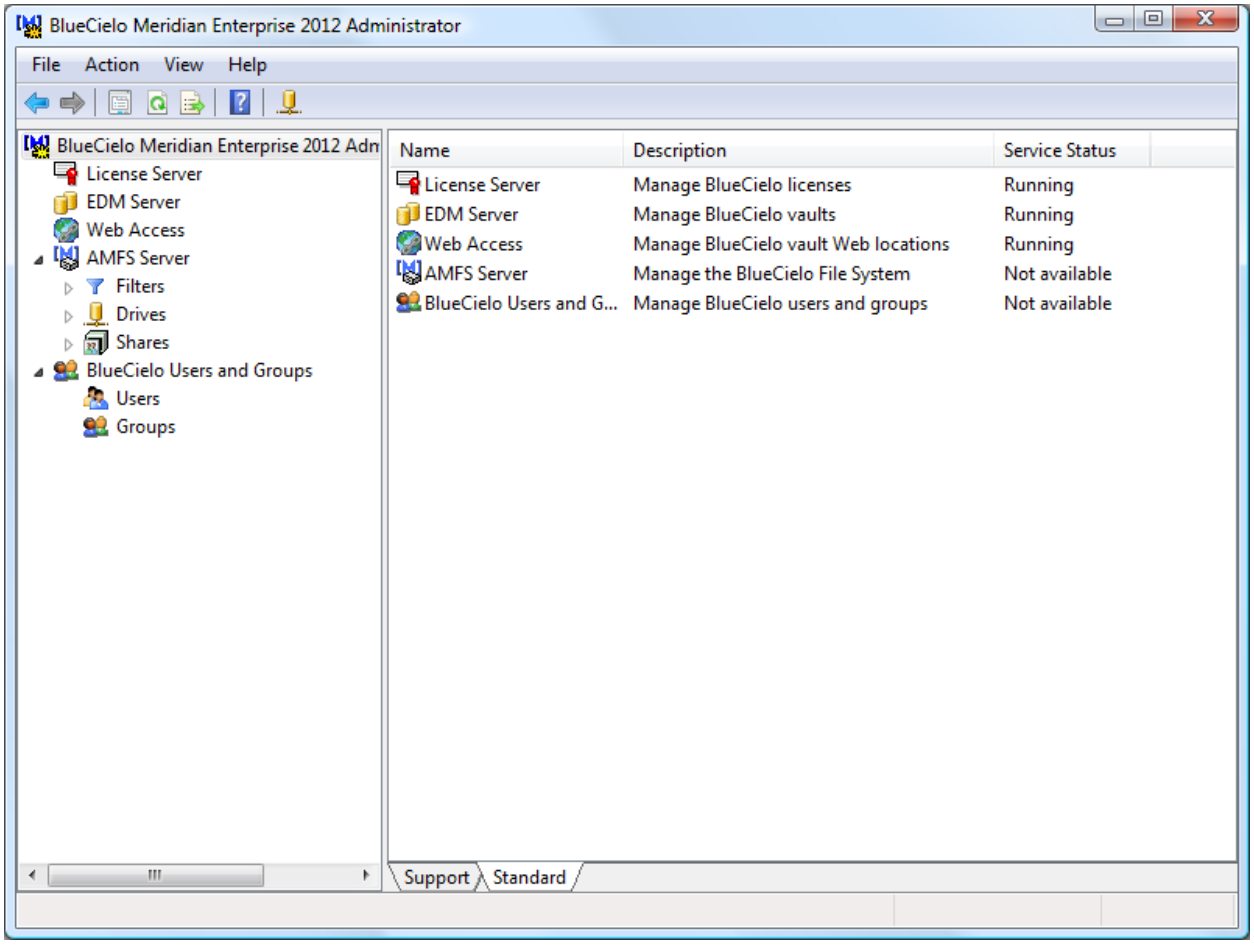
Vaults are created and maintained with the Meridian Enterprise Administrator tool.

Meridian Enterprise Administrator

You use the Meridian Enterprise Administrator tool to manage the various Meridian services described in Meridian Architecture. When you open it from the **Meridian** program group of the Windows **Start** menu, looks similar to the following figure.

Important!

We recommend that access to the administration tools be secured by only installing them (**Administrator** component in the setup packages) on the computers used by authorized System Administrators. For additional server security requirements, see Meridian Server Privileges.



When you select an item in the left pane, its contents appear in the right pane, which you can use to configure the item. The properties of each item can be used to configure additional options. The toolbar displays various buttons depending on the selected item as described in the following topics.

Toolbar Buttons

This topic describes the purpose of the buttons in toolbars you will see in the Meridian Enterprise Administrator tool.

Common Toolbar Buttons

The buttons on the **Common** toolbar are described in the following table.

Common toolbar buttons

Button	Description
	Selects a different computer to manage as described in Administer Meridian Enterprise Remotely.
	Navigates back and forward through previously viewed items, respectively.
	Navigates up one level in the configuration tree.
	Opens the property pages for the selected item.
	Deletes the selected item.
	Refreshes the configuration tree.
	Exports the list shown in the right pane to a text file.
	Shows Help.
	Starts the selected service.
	Stops the selected service.
	Restarts the selected service.

EDM Server Toolbar Buttons

The buttons on the **EDM Server** toolbar are described in the following table.

EDM Server toolbar buttons

Button	Description
	Creates a new vault on the current server as described in Create a New Vault.
	Opens the **Restart After Restore Wizard** described in Restore Backups.
	Opens the **Prepare for Backup Wizard** described in Prepare For Backups.
	Acknowledges the current server time. Enabled only when the server time has gained more than seven days (default) or the value of the **DaysSinceLastOpen** registry key described in Windows Registry Keys.
	Upgrades vaults after a new Meridian version has been installed as described in Upgrade Meridian.
	Opens the **Create Recovery Log Wizard** described in Create a Recovery Log.
	Removes history from the selected vault as described in Remove Vault History.
	Opens the **Vault Archive Wizard** described in Archive Documents.
	Unlocks all documents in the selected vault.
	Opens the selected vault in the Meridian Enterprise Configurator.
	Makes the selected vault the default vault.

PowerWeb Toolbar Buttons

The buttons on the **PowerWeb**toolbar are described in the following table.

PowerWeb toolbar buttons

Button	Description
	Opens the **New Web Location Wizard** described in Create a PowerWeb Location.

Filters Toolbar Buttons

The buttons on the **Filters** toolbar are described in the following table.

Filters toolbar buttons

Button	Description
	Adds a new file extension filter as described in File Filters.
	Tests sample file names with the current file extension filters.

Users Toolbar Buttons

The buttons on the **Users** toolbar are described in the following table.

Users toolbar buttons

Button	Description
	Adds a new Meridian user as described in Create and Edit User Accounts.

Groups Toolbar Buttons

The buttons on the **Groups** toolbar are described in the following table.

Groups toolbar buttons

Button	Description
	Adds a new Meridian user group as described in Create and Edit User Groups.

Hypertrieve Database Engine

The Hypertrieve database engine is a highly efficient, object-oriented database that is developed by Accruent and embedded into Meridian Enterprise. It is optimized for use with Meridian and the **Use HyperCache** option described in Configure Hypercache.

Hypertrieve requires very little system administration and, in fact, has no database management user interface. The data files for a vault stored in Hypertrieve reside in the location specified when the vault was created, `C:\BC-Meridian Vaults` by default. Each of the Hypertrieve files are named *<VaultName>*`.*` where each file extension is described in the following table.

Hypertrieve database engine file types

File Extension	Description
`.csv`	Progress information for a stopped batch import so that the import may be resumed at a later time.
`.hdb`	Main data file. This file is always open when the EDM Server service is running.
`.lck`	Database lock file. This file is always present when the `.hdb` file is open by the EDM Server service.
`.log`	Transaction log file. This file accumulates document property changes until one of these events occurs: • The log file reaches the size specified by the **Maximum log size** option • A Prepare for Backup operation is executed • The EDM Server service is stopped When one of these events occurs, the contents of the log file are committed to the `.hdb` file, a new snapshot is generated and an empty log file is initialized.
`.snp`	The last snapshot file created either by the **Minimum snapshot interval** option or a Prepare for Backup operation.

Create a New Vault

A *vault* is a repository for related documents and their metadata within Meridian Enterprise. A vault consists of a database that contains the document metadata and a file system folder structure that contains the document files. These files are called *stream* files.

Stream files include all document revisions, thumbnails, renditions, and redlines. The vault database contains all document metadata (properties), vault configuration settings (Navigation views, document types, workflow definitions, and so on), and templates.

A vault can be configured with the Meridian Enterprise Configurator to meet the requirements of a single product, project, workgroup, department, or the entire enterprise. For more information on vault configuration, see *Configure Vault Settings* in the *Meridian Enterprise Configuration Guide*.

Before it can be configured, the vault must be created. After the vault has been created, the Meridian Enterprise Administrator tool can be used to create, run, and schedule essential maintenance tasks.

Each Meridian application server can have any number of vaults, limited only by the server computer hardware. However, only up to 63 vaults may be open at one time. Which vaults may be opened is not configurable, so we recommend that you create no more than 63 vaults.

Notes for using an Oracle database for your vault

Review the following information if you plan to use a Oracle database for your vault.

- Unlike the Hypertrieve and SQL Server database engines, the Oracle database engine requires that an Oracle *instance* already exist before a vault can be created. An existing instance can be used but we recommend that you can create a new instance dedicated to Meridian. Use the Oracle Database Configuration Assistant to create a new instance according to your preferences. Meridian functionality and performance is independent of most instance initialization parameters. If multiple vaults will be hosted by Oracle, we recommend that you create a separate instance for each vault. This is to limit the Oracle database size in the event that vaults are deleted or when the **Vault Consistency Wizard** is used.
- We recommend that you use only eight characters for the name of an Oracle vault. The reason is that the Oracle table representing the vault only uses the first eight characters of the vault name, and if the difference between different vault names occurs after the first eight characters, then the vaults will appear to have the same name.

- After you create an Oracle instance, the EDM Server service account needs to be created in the database using DBA Studio or SQL Plus. The account name must be MERIDIAN (upper case) and the initial password must be MANAGER (upper case) in order to create the first vault. For information on the requirements for this account, see EDM Server Service Account Requirements For Oracle. You can change the EDM Server service to use a different account later as described in Configure the Oracle Account Used By Meridian.

Procedures

To create a new vault:

1. In the Meridian Enterprise Administrator, click **EDM Server** in the left pane.

   The active vaults are listed in the right pane.

2. Click **Next**.

   The **Vault Name and Database Engine Type** page appears.

3. Type a name for the new vault.

   Do not use spaces in the name.

4. Make a selection from **Database engine**.

   The available database engine types are those that were selected when Meridian was installed on the server and that have registered licenses.

   For Meridian, the supported database engines are Hypertrieve, SQL Server, and Oracle. Additional choices among the database engine types may be present for backward compatibility. For more information about each engine type, see Hypertrieve Database Engine, How Meridian Works With SQL Server, and How Meridian Works With Oracle.

5. Click **Next**.

   The **How to Initialize the Vault** page appears.

6. Click options or type values using the descriptions in the following table.

Vault initialization options

Option	Description
Create empty vault	Creates an empty vault containing no documents or configuration information. Select this option if you will be importing an existing vault configuration file or will configure the vault manually. For more information on configuring an empty vault, see *Configure Vault Settings* in the *Meridian Enterprise Configuration Guide*.

Option	Description
Maintain history	Retains all revisions of documents. Otherwise, only the latest revision will reside in the vault. This option uses more disk space. To remove unused revisions, they can be archived as described in Archive Documents or removed as described in Remove Vault History.
Import contents of another vault	Imports the documents and configuration settings from an existing vault into the new vault. Select this option if you want to create a replica of an existing vault for testing, development, or similar purposes. **Note:** • This option cannot be used to import a vault from an earlier version. The recommended workaround is described in Move a Vault. • After the vault has been created, restart the Accruent EDM Server service to load the contents into HyperCache.
Source vault	Select the source vault to import into the new vault. To exclude specific properties from the source vault, see Exclude Existing Property Values When Importing a Vault.
Copy stream files	Copies the document files of the source vault to the new vault. This makes the new vault an independent replica of the source vault. Be sure adequate free disk space exists to duplicate all of the source vault's files.
Use existing stream files	Causes the new vault to use the existing document files of the source vault instead of copies. This makes the source vault and the new vault both dependent on the same document files. Select this option only if the source vault will be abandoned. Do not select this option if the source vault will continue to be used. Otherwise, revision conflicts will occur between revisions made in both vaults.

7. Click **Next**.
8. If the **Create empty vault** option is enabled, click options or type values using the descriptions in the following table.

   Otherwise, skip to step 9.

Configuration import options

Option	Description
Do not import configuration data into the new vault	Select this option to leave the configuration of the new vault empty so that you can begin manual configuration.

Option	Description
Import configuration data from a template	Imports an existing vault configuration (.MET) file during vault creation. Vault configuration files are exported from the Meridian Enterprise Configurator as described in the *Export Configuration Data* sub-procedures in the *Meridian Enterprise Configurator* article in the *Meridian Enterprise Configuration Guide*.
Path to configuration file	Type the path to an existing vault configuration file or click **Browse** and select a file.

9. Click **Next**.

   The **Configure Database Engine** page appears.

10. Click options or type values using the descriptions in the following table.

Database engine options

Option	Description
Path for database files	This option appears only if the HyperTrieve database engine is selected. Type a path where the files created by the database engine should be stored or click **Browse** and select a folder. This location must have adequate free space for all of the metadata that will be created during the import, plus future growth. For guidelines on estimating the space required and location options, see Document Storage Space Requirements.
Computer running SQL Server, **OR** Instance of Oracle server	These options appear only if the SQL Server or Oracle database engines were selected in step 4. Type the name of the SQL Server computer or Oracle instance. If this is the same computer as the Meridian application server, leave this option blank. The database files will be controlled by the selected database engine. For more information on using a separate database server, see Deployment Strategies.

Option	Description
Path for content (stream) files	Type a path where the files created by the database engine should be stored, or click **Browse** and select a folder. This location must have adequate free space for all of the document files that will be created during the import and their future revisions, plus space for future growth. For guidelines on estimating the space required and location options, see Document Storage Space Requirements. The content (stream) files may be located on a separate file server or network storage device by specifying a UNC path. For more information on using a separate storage location, see Deployment Strategies. **Note:** If content indexing will be enabled for the vault, storing content files at a UNC location requires that the indexing service reside on the Meridian Enterprise application server and a registry value modified as described in Configure Content Indexing.
Location for EDM server local files	Type a path on the local computer where temporary and backup files created by the database engine should be stored, or click **Browse** and select a folder.

11. Click **Next**.

    The next **Configure Database Engine** page appears. If the SQL Server or Oracle database engines were selected in step 4, a page appears listing additional database engine options.

    Click options or type values using the descriptions in the following table. Otherwise, skip to step 12.

Database file options

Option	Description
Path for database files	Type an existing path where the data files created by the database engine should be stored. If a remote SQL Server instance is specified in **Computer running SQL Server**, type the path on the remote server. If the database is hosted on the local computer, click **Browse** and select a folder. This location must have adequate free space for all of the metadata that will be created during the import, plus future growth. For guidelines on estimating the space required and location options, see Document Storage Space Requirements. For additional folder requirements, see Integrate With a Separate SQL Server Computer.

Option	Description
Path for index files	Type an existing path where the index files created by the database engine should be stored. If a remote SQL Server instance is specified in **Computer running SQL Server**, type the path on the remote server. If the database is hosted on the local computer, click **Browse** and select a folder. This location must have adequate free space for all of the index data that will be created during the import, plus future growth. For guidelines on estimating the space required and location options, see Document Storage Space Requirements.
Path for log files	Type an existing path where the transaction log files created by the database engine should be stored. If a remote SQL Server instance is specified in **Computer running SQL Server**, type the path on the remote server. If the database is hosted on the local computer, click **Browse** and select a folder. This location must have adequate free space for all of the log files that will be created during the import plus space for future growth. For guidelines on estimating the space required and location options, see Document Storage Space Requirements.
Database exists	Enable this option if the SQL Server database to store this vault's data already exists as described in Create the Vault Database Manually.
Disk configuration scenario	Select the option that best describes the database server that will be used by this vault, which will enable the corresponding path options on this page.

12. Click **Next**.

    The next **Configure Database Engine** page appears.

13. Select database cache size values using the descriptions in the following table.

    These settings can be adjusted later. For more information on optimizing vault performance, see Optimize Performance.

Database cache options

Option	Description
Relative cache size	Type a percentage of the total database size that should be held in cache memory. Larger numbers generally result in better performance. This setting will ensure that an optimum amount of data is cached as the vault grows over time.
Maximum cache size	Type the maximum amount of cache memory to be allocated to this vault. This setting limits the size of the vault cache so that it does not consume too much of the server's memory.

Option	Description
Use HyperCache	Enables (default) HyperCache configuration as described in Hypercache.

14. Click **Next**.

    If the SQL Server or Oracle database engines were selected in step 4, skip to step 15.

15. Select database configuration settings using the descriptions in the following table.

Hypertrieve database options

Option	Description
Maximum size of the database log	Accept the default unless an existing vault will be imported, in which case type a larger value or increase the value of **Minimum time between snapshots** so that snapshots are not performed during the import, which can delay import completion.
Minimum time between snapshots (minutes)	Accept the default or type a larger interval so that snapshots are not performed during large imports or during production hours, if necessary.

16. Click **Next**.

    The next **Completing the New Vault Wizard** page appears.

17. Confirm the settings that are shown and click **Finish** to begin vault creation.

    Depending on the options selected, vault creation can take several minutes or many hours.

18. If the SQL Server database engine was selected in step 4, continue with the task described in Integrate With a Separate SQL Server Computer.

Troubleshooting

If the synchronization between Meridian and Meridian Explorer fails inconsistently:

1. Check the SQL logs.
2. If an error is found, take corrective action such as increase the temporary database size.
3. Restart the **EDM Server**.
4. Restart **Meridian Enterprise Server**.
5. Retry the synchronization.

Exclude Existing Property Values When Importing a Vault

When creating a new vault in order to migrate data from an existing vault, you have the option to exclude unwanted property values from the new vault. This is possible not only for released or in-progress documents, but also for previous releases or deleted documents. The task that follows will remove the property values completely, even in history.

> **Note:**
> This task does not prevent the property definition itself from being imported into the new vault. The property definition will exist in the vault but the imported documents will not have any values for the excluded properties. It is not possible to remove a used property definition. To remove the unused property definition, delete it as described in *Create And Edit Custom Properties* in the *Meridian Enterprise Configuration Guide*.

To exclude property values during import:

1. Create a new text file and give it a descriptive name (for example, `ImportFilter.ini`).

   This file should contain the following information:

   - A section named **[Generic]**.
   - Under the **[Generic]** section, a setting named **Vault** equal to the name of the vault to import (for example, **Vault=EDM**).
   - Optional: Under the **[Generic]** section, create settings as necessary using the descriptions in the following table.
   - For each property set in the source vault for which you want to exclude property values, create a section in the file with the internal name of that property set (for example, **[Custom]**).
   - For each property set section, create a setting for each property that you want to exclude and set it equal to **1** (for example, **ChangeManagementDateCompleted=1**). Omit properties that you want to include in the import to the new vault.

2. Add a string type value named **ImportFilterFile** to the registry of the Meridian application server under the following key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
   Meridian\CurrentVersion\OML
   ```

   This value should contain the path and name of the import filter file that you created in step 1.

3. Using the Administrator tool, create a new vault using the existing vault as input as described in Create a New Vault.

   After the import, the new vault will not contain the property values specified in the import filter.

Optional filter file settings

Option	Description
NoHistory	When this setting has a value of **1**, no history will be imported to the new vault. Omit this setting if you want to import all prior revisions of documents.
NoSequences	When this setting has a value of **1**, no sequence numbers will be imported to the new vault. Sequence numbers are often used for programmatically calculating object names such as documents. Omit this setting to import the current values of all sequence numbers so that new objects in the new vault continue the sequences begun in the old vault.
SplitImportFrom	When this setting has a value of **1**, the source file path is split into a path and a file name and stored in the **AMFSObjectPropertySet._IMPORTEDFROMPATH** and **AMFSObjectPropertySet._IMPORTEDFROM** properties, respectively. **Note:** The **AMFSObjectPropertySet._IMPORTEDFROM** property value can also be configured with the server and client **UseImportedFrom** registry values described elsewhere in this document.

Following is an example `.ini` file:

```
[Generic]
Vault=EDM
NoHistory=0
NoSequences=1
SplitImportFrom=1

[Custom]
ChangeManagementDateCompleted=1
ChangeManagementDateEntered=1
ChangeManagementEnteredBy=1
ChangeManagementPriority=1
ChangeManagementRemarks=1
ChangeManagementRequestType=1
ChangeManagementStatus=1
ChangeManagementWeekDue=1
```

View and Edit Vault Properties

After you create a vault, you can later view and edit the options that you set during creation as well as others. You might want to do this to:

- Optimize its performance
- Reconfigure its database file locations
- Configure it for offline mode use
- Change history retention
- Adjust client options

To view or edit a vault's properties:

1. In the Meridian Enterprise Administrator, click **EDM Server** in the left pane.

   The active vaults are listed in the right pane.
2. Select the vault in the right pane for which you want to view or edit its properties.
3. On the **Action** menu, select **Properties**.

   The vault's **Properties** dialog box appears. Many of the options that are accessible from this dialog are the options that were set when the vault was created.
4. Click options or type values using the descriptions in the following table.

Vault configuration options

Option	Description
Name	Internal name of the vault. Read-only.
Display name	Name of the vault as seen by users. Read-only. For information on renaming a vault, see Rename a Vault.
Engine	Name of the database engine for the current vault. Read-only.
SQL Server	Name of the instance of SQL Server where this vault's database is hosted. Available only if the vault was created with the SQL Server engine. If the instance is hosted on the same computer as the Meridian application server, this option is blank. Read-only.
Account	SQL Server account name used to connect to the vault database on the server specified in SQL Server. Available only if the vault was created with the SQL Server engine. For information about setting this option and its password, see Configure the SQL Server Account Used By Meridian.

Option	Description
Database path	Path of vault database files. Read-only. For information about moving a vault, see Move a Vault.
Index path	Path where the index files created by the database engine are stored. Available only if the vault was created with the SQL Server engine. For guidelines on estimating the space required and location options, see Document Storage Space Requirements.
Log path	Path where the transaction log files created by the database engine are stored. Available only if the vault was created with the SQL Server engine. For guidelines on estimating the space required and location options, see Document Storage Space Requirements.
Content path	Path of vault content files. Read-only. For information about moving a vault, see Move a Vault.
Backup path	Path where the backup files created by the SQL Server and Oracle database engines are stored. For guidelines on estimating the space required and location options, see Document Storage Space Requirements.
Maintain history	Retains all revisions of documents. Otherwise, only the latest revision will reside in the vault. This option uses more disk space. To remove unused revisions, they can be archived as described in Archive Documents or removed as described in Remove Vault History.
Hide documents from users with insufficient privileges	Controls the visibility of documents depending on the user's security privileges. Enabling this option will have a negative effect on server performance when displaying folder contents, evaluating security, and searches. **Note:** The user may still see the presence of the vault and open it but they will not be able to see any documents. To hide the vault completely from vault selection dialog boxes, enable the **Hide vaults to which a user has no access** option of the EDM Server and do not grant the user the **List Content** privilege for the root folder of the vault. This is supported for environments with one EDM Server and one web server. Multiple EDM Servers in the same environment will produce unexpected results and this option should not be used in that case.
Force clients to access documents from Local Workspace	Controls the use of Local Workspace. For more information, see Local Workspace.

5. Click the **Advanced** button to view or edit the vault's performance options as described in Optimize Vault Performance.

6. Click the **Status** button to view the current status of the prerequisites for working with the vault in Offline mode as described in *Offline Mode And Remote Mode* in the *Meridian Enterprise User's Guide*.
7. Click the **Content Indexing** tab to view or edit the vault's content indexing options as described in Content Indexing.
8. Click the **Advanced Features** tab to view or edit the vault's additional options described in the following table.
9. Click **OK**.

Extensibility options

Option	Description
Audit table connection string	Connection to an external database where vault audit trail data is stored by the Meridian FDA Module. Type a valid connection string to an existing OLE DB database or click the hyperlink and build one with the **Data Link Properties** dialog that appears. For information about creating a connection string, see Data Connections, Data Sources, and Connection Strings (SSRS) on Microsoft TechNet. Enabling this option requires a Meridian FDA Module server license. For more information about this setting, see Configure the Audit Log Connection. To use Meridian Enterprise Server for the audit trail, type the server name, IP port number, domain name, and account name using the following syntax. By default, the account that is used for the connection is specified during installation as described in Install the Server Components. To use a different account, specify it with *<DomainName>\<AccountName>* as shown. *<ServerName>:<PortNumber>@<DomainName>\<AccountName>* This should be the same address as specified for the **Address** option described in Configure the Connection To Meridian Enterprise Server.

Option	Description
Notifications table connection string	Connection to an existing external database where document subscription data is stored. Type a valid connection string to an existing OLE DB database or click the hyperlink and build one with the **Data Link Properties** dialog that appears. For information about creating this database, see Create a Subscriptions Database. For information about creating a connection string, see Data Connections, Data Sources, and Connection Strings (SSRS) on Microsoft TechNet. For information about configuring notification definitions to use this database, see the *Configure Event Notifications* article in the *Meridian Enterprise Configuration Guide*. **Note:** This table is not used to store notification message information, only subscription data. The design assumption is that most customers will use both notifications and subscriptions. If you only want to use notifications, you must still enter a text value for this option. The value does not need to be a valid connection string. Notifications are enabled only if this option is not empty.
Enable Advanced Project Workflow Module	Enables the features of the Meridian **Advanced Project Workflow** module. Enabling this option requires a Meridian **Advanced Project Workflow Server** license and Meridian **Asset Management Module** client extension licenses. This option is required to link Meridian Enterprise projects with Meridian Portal projects.
Enable Asset Management Module	Enables the features of the Meridian Asset Management Module. Use of this module requires Meridian Asset Management Module client extension licenses.
Enable Meridian Publisher extension	Enables the features of Publisher. Requires appropriate Publisher licenses to be registered.
Enable packages support	Enables viewing the packages that have been exported from Meridian Explorer that are related to a document.
Repository Name	Enter the name of the Meridian Explorer repository from which the packages are made. This option is required to enable the **Export Packages** and **Import Packages** pages in PowerWeb when it is integrated with Meridian Portal.
MaximumWorkflowLogSize	The maximum workflow log size for a vault in bytes. By default this value is set to **0**, which means there is no maximum size. You can also configure this setting in your registry keys. If the user performs an action and the log exceeds the maximum configured size, lines are removed from the start of the log until the log is not larger than the maximum size.

Create a Subscriptions Database

The document event subscription feature requires an existing external database in which to store subscription information for each user. By default, Meridian Enterprise does not create this database automatically. If subscriptions will be allowed in the vault, a database must be created by a database administrator. The Meridian application server and the database must meet the requirements described in Meridian Application Server Requirements. Scripts for SQL Server and Oracle are installed by the Meridian Enterprise setup program for your convenience that will create the database and the necessary schema. The scripts must be executed by a user with sufficient rights to perform the actions in the scripts.

Once you have created your subscriptions database, you will need to connect it to your vault using the Notifications table connection string setting.

Important!
If the subscription database already exists, the scripts will delete it first and then recreate it.

SQL Server

To create a subscriptions database in SQL Server:

1. Copy the following script file from the Meridian application server to the SQL Server host computer:

   `C:\Program Files\BC-Meridian\Program\BC Notification\BCNotesDB.sql`

2. On the SQL Server host computer, navigate to the folder where you copied the file in step 1.
3. Run the script using the `sqlcmd` command-line program and one of the following examples:

   Note:
   - We recommend using the database name **<*VaultName*>Subscriptions**.
   - If the database server is running SQL Server Express, SQL Server Small Business, or another edition that creates a default named instance when the software is installed, specify the name of the database server and the SQL Server instance name together, for example, *<ServerName>***\SQLEXPRESS** or *<ServerName>***\MSSMLBIZ**.

   ```
   sqlcmd -S <ServerName> -E -i BCNotesDB.sql -v DatabaseName =
   "<SubscriptionsDatabaseName>"
   ```

   OR

   ```
   sqlcmd -S <ServerName> -U <UserName> -P <Password> -i
   BCNotesDB.sql -v DatabaseName = "<SubscriptionsDatabaseName>"
   ```

Oracle

To create a subscriptions database in Oracle:

1. Copy the following file on the Meridian Enterprise application server to the Oracle host computer:

   ```
   C:\Program Files\BC-Meridian\Program\BC
   Notification\ORACreateTablesNt.sql
   ```

2. On the Oracle host computer, navigate to the folder where you copied the files in step 1.
3. Open SQL *Plus.
4. Run the following command:

   ```
   @ORACreateTablesNt.sql
   ```

Monitor Vault Status

After vaults are created, configured, populated with documents, and put into production use, we recommend that a System Administrator monitor their status on a regular basis, for example, weekly for the first month after a new vault is created and monthly thereafter. Monitoring vault status ensures that the vaults are operating correctly, backed up, and remain free of inconsistencies. Investing a small amount of time in monitoring vault status can help prevent or minimize data loss later.

To monitor vault status:

1. In the Meridian Enterprise Administrator, click **EDM Server** in the left pane.

   The active vaults are listed in the right pane.
2. Review and confirm the values in the **Status** column for each vault.

   They should each contain **Operational**. Other possible values include:

   - **Backup and upgrade required**

     See Prepare For Backups and Upgrade Meridian Vaults.
   - Backup failed
   - **Backup required**

     See Prepare For Backups and Upgrade Meridian Vaults.
   - Newer software version required
   - **Reindex required**

     See Change Operating System Versions.
   - Repair in progress
   - Undefined
   - Upgrade in progress
   - **Upgrade required**

     A vault upgrade is required after the Meridian application server software has been upgraded as described in Upgrade Meridian Vaults

   A vault backup is required if one has not been successfully performed within the last five days (default) as described in Prepare For Backups. You can determine the date of the last successful backup by viewing the modification dates of the files contained in the vault's `Backup` folder. If you have configured a recovery log task to be executed by the Windows Task Scheduler, also check the date of the last recovery log file. If it is the same as the last successful backup, chances are good that both tasks failed for the same reason, typically an expired password for the service account used to run the scheduled tasks.

> **Note:**
> The number of days since the last successful backup before an alert is displayed when the Meridian Enterprise Administrator is opened. This setting can be configured with the **AlertNoBackup** registry value described in Windows Registry Keys.

3. Review and confirm the values in the **Content Indexing** column for each vault.

   The possible values include **Enabled** and **Disabled**. To enable content indexing for a vault, see Content Indexing.

4. On the Meridian application server, open and review the Application event log for vault status messages as described in Review the Application Event Log.

   If the numbers in the vault status messages are not zeros, consider running the **Vault Consistency Wizard** as described in Vault Consistency Toolkit. Also review the log for other warning or error messages originating from any of the Meridian services.

Audit Vault Activity

Meridian Enterprise is capable of logging all actions that have been completed that create, modify, delete, or export data related to any object in the vault using any of the client applications and application links, including Meridian Enterprise Configurator. This feature meets the requirements of Title 21 Part 11 of the U.S. Code of Federal Regulations that applies to the Food and Drug Administration. Once configured for a vault, audit data is logged automatically. No client configuration is required.

Audit data is only logged for standard Meridian Enterprise commands. Custom commands can be audited by adding calls to the **Vault.AuditEvent** method in the vault's VBScript event handlers. The data is stored in a secured database separate from the document metadata. Audit log data is generated automatically in chronological order. Data cannot be imported into the activity database. No user, regardless of their privileges, can modify the audit data. New audit data does not overwrite existing audit data. Audit data is retained for the life of the vault. For a list of the audited actions, see Audited Actions.

Note:

- Releasing documents using VBScript (for example, `Document.ChangeWorkflowState AS_WF_RELEASED, "", ""`) is not logged if the **SDWFEvents** setting is set to **N** (default) in the vault configuration. If such script exists in the vault configuration and the document type workflow events must be prevented, then you must provide custom notification scripting.

  If the document type workflow events do not need to be prevented, set **SDWFEvents** to **Y**. The setting can be found in the **[ScriptEvents]** section of the **Application Integration** tab in the **Environment** branch of the configuration tree in Configurator.
- Electronic signatures made in PowerWeb are only logged if the **Enable PowerWeb client components** option is enabled for that user.

Meridian Enterprise supports one of the following stores for audit data:

- Standalone database that can be viewed by users with the special audit log viewer web application described in this chapter. The data can be viewed, filtered, and exported by authorized users as described in *View And Save the Audit Log* in the *Meridian Enterprise User's Guide*.

  We recommend using this method only if Meridian Enterprise Server is not deployed. Configuring a Meridian Enterprise server to use this method is described in the following topics.

- Meridian Enterprise Server database. We recommend using this method if Meridian Enterprise Server is deployed. Configuring a Meridian Enterprise server to use this method is done with the **Use Enterprise Server for the audit log** option described in Configure the Connection To Meridian Enterprise Server.

Activate audit log in PowerWeb

1. Open Meridian Administrator.
2. Select **Settings**.
3. Select **Use Enterprise Server for audit log**.
4. Configure the audit log database.

Create an Audit Log Database

> **Note:**
> This task is required only if the audit log data must be stored in a standalone external database. It is not required if the audit log data will be stored in Meridian Enterprise Server.

The audit log feature requires an existing external database in which to store the vault event information. By default, the Meridian Enterprise does not create this database automatically. The database must be created by a database administrator. Scripts for SQL Server and Oracle are installed by the Meridian Enterprise setup program for your convenience that will create the database and the necessary schema. The scripts must be run by a user with sufficient rights to perform the actions in the scripts.

- If the subscription database already exists, the scripts will delete it first and then recreate it.
- Depending on the amount of activity in your vaults, the audit log database can grow quite large. If the amount of disk space allowed for the database is restricted, errors can occur and background processes may fail. We highly recommend that you allow unlimited growth of the database with the database management tools and periodically monitor the database size.

Audit log data is stored using the UTC time zone, and is not based on the server time.

SQL Server

To create an audit log database in SQL Server:

1. Copy the following script file from the Meridian Enterprise application server to the SQL Server host computer:

   ```
   C:\Program Files\BC-Meridian\Program\BC Audit\BCAuditTrailDB.sql
   ```

2. On the SQL Server host computer, navigate to the folder where you copied the files in step 1.
3. Run the script using the `sqlcmd` command-line program and one of the following examples:

   ```
   sqlcmd -S <ServerName> -E -i BCAuditTrailDB.sql -v DatabaseName =
   "<AuditDatabaseName>"
   ```

   Or to use different credentials than your own:

   ```
   sqlcmd -S <ServerName> -U <UserName> -P <Password> -i
   BCAuditTrailDB.sql -v DatabaseName = "<AuditDatabaseName>"
   ```

We recommend using the database name **<*VaultName*>AuditLog**.

If the database server is running SQL Server Express, SQL Server Small Business, or another edition that creates a default named instance when the software is installed, specify the name of the database server and the SQL Server instance name together, for example, <*ServerName*>**\SQLEXPRESS** or <*ServerName*>**\MSSMLBIZ**.

Oracle

To create an audit log database in Oracle:

1. Copy the contents of the following folder on the Meridian Enterprise application server to the Oracle host computer:

   ```
   C:\Program Files\BC-Meridian\Program\BC Audit
   ```

2. On the Oracle host computer, navigate to the folder where you copied the files in step 1.
3. Start SQL *Plus.
4. Run the following command:

   ```
   run @ORACreateTables.sql
   ```

Configure the Audit Log Connection

> **Note:**
> This task is required only if the audit log data must be stored in a standalone external database. It is not required if the audit log data will be stored in Meridian Enterprise Server.

Logging audit data requires an available OLE DB database and an OLE DB driver for that database must be installed on the Meridian Enterprise application server. The database does not need to be the same database as where the document metadata is stored.

The audit log table must be created by a database administrator as described in Create an Audit Log Database. You must know a valid connection string for that database or the parameters necessary to build one.

If the **Authenticate logon credentials with the operating system** option is enabled as described in the *Configure Authentication* article in the *Meridian Enterprise Configuration Guide*, Meridian Enterprise versions prior to 2017 SP1 require the **Host** parameter to be set in the connection string. With version 2017 SP1 and later, the **Host** parameter does not need to be specified in the audit log database connection string if the audit log database is located on the same server.

To configure the audit log connection:

1. In the Meridian Enterprise Administrator, click **EDM Server** in the left pane.

   The active vaults are listed in the right pane.
2. Select the vault in the right pane for which you want to configure an audit log database.
3. On the **Action** menu, select **Properties**.

   The vault's **Properties** dialog box appears.
4. Click the **Advanced Features** tab.

   The **Advanced Features** options appear.
5. Click options or type values using the descriptions in the following table.
6. Click **OK**.

Audit log database options

Option	Description
Audit table connection string	Connection to an external database where vault audit trail data is stored by the Meridian FDA Module. Type a valid connection string to an existing OLE DB database or click the hyperlink and build one with the **Data Link Properties** dialog that appears. For information about creating a connection string, see Data Connections, Data Sources, and Connection Strings (SSRS) on Microsoft TechNet. To use Meridian Enterprise Server for the audit trail, type the server name, IP port number, domain name, and account name using the following syntax. By default, the account that is used for the connection is specified during installation as described in Install the Server Components. To use a different account, specify it with *<DomainName>\<AccountName>* as shown. *<ServerName>:<PortNumber>@<DomainName>\<AccountName>* This should be the same address as specified for the **Address** option described in Configure the Connection To Meridian Enterprise Server.

Install the Audit Log Viewer

> **Note:**
> This task is required only if the audit log data must be stored in a standalone external database. It is not required if the audit log data will be stored in Meridian Enterprise Server.

The Meridian audit log is enabled by creating the audit log database as described in Create an Audit Log Database. The database contains information about the actions listed in Audited Actions. The audit log viewer allows users to view the audit log data read-only. The viewer can be configured as described in Configure the Audit Log Viewer.

The audit log viewer is a web application that is installed with the Meridian Enterprise PowerWeb components but the installation must be completed manually on the web server that will run the application. We recommend installing it on the PowerWeb web server.

> **Note:**
> The audit log viewer web application requires Microsoft .NET Framework 4.6 on the web server where the application is hosted. The **Publisher extension** component must have been selected when Meridian Enterprise was installed on the computer.

Installation

To install the audit log viewer:

1. On the web server, in Internet Information Services Manager, in the default website, locate the web application **WebExtensibilityDBViewer**.
2. Disable all authentication types except **Windows Authentication**.
3. Set user permissions to the viewer to meet your organization's requirements.

Test Audit Log Viewer

To test the audit log viewer:

1. Perform one or more of the actions listed in Audited Actions.
2. View the audit log as described in *View And Save the Audit Log* in the *Meridian Enterprise User's Guide*.

   By default, the audit log viewer can only be opened from within Meridian Enterprise. The database connection string, user name, and user privileges are passed in the URL to the web application as encrypted data.

To open the audit log viewer outside of Meridian Enterprise, type a connection string (without the **Provider** keyword) in the **connectionString** attribute of the **AuditDBConnectionString** setting in the **appSettings** section of the `web.config` file of the web application.

Configure the Audit Log Viewer

This task is required only if the audit log data must be stored in a standalone external database. It is not required if the audit log data will be stored in Meridian Enterprise Server.

After the audit log viewer has been installed as described in Install the Audit Log Viewer, some of its features can be configured to meet your requirements:

- Visibility and order of the columns
- Visibility of the viewer header (logo and title), such as hiding it when showing the viewer as an external property page for document types, as described below
- Modify the text of the event descriptions as described in Localize the Audit Log Database

Change Date / Time Format of Viewer

To change the date and time format used in the audit log viewer:

1. Navigate to `C:\inetpub\wwwroot\BCEnterprise\Languages` on your machine.
2. Open **English.xlsx**.
3. Change the date / time formats in the following rows:
    - Row 3 – DateFormat: This value MUST be the same as the ServerDateFormat value.
    - Row 4 – DateTimeFormat: This value MUST be the same as the ServerTimeFormat value.
    - Row 9 – ServerDateFormat
    - Row 10 – ServerTimeFormat

    Refer to the table below for the supported date / time formats.
4. Save your changes.
5. Reset Internet Information Services (IIS).

Date / Time Formats Supported for Audit Log

Category	Input	Output
Date	M/d/yyyy	4/5/2017
Date	M/d/yy	4/5/17
Date	MM/dd/yy	04/05/17

Category	Input	Output
Date	MM/dd/yyyy	04/05/2017
Date	yy/MM/dd	17/04/05
Date	yyyy-MM-dd	2017-04-05
Date	dd-MMM-yy	05-Apr-17
Date	dddd, MMMM d, yyyy	Wednesday, April 5, 2017
Date	MMMM d, yyyy	April 5, 2017
Date	dddd, d MMMM, yyyy	Wednesday, 5 April, 2017
Date	d MMMM, yyyy	5 April, 2017
Time	h:mm tt	9:40 AM
Time	hh:mm tt	09:40 AM
Time	h:mm	9:40
Time	hh:mm	09:40
Time	h:mm:ss tt	9:40:07 AM
Time	hh:mm:ss tt	09:40:07 AM
Time	h:mm:ss	9:40:07
Time	hh:mm:ss	09:40:07

Change Visibility and Order of Columns

To change the visibility and order of the columns:

1. Open the `web.config` configuration file of the audit log viewer in any text editor.

   By default, the file is located in `C:\inetpub\AMM\WebExtensibilityDBViewer`.
2. In the **appSettings** section of the file, modify the values of the settings described in the following table.

Column settings

Setting	Description
AuditTableColumns	Contains **add** elements for each column name. The **key** attribute is the name of the column. Set the **value** attribute to **true** to show the column. Set it to **false** to hide the column. Arrange the order of the **add** elements to change the order of the columns in the viewer.

Hide Viewer Header

To hide the viewer header:

In the URL to show the viewer, set the **HideHeader** parameter to a non-zero number. For example, the following URL will show the audit log viewer without the header:

```
http://localhost/WebExtensibilityDBViewer/AuditView.aspx?MachineName=
MyServer&VaultName=MyVault&HideHeader=1
```

Add an Audit Log Property Page

> **Note:**
> This task is required only if the audit log data must be stored in a standalone external database. It is not required if the audit log data will be stored in Meridian Enterprise Server.

In a standard deployment of the audit log viewer, users can open the report by clicking **View Audit Report** on the **Tools** menu in PowerUser. The viewer opens in a new browser window with all records available and ready for the user to begin filtering or searching. This method is useful if users typically need to check the activity for sets of documents.

The audit log viewer can also be implemented as a document property page to show only the audit records for the current document. This method is useful if users typically need to check the activity for individual documents, not sets of documents.

To add an audit log property page:

1. Confirm that the audit log viewer works correctly in its default configuration.
2. In Meridian Enterprise Configurator, create a new property page that shows an external URL as described in *Create a New Property Page* and *Configure External Pages* in the *Meridian Enterprise Configuration Guide*.
3. Type the following VBScript statement in **Page URL**:

   ```
   "http://<ServerName>
   /WebExtensibilityDBViewer/AuditView.aspx?MachineName=<ServerName>
   &VaultName=<VaultName>&HideHeader=1&ObjectID=" & Document.ID
   ```

   Where *<ServerName>* is the name of your web server and *<VaultName>* is the name of the vault where the documents reside for which you want to view the audit log.

   To show the audit records for all documents, omit the `&ObjectID` parameter and the `Document.ID` property. The page will then show the same records as the **View Audit Report** command.
4. Assign the page to the applicable document types as described in *Apply Property Pages To a Document Type* in the *Meridian Enterprise Configuration Guide*.

   Assign the page as a property page only, not as a wizard page.

Localize the Audit Log Database

> **Note:**
> This task is required only if the audit log data must be stored in a standalone external database. It is not required if the audit log data will be stored in Meridian Enterprise Server.

By default, the Meridian audit log contains vault event descriptions in English. These descriptions will appear in reports and other places where the data is shown. Each description can be localized in the audit log database manually using the database management system tools or it can be more conveniently localized using a separate description file.

Localize Audit Log Database

To localize the audit log database:

1. Open the following description file on the Meridian Enterprise application server in Microsoft Excel:

   `C:\Program Files\BC-Meridian\Program\BC Audit\Audit Actions ENG.xlsx.`

2. Edit the action descriptions in column **B** to meet your requirements and save your changes as a new comma-separated value (CSV) file.
3. Copy the CSV file to the audit log database host computer, whether SQL Server or Oracle.

Load Modified Description File into SQL Server Audit Log Database

To load the modified description file into a SQL Server audit log database:

- On the SQL Server host computer, navigate to the folder where you copied the description file and run the Bulk Copy Program (`BCP.exe`) as in the following example:

  > **Note:**
  > If the modified description file uses the comma character (,) to separate fields instead of the semi-colon character (;), replace the semi-colon in the following example with a comma.

  `BCP Actions in <DescriptionFile>.csv -c -t ; -T -S <ServerName> -d <DatabaseName>`

The program replaces the existing descriptions in the audit log database with your localized descriptions.

Load Modified Description File into Oracle Audit Log Database

To load the modified description file into an Oracle audit log database:

1. Copy the following files from the Meridian Enterprise application server to the folder where you copied the definition file on the Oracle host computer:

   ```
   C:\Program Files\BC-Meridian\Program\BC Audit\Ora_Import_
   Actions.bat
   C:\Program Files\BC-Meridian\Program\BC Audit\Ora_Import_
   Actions.ctl
   ```

2. On the Oracle host computer, run the following command line:

   ```
   Ora_Import_Actions.bat <OracleUser>
   ```

   The program replaces the existing descriptions in the audit log database with your localized descriptions.

Audited Actions

When vault auditing is enabled and the audit log database is correctly configured, the Meridian logs vault activity to the specified table. The table has the structure shown in the following table. The audit data is the same whether it is stored in a standalone database or in the Meridian Enterprise Server database.

Audit Table Structure

The structure of the audit table is listed in the table below.

Audit table structure

Field Name	SQL Data Type
ID	int IDENTITY
Vault	nvarchar(255) NOT NULL
Context	nvarchar(255) NULL
LoginName	nvarchar(255) NOT NULL
UserFullName	nvarchar(255) NULL
Action	nvarchar(255) NOT NULL
ActionArg1	sql_variant NULL
ActionArg2	sql_variant NULL
ActionArg3	sql_variant NULL
ActionDate	datetime DEFAULT UTCNow
ObjectID	uniqueidentifier NULL
ObjectName	nvarchar(255) NULL
ObjectPath	nvarchar(255) NULL
ObjectRevision	nvarchar(255) NULL

Vault Content Actions

> **Note:**
> The values of **Action** for built-in Meridian actions are predefined strings in English. Custom command action strings must be defined by the custom functions.

The vault content actions that the Meridian logs to the audit log database are listed in the following table. The values of the action arguments (for example, **ActionArg1**) depend on the action performed. Custom actions can also be logged with the **Vault.AuditEvent** method described in the *Meridian Enterprise VBScript API Reference Guide*.

Meridian Enterprise vault content actions

Category	Action	ActionArg1	ActionArg2	ActionArg3	Notes
Document	Asset Management Module create reference	Destination document ID (string)	Reference type internal name (string)	Reference ID (string)	
Document	Asset Management Module remove reference	Destination document ID (string)	Reference ID (string)		
Document	CAD link create reference	Destination document ID (string)	Destination document name (string)	Destination document path (string)	
Document	CAD link remove reference	Destination document ID (string)	Destination document name (string)	Destination document path (string)	
Document	CAD link update properties from file				

Category	Action	ActionArg1	ActionArg2	ActionArg3	Notes
Document	CAD link update properties to file				This action is not logged when Application Integration is in Online mode because the property values can still be changed by the user or other software and those changes cannot be logged. Therefore, we recommend that the Invoke action be audited instead to detect potential document property changes. For the MicroStation link in Remote mode, occurs twice for each update.
Document	Change type	New document type name (string)			
Document	Change property	*<PropertySet>*.*<PropertyDef>*	New property value (first 255 characters)	Old property value (first 255 characters)	Changes to memo type properties are only detected for the last 2000 characters.
Document	Change redlines				
Document	Copy				
Document	Copy to Clipboard				

Category	Action	ActionArg1	ActionArg2	ActionArg3	Notes
Document	Create	Document type name (string)	Source file or template (string)		Only supported for vaults that use Local Workspace, not the Accruent File System (AMFS).
Document	Create manual reference	Destination document ID (string)	Reference type internal name		
Document	Cut to Clipboard				
Document	Delete manual reference	Destination document ID (string)	Reference type internal name		
Document	Derive				
Document	Discussion comment added	Comment text (string)	Comment status (**Open** or **Closed**)		
Document	Discussion comment edited	Comment text (string)	Comment status (**Open** or **Closed**)	When a redline is added, **Redline**. When a file is attached, the file name.	
Document	Discussion comment closed		Comment status (**Open** or **Closed**)		
Document	Discussion comment deleted		Comment status (**Open** or **Closed**)		
Document	Drag-and-drop started				This event is not supported by PowerWeb
Document	Download document				This event is supported only by PowerWeb

Category	Action	ActionArg1	ActionArg2	ActionArg3	Notes
Document	Global Collaboration Framework copy to briefcase	**Enlistment** or **Update**	**Transfer Owner** if ownership transferred, otherwise empty	Destination share name (string)	
Document	Global Collaboration Framework import from briefcase	**Enlistment** or **Update**	**Transfer Owner** if ownership transferred, otherwise empty	Source share name (string)	
Document	Import	Document type name (string)	Source file or template (string)		
Document	Import briefcase	Document type name (string)	Source file (string)		
Document	Invoke (open in registered application)	Verb (application) name (string)			
Document	Meridian Asset Management Module create reference	Destination document ID (string)	Reference type internal name (string)	Reference ID (string)	
Document	Meridian Asset Management Module remove reference	Destination document ID (string)	Reference ID (string)		
Document	Move				This action is not possible in PowerWeb but copying and pasting from the Windows Clipboard is logged as a Create event.

Category	Action	ActionArg1	ActionArg2	ActionArg3	Notes
Document	Purge				
Document	Rendition copy to Clipboard				
Document	Rendition started				
Document	Rendition finished	Succeeded or failed	Watermark prior revision		
Document	Rendition attached	Source file path (string)			
Document	Rendition published	Succeeded or failed	Watermark prior revision		
Document	Replace				Only supported for vaults that use Local Workspace, not the Accruent File System (AMFS).
Document	Revision number update	Succeeded or failed			
Document	Print				
Document	Rename				Only supported for vaults that use Local Workspace, not the Accruent File System (AMFS).
Document	Replace content				
Document	Scan	Document type name (string)	Scan file (string)		
Document	Undelete				

Category	Action	ActionArg1	ActionArg2	ActionArg3	Notes
Document	Unlock for others	Name of the user who locked the document (string)			
Document	Upload document				This event is supported only by the PowerWeb
Folder	Assign role	Folder name (string)	Folder ID (string)	Folder path (string)	
Folder	Change type	New folder type name (string)			
Folder	Copy to Clipboard				
Folder	Create	Folder type name (string)			
Folder	Delete				
Folder	Drag-and-drop started				
Folder	Move				
Folder	Purge				
Folder	Remove role	Folder name (string)	Folder ID (string)	Folder path (string)	
Folder	Rename				
Folder	Undelete				
Working Copy/Quick Change	Add to to-do list	To-do list name (string)	Full user name (string)		
Working Copy/Quick Change	Begin draft revision				

Category	Action	ActionArg1	ActionArg2	ActionArg3	Notes
Working Copy/Quick Change	Restore revision	Restored revision number (string)			
Working Copy/Quick Change	Revoke draft revision	Draft reassigned (Boolean)			
Working Copy/Quick Change	Submit draft revision	Draft reassigned (Boolean)			
Document Type Workflow	Change manager	New manager (string)			
Document Type Workflow	Change state	Current state (string)	New state (string)		See the note in Audit Vault Activity.
Document Type Workflow	Change to-do person	New person (string)			
Document Type Workflow	Revoke document				
Workflow Definition	Assign to-do persons	New persons (joined string)			
Workflow Definition	Assign managers	New managers (joined string)			
Workflow Definition	Create new revision				
Workflow Definition	Run transition	Transition name (string)	Workflow name (string)		
Workflow Definition	Migrate	State name (string)	Workflow name (string)		
Workflow Definition	Reroute	State name (string)	Workflow name (string)		

Category	Action	ActionArg1	ActionArg2	ActionArg3	Notes
Hybrid Document	Attach part	Attached document ID (string)	Attached document path (string)		
Hybrid Document	Create part	New part name (string)			
Hybrid Document	Delete part	Part name (string)			
Hybrid Document	Detach part	Detached document ID (string)	Detached document path (string)		
Hybrid Document	Import part	New part name (string)	Source file (string)		
Project Workflow	Assign Managers	New managers (joined string)			
Project Workflow	Run transition	Transition name (string)			
Project Workflow	Reroute	State name (string)			
Project Copy	Confirm Merged with Master				
Project Copy	Confirm Superseded by Master				
Project Copy	Copy to project				
Project Copy	Copy to project and lock				
Project Copy	Discard from project				
Project Copy	Link to Master Document				

Category	Action	ActionArg1	ActionArg2	ActionArg3	Notes
Project Copy	Release as master				
Project Copy	Require Merge				
Project Copy	Transfer to project				
Project Copy	Undo Make Obsolete				
Project Copy	Unlink from Master Document				
Export Package	Status changed	Package name (string)	Package ID (integer)	Previous state name => New state name (string)	
Export Package	Recipient changed	Package name (string)	Package ID (integer)	Previous recipient name => New recipient name (string)	
Export Package	Name changed	Package name (string)	Package ID (integer)	Previous package name => New package name (string)	
Export Package	Job changed	Package name (string)	Package ID (integer)	Previous job name => New job name (string)	
Export Package	Document added	Package name (string)	Package ID (integer)	Document ID & document name (string)	
Export Package	Document removed	Package name (string)	Package ID (integer)	Document ID & document name (string)	
Export Package	Created	Package name (string)	Package ID (integer)		

Category	Action	ActionArg1	ActionArg2	ActionArg3	Notes
Export Package	Deleted	Package name (string)	Package ID (integer)		
Import Package	Create import profile	User comments	Package name (string)		
Import Package	Edit import profile	User comments	Package name (string)		
Import Package	Delete import profile	User comments	Package name (string)		
Import Package	Create package	User comments	Package name (string)		
Import Package	Start package	User comments	Package name (string)	Package status (string)	
Import Package	Import document from package	Import action description	Package name (string)	Package location(string)	
Import Package	Import document from package as new revision	Import action description	Package name (string)	Package location(string)	
Import Package	Change package status	User comments	Package name (string)	Package status (string)	
Import Package	Delete package	User comments	Package name (string)		
Security	Log on attempts	Result			
Security	User assigned to role or removed from role				

Category	Action	ActionArg1	ActionArg2	ActionArg3	Notes
Electronic Signature	Sign document	PowerUser only			The signing of documents from the PowerWeb client is not logged due to technical limitations. We recommend that audit logging of successful signing during workflow transitions from PowerWeb be performed in VBScript on the **DocWorkflowEvent_AfterChangeWFState** event. The implementation should check the transition that is occurring (**TargetState** parameter) and the type of client being used (`Client.Type = "HTML"`).
Briefcase	Checkin	Briefcase name			
Briefcase	Import	Briefcase name			
Briefcase	Lock	Lock ID			
Briefcase	Unlock	Lock ID			
Briefcase	Update	Briefcase file name			

Vault Configuration Actions

The vault configuration actions that Meridian logs to the audit log database are listed in the following table.

Meridian Enterprise vault configuration actions

Action	Information
Commands	Created, changed, or deleted
Configuration data	Imported or exported
Document types	Created, changed, or deleted
Environment	Changed
Event script	Changed
Extensions	Created, changed, or deleted
Field-Path definition	Changed
Folder types	Created, changed, or deleted
Lookup lists	Created, changed, or deleted
Navigation views	Created, changed, or deleted
Opened in Configurator	Opened or opened read-only
Pages	Created, changed, or deleted
Property definitions	Created, changed, or deleted
Property sets	Created, changed, or deleted
Reference types	Created, changed, or deleted
Reports	Created, changed, or deleted
Roles and privileges	Changed
Scopes	Created, changed, or deleted
Tables and queries	Created, changed, or deleted
Work area templates	Created, changed, or deleted
Workflow definitions	Created, changed, or deleted

Meridian Explorer Repository Actions

The repository actions that Meridian Explorer logs to the audit log database are listed in the following table.

Meridian Explorer repository actions

Category	Action	ActionArg1	ActionArg2	ActionArg3
Security & User Management	User logon			
Security & User Management	User logoff			
Security & User Management	Create user			
Security & User Management	Create user group			
Security & User Management	Add user to group			
Security & User Management	Remove user from group			
Security & User Management	Add group to group			
Security & User Management	Remove group from group			
Security & User Management	Update user details			
Security & User Management	Update user group details			
Security & User Management	Delete user			
Security & User Management	Delete user group			
Security & User Management	Update application permissions	Group name	Permissions	
Security & User Management	Create permission level			

Category	Action	ActionArg1	ActionArg2	ActionArg3
Security & User Management	Update permission level			
Security & User Management	Delete permission level			
Security & User Management	Create user role			
Security & User Management	Update user role			
Security & User Management	Delete user role			
Security & User Management	Update security hierarchy	Area	Path	
Security & User Management	Update security profile	Document or ObjectTag	Path	Description
Security & User Management	Clear security profile	Document or ObjectTag	Path	
Document/Tag Project	Open Explorer view	Description	ID	Type
Document/Tag Project	View native file			
Document/Tag Project	View rendition			
Document/Tag Project	Download native file			
Document/Tag Project	Download rendition			
Document/Tag Project	Draft print			
Comment	Add comment	Comment text	Status	Attachment
Comment	Update comment	Comment text	Status	Attachment
Comment	Delete comment			
Configuration	Deploy Explorer views			

Category	Action	ActionArg1	ActionArg2	ActionArg3
Configuration	Create new repository	Type		
Configuration	Take repository offline	Type		
Configuration	Bring repository online	Type		
Configuration	Upgrade repository	Type		
Configuration	Unregister repository	Type		
Configuration	Update global permissions	Permissions	User name	Group name
Configuration	Update user assignments		Assignments	
Configuration	Import repository configuration	File name		
Publishing	Remove pending items	Job name	IDs	
Publishing	Edit synchronization time stamp	Job name	New value	
Publishing	Restart job	Job name		
Publishing	Cancel job	Job name		
Publishing	Create new job	Job name	Source	Destination
Publishing	Edit job	Job name	Source	Destination
Publishing	Enable job	Job name		
Publishing	Disable job	Job name		
Publishing	Delete job	Job name		
Publishing	Create new rendering profile			
Publishing	Edit rendering profile	Name		
Publishing	Delete rendering profile	Name		
Publishing	Import jobs	Names	Filename	

Category	Action	ActionArg1	ActionArg2	ActionArg3
Publishing	Export jobs	Names	Filename	
Collections & Export Package	Create collection		Name	
Collections & Export Package	Delete collection		Name	
Collections & Export Package	Rename collection		Name	Change
Collections & Export Package	Change collection status		Name	Change
Collections & Export Package	Add document to collection		Name	
Collections & Export Package	Remove document from collection		Name	
Collections & Export Package	Add object tag to collection		Name	
Collections & Export Package	Remove object tag from collection		Name	
Package	Convert collection to package		Name	
Package	Create package		Name	
Package	Delete package		Name	
Package	Rename package		Name	Change
Package	Start package		Name	Change
Package	Change package status		Name	Change
Package	Change package recipient		Name	Change
Package	Change package options		Name	Change
Package	Change package destination		Name	Change

Category	Action	ActionArg1	ActionArg2	ActionArg3
Package	Add document to package		Name	
Package	Remove document from package		Name	
Package	Add object tag to package		Name	
Package	Remove object tag from package		Name	
Package	Import document from package	Comment	Name	Path
Package	Import document from package as new document	Comment	Name	Path
Package	Update document from package data	Comment	Name	Path
Package	Import document from package as new revision	Comment	Name	Path
Package	Import document from package as new version	Comment	Name	Path
Package	Create reference for document from package	Comment	Name	Path
Package	Add hybrid part for document from package	Comment	Name	Path
Package	Update thumbnail for document from package	Comment	Name	Path
Package	Create import profile	Comment	Name	
Package	Delete import profile		Name	
Package	Edit import profile		Name	Filename

Category	Action	ActionArg1	ActionArg2	ActionArg3
Package	Import package profile	Profiles	Filename	
Package	Export package profile	Profiles	Filename	

File Filters

Many applications that are used to create vault documents also create temporary or backup files while a document is being edited. For example, AutoCAD creates backup and lock files. These files are typically created in the same folder as the document file unless the application is configured to save them elsewhere. Filters can be defined to prevent creating these files in the vault. If Meridian local workspace is enabled (the default) or a shared workspace folder is configured, the filters prevent the temporary files from being synchronized to the vault. If Meridian local workspace is disabled, the files are redirected to a location on the Meridian application server outside the vault instead. This is done transparently to the application so that file operations occur normally.

> **Note:**
> Even though application temporary files can be filtered out of the vault, better application performance can usually be obtained by configuring the application to store the files in a location on the user's local computer instead, if possible.

Meridian Enterprise defines default filters for the most popular CAD, Office, and Windows temporary file extensions. To exclude other temporary files from being created in a vault, you can define additional filters.

View Current File Filters

To view the current file filters:

- In the Meridian Enterprise Administrator, expand **AMFS Server** in the left pane and select **Filters**.

  The existing file filters are listed in the right pane.

Add New Filter

To add a new filter:

1. From the **Action** menu, point to **New** and select **Filter**.

   The **New Filter** dialog box appears.
2. Type options using the descriptions in the following table.
3. When **Result** reports matches for all of the expected temporary file names that will use the filter, click the **Create** button.

The filter is added to the list of existing filters. Filtered files are stored by default in the folder `C:\BC-Meridian Vaults\<VaultName>\AMFSTEMP`.

File filter options

Option	Description
Mask	Type a file name mask for the files that you want filtered out of the vault. The mask should use wildcard characters for the variable portions of the file name. For example, type an asterisk (*****) to represent any continuous string of variable characters. Type a question mark (**?**) for any single variable character. See the list of existing filters for examples.
Description	Type a description to appear in the **Description** column of the list of existing filters.
Name	Type an example of the file name that you want to exclude from the vault and click the **Run** button to test the mask expression. The result will appear in **Result**.

Change Default Location

To change the default location:

1. In the Meridian Enterprise Administrator, select **AMFS Server** in the left pane.
2. On the **Action** menu, select **Properties**.

   The **AMFS Server Properties** dialog box appears.
3. Choose between two options:
   - Type a different folder path.
   - Browse and select a folder path.
4. Click **OK**.

   The files that reside in this folder can be deleted on a periodic basis if they are not in use. It is safe to assume that any file more than 24 hours old is not in use.

Vault Consistency Toolkit

Certain database inconsistencies may appear over time in a Meridian Enterprise vault. Inconsistencies may also occur when many deletions have been performed after documents have been purged from the vault. Some of these inconsistencies may lead to document content being detached from the database. The Vault Consistency Toolkit is provided to repair these inconsistencies. The Vault Consistency Toolkit consists of the **Vault Consistency Wizard** (VCW) and the **Stream Recovery Wizard**.

The **Vault Consistency Wizard** (VCW) analyzes a vault's database for inconsistencies, can optionally repair any inconsistencies found, and can optionally reclaim storage space used by deleted objects. This process places a high demand for resources on the server and can take a significant amount of time to complete, depending on the size of the database.

The **Stream Recovery Wizard** can recover orphaned document content files after the VCW has been run. The recovered files can then be examined and attached to documents in the vault, imported as new documents, or deleted if they are obsolete.

> **Important!**
> Before running the VCW, perform the preparation steps described in Prepare the Meridian Server and Vault Configuration. Failure to make the preparations will probably cause the VCW to fail.

Prepare the Meridian Server and Vault Configuration

Before running the **Vault Consistency Wizard** (VCW), you must prepare the Meridian application server and the vault for maximum performance and stability. Then you need to perform some database-specific preparation steps. These steps take into consideration the database differences that exist between Hypertrieve, SQL Server, and Oracle that can impact the VCW.

The VCW does need not to be executed only on the server computer where the vault resides. A backup of the vault can be restored onto an offline computer, possibly with better hardware, and the VCW run there while the source vault remains available for read-only access. The online vault can be made read-only by modifying the security role assignments to prevent any changes. Document authors and editors may want to check out active documents to their Local Workspace before the vault is made read-only. They can then modify the Local Workspace copies offline. After the VCW has finished and the resulting vault has been verified that no inconsistencies exist, it can be restored back onto the original server and production resumed.

The VCW is very memory and disk intensive. When running the VCW, the amount of physical memory installed on the server and the speed of the hard disks can affect the time it takes to run the VCW.

Complete the following steps before running the **Vault Consistency Wizard**.

Important!
Perform these steps in the order they are listed in this document!

1. Run a Prepare for Backup operation on the vault. Save this backup to a secure location before proceeding.
2. If the vault does not use the Hypertrieve 5 database engine, configure the Meridian application server for optimum single-user performance as described in Configure the EDM Server Service.

   This will allow the server to use the maximum amount of system resources for the VCW.
3. Disable all scheduled Prepare for Backup tasks.

   Disabling all scheduled tasks is optional but recommended. The steps to disable a scheduled task depend on the version of Windows used. Refer to the documentation for your version of Windows for details.
4. Disable all virus scanner software.

   The steps to disable virus scanner software depend on the software used. Refer to the documentation for your virus scanner software for details.
5. If Oracle or SQL Server is the vault's database engine, confirm that the following registry value (DWORD), if present, is set to the default of **8**.

If the value is not present, you do not need to create it.

`HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<VaultName>\CompoundItemService\LoggingLimit`

This registry value configures the maximum amount of disk space (in megabytes) to use for write-ahead log files by the database driver. After running the VCW on a SQL Server vault, the database file names will have changed slightly. However, the SQL Server database name and the Meridian vault name should be the same as before running the wizard.

6. If SQL Server is the vault's database engine (dedicated to Meridian only) and SQL Server resides on the same computer where the VCW is run (Meridian server), then the following setting should be considered.

   By default, SQL Server uses as much of the available server memory as you allow it. This can cause problems with the VCW depending on the amount of physical memory and the size of the vault database, so SQL Server memory use should be adjusted while the VCW is run.

   In SQL Server Management Studio, set the maximum memory used by SQL Server with to the following formula:

   Physical memory – 4 GB for the operating system – database file size X 1 if the **Optimize database cache memory** option is enabled as described in Run the Vault Consistency Wizard. If the option is disabled, then the database file size X 2.

7. To prevent users from accessing the vault while running the **Vault Consistency Wizard**:
   a. Open the **Local Users and Groups Microsoft Management Console**.
   b. Navigate to **Groups** > **Windows Local Groups** > **Distributed COM Users**.
   c. Remove access for **Authenticated Users**.

   > **Important!**
   > You will need to re-enable access after the **Vault Consistency Wizard** has completed running.

8. Restart the AutoManager EDM Server service.

Run the Vault Consistency Wizard

Only after performing the steps described in Prepare the Meridian Server and Vault Configuration are you ready to run the **Vault Consistency Wizard** (VCW).

> **Important!**
> Run the VCW after business hours, such as on a weekend.

Run the Wizard

To run the VCW:

1. Open Windows Explorer and navigate to the folder containing the Meridian executable programs.

   By default, the folder is located at `C:\Program Files\BC-Meridian\Program`.
2. Run `AMVltCons.exe`.

   The **Vault Consistency Wizard** appears.
3. Click **Next**.

   The **What to Repair** page appears.
4. Click **Browse**.
5. Select the vault to be repaired.
6. For most vaults, the VCW will run acceptably with the default options.

   Enable or disable options using the descriptions in the following table only if necessary or instructed by Accruent Technical Support.
7. Click **Next**.

   The final wizard page appears.
8. Click **Finish**.

   A progress bar shows the processing progress. When the operation is finished, a dialog box will appear that shows a brief summary of what was found. If inconsistencies are shown, you can view the log file for more details.

   > **Important!**
   > Remember to reverse the server and vault preparation changes described in Prepare the Meridian Server and Vault Configuration after the VCW has completed.
9. To restore user access to the vault after running the **Vault Consistency Wizard**:

a. Open the **Local Users and Groups Microsoft Management Console**.

b. Navigate to **Groups** > **Windows Local Groups** > **Distributed COM Users**.

c. Re-enable access for **Authenticated Users**.

Vault Consistency Wizard options

Option	Description
Check only	Performs a check of the vault database but does not make any changes to it unless the following option is enabled.
Clean up deleted static collections after successful check	Removes orphaned references from documents to static collections that have been deleted with the **LargeSelectionThreshold** registry value set as described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\OML.
Check, Repair and Compact	After the database checks have been performed, any inconsistencies found are repaired, and the database is compacted to reclaim unused disk space.
Optimize database cache memory (large vault)	Enables automatic configuration of memory used by the database cache while the VCW runs to prevent out of memory errors. Enabled by default.
Analysis options	Each option indicates a potential check that the VCW can perform on the vault. Accept the default options unless directed by Accruent technical support. • **Property indexes**: Consistency of the search indexes for the internal and custom properties • **Link targets**: Presence of objects referred to by other objects. This option can significantly increase the amount of time required to complete the VCW. • **Link consistency**: Consistency of the links between objects. This option can significantly increase the amount of time required to complete the VCW. • **Value references**: Presence of value data for internal and custom properties • **String domain**: Consistency of string values • **Skip termination check**: Omits checking for proper termination of database pages • **Numeric domain**: Consistency of numeric values • **ID domain**: Consistency of ID values • **Object locations**: Consistency of the vault locations of objects • **BLOB domain**: Consistency of binary data • **Name domain**: Consistency of name values

Logs

When the VCW runs, it logs its activities to the file `Check.txt` similar to the following example. By default, the file is located in the vault folder. Additional information can be found in the Windows application event log. Review them for any inconsistencies in the vault status values and keep them in case you have further problems and need to send them to Accruent Technical Support.

It is normal for the quantities of items to be different between when the index is rebuilt before and after repairs are made. This is the expected result of purging useless data and compressing the vault database.

Ideally, the six numbers that are reported for the vault status should be 0 after running the VCW check/repair/compact operation. The numbers of documents and versions should be identical before and after running the VCW (17422 documents and 23883 versions in the preceding example). That indicates that the vault is in excellent condition.

Single digit numbers greater than zero that appear in the Windows application event log before running the VCW are not cause for alarm. Run the VCW and they should change to 0. If any of the numbers are not 0 after running a VCW check/repair/compact operation or any of the numbers of the vault status consistently increases from one backup to another, contact Accruent Technical Support.

For more information about the status numbers, see the AutoManager OML source in Review the Application Event Log.

The log file might contain lines with the message "time effectivity ZERO interval". The background for this is that the Hypertrieve database supports versioning through "time effectivity". Each record in the database contains fields indicating the time interval during which the record is valid. A database query is always made for a particular point in time, and all records which are not valid for that time are filtered out.

A record is valid when the start of the record's time interval is equal to or less than the point in time specified in the query, and the end of the interval is greater than the query time point. Records for which start and end of the interval are equal will always be filtered out. Other than taking up some space in the database file, these records do not affect Meridian functionality.

The existence of these "zero-interval" records is related to the unique time and context-versioned nature of Meridian transactions. Generally, their generation is difficult to avoid. When seeing these messages, you can assume that the reported database records have no consequence for the Meridian functionality.

```
===========
ht5ora.dll
===========
0 - Before Check&repair
       Number of documents:    13700
       Vault status for Datastore TEST, Section TEST: 0, 0, 0, 0, 0, 0.
```

```
Docs: 17422, Vers: 23883

1 - Chek&Rep
       Database Check of Software\Cyco\AutoManager
Meridian\CurrentVersion\Installed DataStores\TEST\CompoundItemService
at 5/11/2016 7:53:32 PM
       RebuildIndex(ObjectSet): started. Values in ID Domain: 133079; Last
Location Index = 16635.
       Repairs committed.
       End Database Check of Software\Cyco\AutoManager
Meridian\CurrentVersion\Installed DataStores\TEST\CompoundItemService
at 5/11/2016 7:56:04 PM
       ---------------------------------------------
       Import started at  5/11/2016 7:56:08 PM
       Import ended at  5/11/2016 8:18:03 PM ; Success.

2 - After Check&Repair
       Number of documents:    13700
       Vault status for Datastore TEST, Section TEST: 0, 0, 0, 0, 0, 0.
Docs: 17422, Vers: 23883

3 - Check Only
       Database Check of Software\Cyco\AutoManager
Meridian\CurrentVersion\Installed DataStores\TEST\CompoundItemService
at 5/12/2016 11:18:59 AM
       RebuildIndex(ObjectSet): started for 81393 objects in 10175
locations.
       No errors found.
       End Database Check of Software\Cyco\AutoManager
Meridian\CurrentVersion\Installed DataStores\TEST\CompoundItemService
at 5/12/2016 11:21:25 AM

4 - After Check Only
       Number of documents:    13700
       Vault status for Datastore TEST, Section TEST: 0, 0, 0, 0, 0, 0.
Docs: 17422, Vers: 23883
```

Run the Stream Recovery Wizard

After running the **Vault Consistency Wizard** (VCW), you can recover any remaining orphaned stream (document content) files with the **Stream Recovery Wizard**. The recovered files can then be examined for valuable data and attached to documents in the vault, imported as new documents, or deleted if they are obsolete. The **Stream Recovery Wizard** will collect all these unattached files and place them in a folder of your choice.

> **Important!**
> It is possible to configure multiple Meridian vaults so that they use the same streams. The **Stream Recovery Wizard** should not be run on either vault in such a configuration and could result in the loss of streams.

To run the **Stream Recovery Wizard**:

1. Open Windows Explorer and navigate to the folder containing the Meridian executable programs.

   By default, the folder is located at `C:\Program Files\BC-Meridian\Program`.
2. Run `AMStmRec.exe`.

   The **Stream Recovery Wizard** appears.
3. Click **Next**.

   The **What to Scan** page appears.
4. Click **Browse**.
5. Select the vault for which you want to recover orphaned stream files.
6. Click **Next**.

   The **Where to Copy Recovered Streams** page appears.
7. Click **Browse**.
8. Select a folder.
9. Click **Next**.

   The **Completing the Stream Recovery Wizard** page appears.
10. Confirm the settings you selected and click **Finish**.

    The stream recovery process begins.

    The recovered files will have a cryptic file name, such as `{0F5092F4-CE15-11D5-0000-8FA0546EE97A}` because all information about their identity has been lost. Unfortunately, identifying, renaming, and resolving the recovered files must be done manually.

Create a PowerWeb Location

Creating a PowerWeb location makes a website for a Meridian Enterprise vault so that it can be accessed over an intranet or the Internet using a web browser.

If the new PowerWeb location is not immediately accessible from a web browser, you may need to restart the World Wide Web Publishing Service (IIS) for it to recognize the new web location.

For information about using PowerWeb in read-only mode or with specific saved searches, see Configure a PowerWeb Location.

Enterprise Server is required to run PowerWeb.

Notes about Authentication

User authentication for the PowerWeb location can be configured in Microsoft Internet Information Services the same as a normal website. If **Basic authentication** is enabled, an additional personal option is available to users, **Clear credentials after logging off**. This clears the users' credentials from the browser cache when they log off of PowerWeb, preventing their credentials from being reused accidentally or maliciously by other persons.

Advise users if they should enable this option to comply with your organization's security policies. This option is only available if the website is configured to use **Basic authentication**.

If the authentication method for the PowerWeb server is set to **Basic authentication**, opening document URLs (as shown in PowerWeb) directly with an application will not work; Windows authentication is required.

Procedures

To create a PowerWeb location:

1. In the Meridian Enterprise Administrator, expand **PowerWeb** in the left pane.

   The existing web locations are listed in the right pane.
2. From the **Action** menu, point to **New** and select **Web Location**.

   The **New Web Location Wizard** appears.
3. Click **Next**.

   The **Specify Vault** page appears.
4. Click **Browse**.
5. Select a vault.

6. Click **Next**.

   The **Specify Location Name** page appears.

7. Type a name for the web location.

   It does not need to be the same as the vault name.

8. Click **Next**.

   The **Completing the New Web Location Wizard** page appears.

9. Confirm the settings you selected and click **Finish**.

   The new location appears in the list in the right pane.

10. Choose between two options:

    - If you are using the Meridian IIS application, use the following URL to open the new PowerWeb location:

      `http://<WebServerName>/Meridian/Start`

    - If you are using the PowerWeb IIS application, use the following URL to open the new PowerWeb location:

      `https://<WebServerName>/PowerWeb/?Main`

    In the locally installed components (LWS Client, Site Cache Client Application Integration, and application add-ins), always use the URL to the Meridian IIS application.

Configure a PowerWeb Location

After you have created a PowerWeb location as described in Create a PowerWeb Location, you can later configure it to change the configuration or to enable some advanced options.

PowerWeb can upload files with sizes up to the limit that is configured for Internet Information Services. The default size may be inadequate for your needs. You can adjust the limit as described in the Accruent knowledge base article How to increase the upload file size limit of PowerWeb.

Important!
Enterprise Server is required to run PowerWeb.

To configure a PowerWeb location:

1. In Meridian Enterprise Administrator, expand **PowerWeb** in the left pane.

   The existing locations are listed in the right pane.
2. In the right pane, select the PowerWeb location that you want to configure and then on the **Action** menu, select **Properties** or double-click the location.

   The location's **Properties** dialog box appears.
3. Click options or type values using the descriptions in the following table.
4. Click **OK**.

PowerWeb location options

Option	Description
Location name	The name of the location as it appears to users in a web browser.
Vault	The vault context to be represented by the location. Click **Browse** to select an active vault.
Scope	The name of a scope to show as the location.
Default Web location for this vault	If the same vault is specified by more than one PowerWeb location, the name of the location that is the default for that vault. Click **Make Default** to make the current location the default location.

Option	Description

Default page	Select an existing shared dynamic collection to open by default when the location is opened in read-only mode. To open the location in read-only mode, use one of the following URLs:
	To open a location with the default page:
	`http://<WebServerName>/Meridian/StartPage&vault=<VaultName>`
	To open a location with a specific page:
	`http://<WebServerName>/Meridian/StartPage&vault=<VaultName>&query=<CollectionName>`
	Where *<CollectionName>* is the **Caption** start page option configured for the shared dynamic collection as described in *Configure a Dynamic Collection* in the *Meridian Enterprise User's Guide*.

Configure External Domain Only Connections

If only users in domains outside the domain where the Meridian web server is installed will use PowerWeb, some additional configuration is necessary so that the web server address will resolve correctly in the external domains.

To configure external domain only connections:

1. With an administrator account on the Meridian web server, modify the `C:\Windows\System32\etc\drivers\hosts` file to include the FQDN of the server (as resolved by external domains) at the localhost address.

   For example, `127.0.0.1 myserver.somewhere.cloudapp.azure.com`.
2. With an administrator account on the Meridian web server, add the FQDN to a REG_MULTI_SZ value named **BackConnectionHostNames** in the key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0`.
3. In the Meridian Enterprise Administrator, open the **PowerWeb Properties** page of the **PowerWeb** server and set **Web server address** to the same FQDN as above.

   For example, `http://myserver.somewhere.cloudapp.azure.com`.
4. In the Meridian Enterprise Administrator, reregister the vault as a PowerWeb location as described in Creating a PowerWeb location.
5. In Meridian Enterprise Server Administration Console, unregister the old vault address as described in the *Unregister repositories* article in the *Meridian Enterprise Server Administrator's Guide*.
6. In Meridian Enterprise Server Administration Console, register the new vault address as described in the *Register a Meridian Enterprise vault* article in the *Meridian Enterprise Server Administrator's Guide*.
7. In Meridian Enterprise Server Administration Console, unregister and reregister the repository in the Meridian Enterprise Server site cache configuration as described in the *Configure site cache servers* article of the *Meridian Enterprise Server Administrator's Guide*.
8. Confirm that the web server address shown is the same as set above.
9. If the configuration works for some vaults but not others, check the **Url** setting of the vault in `C:\ProgramData\BlueCieloECM\SiteCache\ContentRepositories.dat`.

Remove Vault History

Important!
Removing vault history is a permanent change that cannot be undone except by restoring a vault from backup. A safer option is to archive historical documents instead as described in Archive Documents.

Removing a vault's history permanently purges historical data from a vault that was created before a specified date and time. Removing history can be useful to remove old revisions of documents that are no longer required.

Removing vault history does not directly compact the database or reclaim unused disk space. To optimize database size and disk usage, see Vault Consistency Toolkit.

To completely remove all vault history and prevent further historical data from being created in the future, consider disabling the vault's **Maintain** option instead.

To remove vault history:

1. In the Meridian Enterprise Administrator, click **EDM Server** in the left pane.

   The active vaults are listed in the right pane.
2. Select the vault for which you want to remove history in the right pane.
3. On the **Action** menu, point to **All Tasks** and select **Remove History**.

   The **Remove History** dialog box appears.
4. Confirm the specified vault is the vault for which you want to remove history.

   If it is not, click **Browse** and select the correct vault.
5. Select a date and time in **Remove all history before** that you want to remove all history before.
6. Select either **Remove documents and metadata** or **Remove documents only**.

   Note:
   Select **Remove documents only** to retain the historical metadata for searches if the documents themselves will no longer be needed. You can remove the metadata later, if necessary.
7. Click **Finish**.

   A message is shown when the specified history has been removed.

Important!
After removing vault history, always run the **Vault Consistency Wizard** as described in Vault Consistency Toolkit to prevent database errors and to reclaim unused disk space.

Rename a Vault

After a vault has been created, it cannot be easily renamed with the Administrator tool.

> **Note:**
> This task pertains to Hypertrieve vaults only. For information on moving SQL Server or Oracle vaults, see the links to related topics at the end of this topic.

> **Important!**
> The following task should only performed after business hours and after backing up all related files and registry settings. This task should only be performed by persons with knowledge of and experience with editing the Windows registry. Incorrect changes can result in the vault being inaccessible to users.

To rename a vault:

1. Choose between two options:
   - In the Meridian Enterprise Administrator, right-click **EDM Server** in the left pane and select **Properties**.

     The service's **Properties** dialog box appears.
   - Use the **Services** applet in **Control Panel**.
2. Change **Startup type** to **Disabled**.
3. Click **Apply**.

   > **Note:**
   > You must disable the services so that they will not automatically restart if requested by client applications.
4. Click **Stop**.

   You are prompted to stop the **Accruent Filesystem Server** service.
5. Click **Yes**.

   Both services are stopped.
6. Repeat steps 3 to 6 with the **Accruent License Server** service and the **AutoManager Task Server** service (if used).
7. If PowerWeb is used, also stop the **World Web Publishing** service on the web server.
8. Open the server's registry in Registry Editor and locate the following key:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<VaultName>`

9. Change the value of **DefaultSection** to the new name.
10. If you want new vaults to be created in a different folder than the default (`C:\BC-Meridian Vaults`), open the server's registry in Registry Editor and locate the following key:

    ```
    HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
    Meridian\CurrentVersion\Installed DataStores
    ```

11. Change the value of **DefaultDataPath** to the new location.
12. In the Meridian Enterprise Administrator, change the **Startup type** property of the services that you cleared previously back to **Automatic** and restart the services.
13. Test access to the vault by various security roles and that changes to documents are saved correctly.

Move a Vault

After a vault has been created, it cannot be easily moved with Meridian Enterprise Administrator tool. These operations require careful copying of the vault data and server configuration that differ depending on whether the vault will be relocated on the same server or moved to a different server.

These operations involve the following data:

- Database files
- Document content (stream) files
- Licenses

The basic process for moving a vault is the same whether the vault will be moved to a new location on the same server or on a new server. Restoring a backup of the vault is the safest and easiest way to ensure that the vault is created properly in the new location.

If you will be moving the vault to a new server and the original server will be taken out of service, consider retaining the name for the new server. Retaining the old server name resolves several issues that will result from using a new server name:

- **Security**: The recommended procedure for setting security on a vault is to assign Meridian security roles to local user groups. Therefore, the computer name of the Meridian application server is part of the role assignments. If the vault is moved to a server with a different name, all of the role assignments must be removed and reapplied using local groups that exist on the new server. If the same computer name is used for the new server, no changes are required to the security roles of the vault.
- **Transparency to the user**: Moving a vault to a server with a new name will not go unnoticed by the users. They will have to be informed about the new server name and browse to this server to find their vaults. Likewise, if PowerWeb is installed on the Meridian application server, the URL for use by PowerWeb users will also change. Thereafter, Meridian will remember the new application server name.

  But more seriously, changing the server name will cause a new, empty local workspace to be created on the client computers where documents that the users were working on before the move will not yet exist. Manual intervention will be required to move the documents to the new local workspaces.
- **Customization**: In some cases, vault customization might have been programmed that depends in some way on the computer name of the Meridian application server. Such customization might need to be debugged or rewritten for the customization to work again.

Instructions for moving a vault are contained in the following topics. These tasks pertain to Hypertrieve vaults only. To move vaults that use other database engines, see Move a SQL Server Vault To a Different Folder or Restore an Oracle Vault To Another Server accordingly.

Move a Hypertrieve Vault

To move a Hypertrieve vault from one server to another (for example, to upgrade the server hardware), we recommend that you back up the vault on the source server with the **Prepare for Backup Wizard** and restore the vault on the destination server with the **Restart After Restore Wizard**. To move only a vault's content files without moving its metadata, see Move the Document Content Files.

> **Important!**
> The following task should only be performed after business hours and after backing up all related files and registry settings.
>
> It is not possible to move (by restoring from backup) a vault from a pre-Windows Server 2008 computer (including Windows XP, Windows Server 2000, or Windows Server 2003) to a post-Windows Server 2008 (including Windows Vista) or later computer without adverse side effects. The possible side effects include folders and documents not being accessible, and vault corruption.
>
> The cause is Windows API functions that behave differently between pre-Windows Server 2008 and post-Windows Server 2008 operating systems.

There are two supported methods to move an existing vault from a pre-Windows Server 2008 computer to a post-Windows Server 2008 computer:

- Import the vault from the source server into a new vault on the post-Windows Server 2008 computer.
- Restore a backup of the vault from the source server onto the new server and reindex the vault with the icosnlsver tool as described in Change Operating System Versions. Migration assistance is available from Accruent Partners and Accruent Technical Support.

See the *Supported Software* document for this release of Meridian for the names and versions of supported operating systems.

The general procedure to move a Hypertrieve vault is:

1. If the vault will be moved to a different server, ensure that enough free disk space is available as described in Document Storage Space Requirements, install the Meridian Enterprise software on the destination server as described in Installation and ensure that client computers can connect to it before proceeding.
2. If the License Server service will also be moved to the other server, register the licenses as described in Register Licenses - Administrator.

If the computer running the License Server service is separate from the source server, this step is not necessary but the License Server computer must also be accessible from the destination server.

3. Create a backup of the vault on the source computer as described in Prepare For Backups.
4. Ensure that no users are connected to the source server by viewing the current license usage as described in View Current License Usage.
5. Confirm that a `DataStore.ini` file is present in the `Backup` folder.

   Before you can move the data, you must first stop the services that use the data.
6. In Meridian Enterprise Administrator, right-click **EDM Server** in the left pane and select **Properties**.

   The service's **Properties** dialog box appears.

   > **Note:**
   > You may also use the **Services** applet in **Control Panel** to perform the following several steps.
7. Change **Startup type** to **Disabled**.

   You must disable the services so that they will not automatically restart if requested by client applications.
8. Click **Apply**.
9. Click **Stop**.

   You are prompted to stop the **Accruent Filesystem Server** service.
10. Click **Yes**.

    Both services are stopped.
11. Repeat steps 3 to 6 with the **Accruent License Server** service and the **AutoManager Task Server** service (if used).
12. If PowerWeb is used, also stop the **World Web Publishing** service on the web server.
13. Copy the entire vault folder contents (including the `Backup` and streams folder structures) to the `BC-Meridian Vaults` folder of the destination computer.

    The original vault folder contents will act as a temporary online backup. After you have completed moving the vault and confirmed that users are correctly accessing the vault in the new location, you can safely delete the original vault folder contents.

    > **Note:**
    > Copying the vault folder can take a long time depending on the size of the vault, content indexing options, and so on. Allow sufficient time for the copy to complete before proceeding.

14. If the vault stream files are not located in the default location (subfolders of the vault database folder) and you are moving the vault to a different server, copy them to the new location also at this time.

    This step can also take a long time. If the stream files are located on a drive that is also accessible from the destination server using the same UNC or drive letter (for example, NAS or SAN devices) and you do not want to move them, they can remain in place.

15. Copy the custom extensions folder and its subfolders to the new location, if necessary.

    By default, the folder is located at `C:\BC-Meridian Extensions`.

16. If the Task Server is used, copy any pending tasks to the new server by copying the contents of the following folder to the same location on the new server: `C:\Documents and Settings\All Users\Application Data\Cyco\AMTasks`.

17. Edit the `DataStore.ini` file on the destination computer and correct the paths in the **Databasename** and **RootPath** settings, if necessary to match the destination computer.

18. Restore the vault as described in Restore Backups using the edited `DataStore.ini` file.

19. In the Meridian Enterprise Administrator or the **Services** applet of **Control Panel**, change the **Startup type** property of the services that you cleared previously back to **Automatic** and restart the services.

20. Test access to the vault by various security roles and that changes to documents are saved correctly.

Move the Document Content Files

As vaults grow in size over time and larger or faster storage solutions are available or as your Meridian Enterprise system expands to multiple servers, it may become beneficial to move the document content (stream) files managed by the vaults to a different location away from the Meridian Enterprise application server while leaving the vault metadata in place. This can make more storage space available to the vaults or consolidate the storage of multiple vaults in a single location. To move a vault entirely (content files and metadata) to a different location, see Move a Hypertrieve Vault.

> **Note:**
> For the Meridian Enterprise application server to be able to access the document content files after they have been moved, the EDM Server service must run under an account that has adequate access to both locations as described in Grant Domain Privileges With a Service Account. Due to the high volume of network traffic between the Meridian Enterprise application server and the document content files, a dedicated, high-bandwidth (Gigabit or higher), low-latency connection between the servers is required.

> **Important!**
> The following task should only be performed after business hours and after backing up all related files and registry settings.

To move the document content files:

1. Ensure that no users are connected to the Meridian Enterprise server by viewing the current license usage as described in View Current License Usage.

   Before you can move the data, you must first stop the services that use the data.

2. In Meridian Enterprise Administrator, right-click **EDM Server** in the left pane and select **Properties**.

   The service's **Properties** dialog box appears.

   > **Note:**
   > You may also use the **Services** applet in **Control Panel** to perform the following several steps.

3. Change **Startup type** to **Diabled**.

   This disables the service so that it will not automatically restart if requested by client applications.

4. Click **Apply**.
5. Click **Stop**.

You are prompted to stop the **Accruent Filesystem Server** service.

6. Click **Yes**.

   Both services are stopped.

7. If PowerWeb is used, also stop the **World Web Publishing** service on the web server.
8. Copy the entire vault folder contents (including the `Backup` and streams folder structures) to the new location.

   The original vault folder contents will act as a temporary online backup. After you have completed copying the files and confirmed that users are correctly accessing them in the new location, you can safely delete the original vault folder contents.

   > **Note:**
   > Copying the vault folder can take a long time depending on the size of the vault, content indexing options, and so on. Allow sufficient time for the copy to complete before proceeding.

9. Modify the registry values described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<vaultname>\StreamService to specify a UNC path to the new location.
10. Change the account under which the EDM Server service runs to an account that has adequate access to both locations as described in Grant Domain Privileges With a Service Account.
11. Restore the **Startup type** of the EDM Server service to **Automatic** and restart the service.

Disable a Vault

Disabling a vault causes it to not be loaded by the EDM Server service but does not delete any of the vault's metadata or documents. This can be useful to free system resources when:

- The vault should be maintained in an offline but ready state
- Performing server-intensive administration tasks on other vaults

Disabling a vault involves renaming it in the server's registry. You can enable the vault at any time by returning the vault to its original name.

To disable a vault:

1. Open the Registry Editor on the Meridian application server and navigate to the following key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
   Meridian\CurrentVersion\Installed DataStores
   ```

2. Expand the key and select the vault name to be renamed.
3. Edit the vault name and insert an underscore at the beginning of the vault name. This will disable the vault when the EDM Server service is restarted later.

   > **Note:**
   > To quickly rename a registry key, highlight the key and press F2.

4. Restart the EDM Server service to reload the enabled vaults but not the disabled vault.

Data Library

The optional Data Library is created and maintained separately from vaults. It synchronizes a SQL Server or Oracle database with document metadata from a single Meridian Enterprise source vault.

Create the Data Library

After the Data Library server components have been installed and configured, you must create and synchronize the Data Library before you can use its data in reports. Creating the Data Library data involves numerous steps that should be performed in the following sequence.

To create the Data Library:

1. Create the repository as described in Create a Meridian Explorer Repository.
2. Create a Data Library synchronization job as described in Configure a Data Library Synchronization Job.

   The publishing job synchronizes document metadata from the Meridian Enterprise vault to the Data Library. Schedule the synchronization job to run on a periodic basis. Repeating the synchronization job ensures that the Data Library is kept up to date with the contents of the source vault.
3. Run the synchronization job as described in Run a Publishing Job.

   Running the job performs the initial import of vault data into the Data Library.
4. Monitor the publishing job as it progresses as described in Monitor Background Tasks.
5. Configure email notification of the publishing job results as described in the *Specify a mail server* article in the *Meridian Enterprise Server Administrator's Guide* (Optional).

   Email notifications allow you to remain informed as to the status of the Publisher updates.
6. Back up the Data Library as described in Back Up a Repository.

Create a Meridian Explorer Repository

Meridian Enterprise Server helps you to create and test a connection to a database server where you want to store the repository. You can use the wizard to create connections to SQL Server or Oracle servers.

If you have sufficient privileges to create a new database on the database server, you can create a repository by performing the following task. If you have access to the database server with another account that does not have access from the Meridian Explorer server, see SQL Server Database Creation Script or Oracle Database Creation Script. If you do not have sufficient privileges, a database administrator will have to create the database for you.

Prerequisites

Before creating a repository, you must complete the following prerequisites.

1. You must know the name of either a Windows user account or a database account with permissions to access the database server and create database tables, indexes, and stored procedures. You also need to know the account password.
2. Meridian Enterprise Server requires that the SQL Server or Oracle instance already exist before a repository can be created. If Oracle will be used, an existing user (schema) can be used but we recommend that you can create a new user dedicated to Meridian Enterprise Server. If multiple repositories will be hosted by Oracle, we recommend that you create a separate user for each repository.
3. Before creating an Oracle Repository or BCConfiguration database, you must configure ODAC.

Procedures

To create a repository:

1. In Meridian Enterprise Server Administration Console, in the **Repositories** group, click **Repositories**.

   The **All Repositories** page appears and lists the existing Meridian Explorer repositories and Meridian Enterprise vaults.
2. Click **New**.

   The **New Repository** dialog box appears.
3. Select **Explorer repository**.

4. Click **Next**.
5. Click options or type values using the descriptions in the following table.
6. Click **Register**.

   A background task is started and you may continue working. Creating the repository can take several minutes. After the new database is created, the new repository name appears in the **Repositories** list.

Database connection options

Group	Option	Description
General	Repository Name	Type a name for the repository as you want it to appear to users.
General	Provider	Select a database provider type from the list.
General	Server (SQL Server only)	Type the name of the SQL Server computer that will host the repository. If the database server is running SQL Server Express, SQL Server Small Business, or another edition that created a named instance when the software was installed, type the name of the database server and the SQL Server instance name, for example, **MyServer\SQLEXPRESS** or **MyServer\MSSMLBIZ**.
General	TNS Network Alias (Oracle only)	Type the name of the Oracle server and instance that will host the repository. For example, **servername:1521/instance** where **1521** is the default port of Oracle communication.
Authentication	Type	If you selected **SQL Server** in the **Provider** option in step 1, select your preference for **Windows** or **SQL Authentication**.
Authentication	User name	SQL Server only: If you selected **SQL Authentication**, type a SQL Server user account with permissions to access the database server and create database tables, indexes, and stored procedures. Oracle only: Type a valid Oracle user account with permissions to access the database server and create database tables, indexes, and stored procedures.
Authentication	Password	Type the password for the user account.

Group	Option	Description
Database	Database (SQL Server only)	To select an existing database or to create a new database: • Click **Edit**. The **Select Database** dialog box appears. To create a new database: • On the **New Database** page, click options or type values using the descriptions in the following table. To select an existing database: • On the **Existing Database** page, select an existing database name and click **OK**. The name appears in the **Database** field.

The options in the following table are only available with the appropriate license. If you think you should have these options and you do not have them, contact your Accruent representative.

Database options

Option	Description
Database	Type a name for the new database.
Primary path	Type a path on the database server for the repository metadata files.
Content path	Type a path on the database server for the repository content files.
Index path	Type a path on the database server for the repository index files.
Log path	Type a path on the database server for the repository log files.

Option	Description
Use file stream	Enable this option if you want the new database to use the SQL Server FILESTREAM feature. We recommend this option for higher performance. If this option is disabled, content copied from the source vault will be stored inside the database as binary large objects (BLOBs). Before using this feature, we strongly recommend that you fully understand the advantages, limitations, and implications of the feature by studying the Microsoft SQL Server documentation. This option requires that the **Windows** authentication option be used to access the database server. By default, the Meridian Enterprise Server copies document content from the stream folders of the source vault. You can configure it as follows to copy the content from an alternative file stream location: • Create a plain text file named `MRE2368.dat` in the folder `C:\ProgramData\BlueCieloECM\Hyperion` that contains the alternate stream folder settings for each Meridian Enterprise vault to be synchronized. The settings must be in JSON notation like the following example: `{ "StreamFolders":[{ "SourceName": "DatastoreName1", "FolderPath": "C:\\Data\\BC-MERIDIAN VAULTS\\DatastoreName1" }, { "SourceName": "DatastoreName2", "FolderPath": "C:\\Data\\BC-MERIDIAN VAULTS\\DatastoreName2" }] }` The synchronization job will attempt to copy the vault stream files from the specified path. If the path does not exist, an error will occur. If a particular stream file does not exist in the specified folder, the job will attempt to copy it from the regular streams folder.
File stream path	If the **Use File Stream** option is enabled, type a path on the database server for the database Filestream files. This option is only enabled if the database server is compatible.

After creating a repository and before vault synchronization with the repository can occur, at least one synchronization job must be configured.

Configure a Data Library Synchronization Job

A Data Library synchronization job is created from the **Data Library** template that is provided with Publisher. This type of job defines the options for publishing documents from a Meridian Enterprise vault to the Data Library.

To configure a Data Library synchronization job:

1. In Accruent Application Manager, expand the name of the publishing job in the configuration tree that you want to configure.
2. Select the **Configuration** branch in the configuration tree.

   The job's configuration pages appear in the right pane.
3. In the **BC Meridian source vault group**, select a vault from the **Vault** list.

   A read-only name appears in the **Repository** group for **Repository name**.
4. In the **Repository** group, click **Edit** to configure the repository connection string as described in Create a Meridian Explorer Repository.
5. Click **Save**.

Run a Publishing Job

Running a publishing job starts the job immediately. Repeating a past publishing job runs the job immediately using the current job options, which might not necessarily be the options that were in effect when the job was first run.

If the source system contains many documents, we recommend that you perform the first run of the publishing job outside of business hours. The publishing job could take a considerable amount time depending on the size of the source data.

Notes about Functionality

- A publishing job will generate an error if licenses for any of its system links or rendering modules are unavailable.
- No two publishing jobs may run at the same time on the same computer. A publishing job and a Meridian Explorer synchronization job may run at the same time.
- When a Meridian Explorer synchronization job runs, it will detect new and modified documents, tags, and projects in the vault and synchronize only those items with the destination system. Publisher records the date and time that the last synchronization job ran so that it can perform another differential synchronization the next time that the job runs. To reset that date and time and thereby force a full synchronization, see *Manage a Meridian Enterprise Vault* in the *Meridian Enterprise Server Administrator's Guide*.
- When a Meridian Explorer synchronization job runs, it will detect new items that have been added to the vault configuration since the last time that the job ran and that can be mapped to corresponding items in the repository. New document types, tag types, folder types, and reference types will be automatically added to the repository configuration and mapped accordingly. New document and folder properties that cannot be matched to corresponding repository items will stop the publishing job and show a warning that the property mappings must be updated to either include or exclude the new properties.

Run Immediately

To run a publishing job immediately:

1. In Meridian Enterprise Server Administration Console, in the **Data Exchange** group, click **Jobs**.

   The **All Jobs** page opens with a list of existing publishing jobs. The jobs are grouped by the name of the computer (cluster node) to which they have been assigned.

2. Select the job that you want to run and then in the toolbar, click **Run**.

   The job is started as a background task. For information about background tasks, see Monitor Background Tasks.

Repeat a Past Job

To repeat a past publishing job:

1. In Enterprise Server Administration Console, open the **Tasks** page as described in Monitor Background Tasks.
2. Select the job that you want to repeat and click **Repeat**.

   A dialog box opens, asking you to confirm your choice.
3. Click **Yes**.

   The job is copied to the top of the **Tasks** list and starts immediately.

Schedule a Single Publishing Job

To schedule the publishing job to run automatically on a periodic basis, thereby keeping the repository up to date, see the *Schedule a Single Publishing Job* article in the *Meridian Enterprise Server Administrator's Guide*.

Monitor Background Tasks

While background tasks (for example, a publishing job) are running, you can monitor their progress and their effects on server performance. You can also review the history of tasks that have run in the past.

- A publishing job will appear as one task in the **Tasks** list but may publish many documents. To view the status of individual documents, view the Publisher queue instead as described in *View the Publisher Queue* in *Meridian Enterprise User's Guide*.
- Changes to documents in the source system (including references) will not appear in the destination system if the documents fail to publish successfully as the result of a failed publishing task.

To view additional details about a task, see Inspect a Background Task.

Monitor Background Tasks

To monitor the background tasks:

- In Meridian Enterprise Server Administration Console, in the **System Management** group, click **Tasks**.

  The **Tasks** page appears and lists the background tasks that have been created and their status.

Filtering the Tasks List

Choose one of the following options:

- To filter the Tasks list by **job status**, in the menu, click the status of the jobs that you want to monitor.

  The list is filtered by the selected status.
- To filter the Tasks list by **job name**, type the beginning of the job name in the **Job code** box and then click the filter icon .

  The list is filtered by the text that you typed.
- To filter the Tasks list by **the name of the user that submitted the job**, type the beginning of the user's name in the **User** box and then click the filter icon .

  The list is filtered by the text that you typed.

- To remove a filter, remove the text that you typed and click the filter icon .
  The full list of jobs is shown.

Inspect a Background Task

You can learn a lot about a background task by viewing closely the information that Meridian Enterprise Server provides about it:

- Status, progress, and details
- Performance effects on the server
- Errors

The performance data is shown as a pie chart. The chart divides the total elapsed time to run the publishing job into its individual processes. This chart can be useful to identify bottlenecks in Meridian Enterprise Server performance.

Inspect Background Task

1. Open the **Tasks** page as described in Monitor Background Tasks.
2. Select the task that you want to inspect and then in the toolbar, click **Open**.

   The **Dashboard** page for the task appears and shows an overview of the task and performance statistics related to the task. To show performance data for the task as a pie chart in the **Performance** pane, enable the **Collect dashboard statistics** option of each task for which you want to see the dashboard. If you do not have the required licenses, you will not have access to these configuration options.

   The statistics for synchronization jobs that use batch synchronization will not appear until after each batch has completed.
3. To view any errors that occurred during the task:
   a. In the menu, click **Diagnostics**.

      The errors are listed in the order that they occurred.
   b. To view only the failed processes:
      - Click the process result (**Passed** or **Failed**) and in the menu that appears, click **Failed**.

        The processes that succeeded are hidden.

Export Task Details

The details of failed tasks can be exported for troubleshooting.

1. Click **Export**.

   The file `LogTaskDetailsExport.xlsx` is downloaded by your browser and you are prompted for what to do with it.

2. Save or open the file.

Back Up a Repository

A repository database is a normal DBMS database that can be backed up with other data managed by the DBMS. However, since the repository is synchronized from data stored in Meridian Enterprise, the repository database is not at a high risk of loss. It can be easily re-created by resynchronizing it from its source vault either manually or by the next run of the synchronization job scheduled task. However, because full synchronization can take a considerable length of time depending on the size of the source vault, you might want to back up the repository database anyway so that it can be restored more quickly.

When stored in SQL Server, the repository database uses multiple file groups. To ensure that the file groups are correctly restored from a backup, we recommend using the Full Recovery Model for the repository database. Also, if the FILESTREAM option of the repository is enabled, be sure to also back up the FILESTREAM path.

Report From the Repository

The Meridian Explorer repository can be a data source for your preferred reporting applications. You can configure reports against the repository using any application that supports the same data source as your repository, for example, Microsoft SQL Server Reporting Services or SAP Crystal Reports. You may also create reports from any application that functions as a web API client.

The repository database includes approximately 50 interrelated tables. To simplify reporting, the repository provides predefined views upon which you can base your reports:

- **dbo.AreaView**: Includes all projects
- **dbo.DocumentView**: Includes all properties for all document revisions. Filter on the **IsLatestRevision** column to exclude prior revisions
- **dbo.FolderView**: Includes all folders
- **dbo.ObjectTagView**: Includes all properties for all asset tag revisions. Filter on the **IsLatestRevision** column to exclude prior revisions

We recommend that you create reports on these views, not on the source tables. If you have special requirements that cannot be easily met using these views, contact your Accruent Partner or Accruent Professional Services for more specific views.

Meridian Enterprise Server provides a web API for external applications that need to query a Meridian Explorer repository for documents based on property filters with HTTP(S) web requests. The web API supports standard AJAX GET and POST requests, and the data is returned in JSON format. For more information about the web API, see the *Web API reference* article in the *Meridian Enterprise Server Administrator's Guide*.

Backups And Recovery

Frequent vault backups are critical to safeguarding the valuable documents residing in Meridian vaults. You should make backups at least daily, even if you have implemented Redundant Array of Independent Disks (RAID) or other data redundancy systems. Vault backups allow you to recover from failures that are not disk-related, such as human or software errors. Even though you will lose all documents and metadata created after the last backup and the vault recovery process can be quite time-consuming, restoring a backup is in most cases the last resort and it enables you to recover from virtually all emergency cases. We highly recommend that you also implement procedures to maintain additional periodic backups using retention schemes such as monthly/weekly/daily.

You use the Meridian Enterprise Administrator wizards to create and restore vault backups. The **Prepare for Backup Wizard** prepares backup files for a vault, which can then be backed up to a safe location by your normal backup software. The **Restart After Restore From Backup Wizard** restores a vault from files created by the **Prepare for Backup Wizard**.

> **Important!**
> You must use the Meridian wizards or their command-line equivalents to make and restore vault backups. Simply backing up and restoring the Meridian vault folders is insufficient and can result in lost data. Likewise, backing up and restoring SQL Server or Oracle vault databases with those system's tools is insufficient for two reasons. The first reason is that only the Meridian tools will ensure that all pending transactions are committed to the vault database before a backup is made and no data is lost. The second reason is that most third-party backup programs do not back up files that are in use, and a vault's database files are in use whenever the EDM Server service is running.

Meridian tracks the amount of time elapsed since a vault was last prepared for backup. When you open the Meridian Enterprise Administrator tool, a warning message is shown if any vaults have not been prepared for backup in over five days. This interval may be adjusted with the **AlertNoBackup** registry key described in Windows Registry Keys. The **Status** column in the **EDM Server** vault list in the Administrator also shows the backup status of vaults.

Regardless of the database engine used by a vault, the data backup and recovery procedures are similar and are described in the following topics. If the SQL Server or Oracle database engines are used, the procedures are slightly different.

Database Recovery

Meridian Enterprise is capable of complete recovery of the Hypertrieve database, although the chances of corruption are very limited due to the transaction-oriented structure. Three levels of database recovery are possible with the Hypertrieve database engine. Each level takes advantage of a snapshot of the database that is made:

- When a Prepare for Backup operation occurs
- On demand as controlled by the **MaximumLogSize** and **MinimumSnapshotInterval** settings described in Configure the MaximumLogSize Setting and Configure the MinimumSnapShotInterval Setting.

When a snapshot is created, the transaction log files are committed to the active database and the database is copied as the snapshot file. The transaction log file is then reset (truncated).

The three levels of database recovery are described in the following topics.

Level 1 Recovery

All Hypertrieve database transactions are written to a transaction log file. If the Hypertrieve database gets corrupted, for example, when the server is switched off without a proper shutdown procedure, Meridian tries to recover the database automatically when the server reboots. The log file will be replayed to rebuild the database. Depending on the length of the log file, this process can be time-consuming. If such an event has happened, information is written to the Windows Application event log. In this case, all data created until the moment of database corruption is maintained.

Level 2 Recovery

If level 1 database recovery does not succeed, a System Administrator can attempt to recover a Hypertrieve database by restoring a snapshot. In this case, data added after that the last snapshot was taken is lost.

To restore a snapshot manually:

1. Stop and disable the EDM Server service.
2. Open Windows Explorer and browse to the folder of the vault that you want to restore.
3. Move the file *<VaultName>*.hdb to a safe location.
4. Copy the file *<VaultName>*.snp to *<VaultName>*.hdb.
5. Enable and restart the EDM Server service.

Level 3 Recovery

If level 1 and level 2 database recovery attempts do not succeed, a System Administrator can restore the database from the backup media as described in Restore Backups. In this case, all data created after the last backup is lost.

Prepare For Backups

Before vault data can be safely backed up, it must first be prepared. The Meridian **Prepare for Backup Wizard** does this for you. After saving all pending transactions to the vault database and closing open files, it creates copies of the database files, which you may then back up with your normal backup software.

If a scheduled task will be created, it's helpful to know when other tasks are scheduled on the same computer so that this task doesn't interfere with those processes and vice versa. We recommend scheduling this task to occur before a recovery log task is executed on the same day and before regular system backups occur. A Prepare for Backup operation can take up to 20 minutes, so this task should be scheduled to occur 30 minutes before any other daily backup tasks and not during production hours.

> **Important!**
> Changes should not be made in a vault between the time when the backup files are prepared and their corresponding stream files are backed up by a regular system backup. Otherwise, the files will not be synchronized and restoring them later may result in lost changes.

This task must be performed at the Meridian application server and not from a client computer if a scheduled task will be created.

To prepare backup files:

1. If the vault data is stored in Oracle, set the **UseCompatibleBackup** registry value as described in Oracle Vault Backups.
2. In the Meridian Enterprise Administrator, click **EDM Server** in the left pane.

   The active vaults are listed in the right pane.
3. From the **Action** menu, point to **All Tasks** and select **Prepare for Backup Wizard**.

   The **Prepare for Backup Wizard** appears.
4. Click **Next**.

   The **What to Back Up** page appears. To export the configuration of the vault also so that it can be included in the backup, enable **Include vault configuration**. This will create a `.met` file as described in the *Export Configuration Data* sub-procedures in the *Meridian Enterprise Configurator* article in the *Meridian Enterprise Configuration Guide*.
5. Click **Browse**.
6. Select the vault to back up.
7. Click **Next**.

   The **When to Prepare for Backup** page appears.

8. Choose between two options:
   - Select **Now** to create the backup files immediately upon finishing the wizard.
   - To schedule a job to run at a later time:
     a. Select **Later**.
     b. Type a user ID and password for the job to run as.

        We recommend that you specify a user account with a password that never expires. If the user account is removed, or the password either expires or is changed, the scheduled task will fail and backup files will not be created.
     c. Click **OK**.

        By default, the job will be repeated daily at the current time.
     d. Click **Set Schedule** to modify the job's schedule in the new dialog that appears.
     e. Select options on the **Schedule** page to coordinate the job with other tasks running on the computer and the time when regular system backups occur.
     f. Click **OK**.

        A new job is created for the Windows Task Scheduler that may be modified with the normal Windows administration tools. For more information about Task Scheduler, refer to the Windows documentation.
9. Click **Next**.

   The **Completing the Prepare for Backup Wizard** page appears.
10. Click **Finish**.

    The backup files are created immediately or at the scheduled time, and placed in the `Backup` subfolder of the `BC-Meridian\Vaults` folder.
11. Back up the files with your normal backup software.

    You should back up each vault folder and all sub-folders (streams and `Backup` folder), but exclude the open database files (`*.hdb` and `*.lck`). The streams folders have 4- or 8-character hexadecimal names, for example, `3D0C` or `1FF20BD3`. Also back up the the `BC-Meridian Extensions` folder.

    The `Backup` folder for a Hypertrieve vault contains the following files:
    - `DataStore.ini`: Vault configuration parameters for use when restoring the vault.
    - *`<VaultName>`*`.snp`: Snapshot of the vault database.
    - *`<VaultName>`*`.log`: Empty database transaction log necessary to restore the vault.
    - *`<VaultName>`*`$LL.mdb`: Microsoft Access database containing lookup list data tables created in Meridian Enterprise Configurator.

- *<VaultName>*.met: Vault configuration settings as managed in Meridian Enterprise Configurator (if **Include vault configuration** is enabled).

When a **Prepare for Backup** operation is scheduled for later execution, the task executes invisibly in command-line mode. This mode returns an error number if the backup fails that you can use in a batch file to send an alert message to a System Administrator. Following is an example batch file that you can modify for your own requirements:

```
"C:\Program Files\BC-Meridian\Program\ambackup" MyVault
If errorlevel 0 Goto End
C:\Windows\System32\Net Send Administrator "Backup failed for
vault MyVault!"
:End
```

Restore Backups

Restoring a Meridian Enterprise vault from a backup consists of the following tasks that must be performed in the order listed:

1. Restore files to disk that were backed up with your normal backup software.
2. Reindex the vault using the sorting order of the current operating system as described in Change Operating System Versions.

   This task is only necessary if the operating system of the server where the vault will be restored is different from the server where the vault was backed up.
3. Restore the vault from the restored files using the following instructions.

   The **Restart After Restore from Backup Wizard** in the Meridian Enterprise Administrator does this without stopping the Meridian services. Regardless, restoring a vault should not be performed during production hours except in emergencies.

Important!
Restoring a vault will completely overwrite the vault's existing database. Be very certain that no valuable data will be lost before proceeding.

Notes about System Behavior

- If any documents were added to the vault after the **Prepare for Backup** wizard was run and its files backed up, they will be missing from the vault restored by the **Restart After Restore** wizard. However, their streams (content files) may still exist in the vault folder structure. The **Stream Recovery Wizard** may be run to reuse the files.
- If the source vault had content indexing enabled and is being restored on a different server, the content index update scheduled task may need to be re-created as described in Restore a Vault That Has Been Indexed.
- If the EDM Server service fails for reasons such as insufficient memory or disk space and automatic restoration of the vault database also fails, no subsequent operations on the vault will be possible until the problem is resolved. Preserve all disk files, disable the vault as described in Disable a Vault, and contact Accruent Technical Support.
- Verify that the files you restore are for the correct backup. If the location of the **BackupLocation** setting described in the following topic has been changed from the default, the default location may not contain the correct files.

  HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<vaultname>\CompoundItemService

Restore a Vault with Restart After Restore From Backup Wizard

To restore a vault from a backup with the **Restart After Restore from Backup Wizard**:

1. Ensure that no users will access the vault while it is being restored.

   The easiest way to prevent vault access is to temporarily disconnect the server from the network.

2. Restore the `Backup` folder using your normal backup software's restore features.

   If no streams files yet exist, also restore the entire streams folder structure. Under most circumstances, you should restore the files to their original locations and overwrite all existing files. For this reason, all vault backups should be verified as complete and accurate before they are restored for production use.

   This step completes the restoration of stream files. The remaining steps in this task describe how to restore the vault database.

3. In the Meridian Enterprise Administrator, click **EDM Server** in the left pane.

   The active vaults are listed in the right pane.

4. From the **Action** menu, point to **All Tasks** and select **Restart After Restore From Backup Wizard**.

   The **Restart After Restore From Backup Wizard** appears.

5. Click **Next**.

   The **Locate Backup Information File** page appears.

6. Click **Browse**.

7. Select the `datastore.ini` file restored in step 2.

   By default, the file is located in the folder `C:\BC-Meridian Vaults\Backup`. The backup information about the vault is shown in **Information about this backup**.

   This file will cause the vault to be restored to its original location. To restore a vault to a different location, see Move a Hypertrieve Vault.

8. Click **Next**.

   The **Completing the Restart After Restore From Backup Wizard** page appears.

9. Confirm the backup information is correct.

10. Click **Finish**.

    The time required to restore a vault depends on the size of the vault and the database engine used. A message will appear when restoration is complete.

Restore a Vault with a Command Line

To restore a vault from a backup with a command line:

- Run the program `AMRestor.exe` with the following syntax where *<BackupFolder>* is the location of the files created by the **Prepare for Backup Wizard**.

```
AMRestor.exe ["M:<ServerName>"] "<BackupFolder>"
```

By default, the program is located in the folder `C:\Program Files\BC-Meridian\Program`.

Change Operating System Versions

Vaults are not compatible with changes of the Windows operating system version running on the Meridian server. This issue affects server operating system upgrades and downgrades as well as vaults moved or restored to a new server with a different operating system version. The reason is that the Windows API sorting functions that support National Language Support (NLS) change between each Windows version.

When an old (prior to 2008a SP1) Meridian vault is upgraded to a newer version on the same operating system version, the existing vaults are not visible because they lack the operating system version and NLS version information that is stored in vaults as described below. In that case, the tool described below can be used with its `update` option to add the information to the vault. The tool can also be used to verify vault compatibility with the current operating system with the `verify` option. Use the `update` option of this tool only if the Meridian software has been upgraded to version 2008a SP1 or later and the operating system version has not changed.

> **Important!**
> In the preceding scenario, the tool will not upgrade a vault created on one Windows version so that it can be opened or restored on a different Windows version without serious damage occurring.

Vaults created by newer versions of Meridian (version 2008a SP1 and later) are also affected by this issue but the operating system version and NLS version information are stored in the vault and a check of this information is performed in the software that will prevent the vault from opening on a different operating system unless the vault is properly reindexed as described below.

There are only two ways to safely transfer an existing vault from a computer running one Windows version to another version:

- Import the vault from the computer running the first operating system into a new vault on the computer running the second operating system. After import, no further action is necessary.
- Reindex the vault on the second operating system with the `icosnlsver` tool described below.

Reindex a vault

To reindex a vault, perform the following tasks in the order listed:

1. Run the **Vault Consistency Wizard** on the vault on the old server (for example, Windows Server 2003) as described in Run the Vault Consistency Wizard.

   Enable only the **Check only**, **String domain**, and **Name domain** options.
2. If any inconsistencies are detected, run the **Vault Consistency Wizard** again with the **Check**, **Repair**, and **Compact** options selected and all **Analysis** options selected.
3. Restore a vault backup made on the old server to the new server (for example, Windows Server 2008).

   An error will occur and the vault cannot be opened.
4. Run the `icosnlsver` tool with the `reindex` command-line parameter on the new server and specify the datastore name to repair.

   The tool will either repair the inconsistencies or report additional problems that may require manual repair, in which case you should contact Accruent Technical Support or your Certified Partner for assistance.

   > **Important!**
   > Test the results of using this tool on a copy of production vaults before use. Only run this tool when the vault is not open by any users. Running this tool as a user other than an administrator of the computer can result in errors if the vault is hosted in SQL Server.

   The procedures for running the `icosnlsver` tool appear below.

Run the icosnlsver tool

To run the `icosnlsver` tool:

1. Ensure no users are connected to the Meridian server.
2. Open a **Command Prompt** window as an administrator in the folder that contains the tool. By default, it is installed in `C:\Program Files\BC-Meridian\Program`.
3. Run the tool using the syntax:

   `icosnlsver [downgrade|reindex|update|verify] <DatastoreName>`

   The available parameters are described in the following table. The results of the tool will display in the Command Prompt window.

Icosnlsver command-line parameters

Option	Description
None	Shows usage information.
`downgrade`	Clears the OS and NLS version information in the vault and resets its version to be compatible with Meridian versions prior to 2008aSP1.
`reindex`	Rebuilds the string domain and name domain indexes in the vault using the sorting order of the current operating system.
`update`	Updates the OS and NLS version information in the vault to be compatible with the current operating system version.
`verify`	Verifies that the OS and NLS version information in the vault is compatible with the current operating system version.
<DatastoreName>	The name of the datastore containing the vault to use. In most cases, the names are the same. The name can be found in the `datastore.ini` file that is used to restore the backup. You do not need to specify the path to the vault files.

Important!
After using this tool to modify an existing vault, run the **Prepare for Backup Wizard** on the vault before putting the vault into production use. Failure to do so leaves a snapshot of the unmodified vault that will be restored in the event of an unexpected termination of the EDM Server service before the next snapshot is created automatically. If the old snapshot is restored, all work performed in the modified vault will be lost. For more information on configuring automatic snapshot creation, see Prepare For Backups.

Following are descriptions of the most likely error codes that could be returned.

Icosnlsver error codes

Code	Description	Solution
0x12f (303)	The vault has errors.	Run the **Vault Consistency Wizard** and repair all errors before trying to reindex again.
0x66 (102)	The vault is corrupt.	Restore the vault from backup before trying to reindex again.
0x6c (108)	The vault is too old, its internal version is <= 9.	Run the **Vault Consistency Wizard** before trying reindex again.

Code	Description	Solution
0x0f (15)	The vault has too many properties.	Set the **AllowMaxProperties** value described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Hypertrieve to **1** and restore the vault from backup.
0x80 (128)	One or more database files are not accessible.	The user account that is used to run the tool should be privileged enough to access the database files.
0x85 (133)	One or more database files are locked.	Disable and stop the AutoManager EDM Server service, make sure there is no second instance of the tool running.
N/A	File or module not found	There is no database engine module installed or the 32-bit tool is launched on a 64-bit platform (or vice versa).

Create a Recovery Log

A recovery log allows you to export the latest revisions of documents or renditions from their streams folders to a location of your choice outside the vault in the event that the vault is unavailable. The documents can then be used normally until they can be replaced in the vault. Recovery logs should be created on a regular basis by a scheduled task similar to preparing backup files.

Important!
If errors occur during the creation of a recovery log, the log will contain error messages. An entry will also be added to the Windows Application event log with the number and types of errors that occurred and the path of the recovery log file. You should monitor the Application event log for such entries and resolve all errors found in the recovery log to ensure that the vault can be completely recovered in the case of an emergency.

Best Practices

Review the following best practices for the Recovery Log:

- Run the **Create Recovery Log Wizard** once with **Incremental recovery log** cleared to schedule creation of a full recovery log task (meaning, containing entries for every document in the vault) to run each weekend.

  Run the **Create Recovery Log Wizard** a second time with **Incremental recovery log** enabled to schedule creation of an incremental recovery log nightly, meaning, containing only entries for documents created that day.

  The weekend will allow more time for the full recovery log task to complete, which might be difficult to schedule without conflicting with other nightly administrative tasks. Nightly incremental recovery logs will complete quickly, making it easier to coordinate with other nightly tasks.

  To further safeguard vault documents, also schedule a recovery log task to run at mid-day when the vault is least busy, reducing the number of documents at risk to those created in one half day.
- If non-Latin characters are used in the names of documents in Meridian, add the Windows Locale corresponding to the national language on the server or workstation on which the recovery log is created. This is required to add the document names to recovery log with the correct characters.

Recovery Log Wizard

To create a recovery log with the **Create Recovery Log Wizard**:

1. In the Meridian Enterprise Administrator, click **EDM Server** in the left pane.

   The active vaults are listed in the right pane.
2. Select the vault in the right pane for which you want to create a recovery log.
3. From the **Action** menu, point to **All Tasks** and select **Create Recovery Log Wizard**.

   The **Create Recovery Log Wizard** appears.
4. Click **Next**.

   The **Select Vault** page appears.
5. Click options or type values using the descriptions in the following table.

   Recovery log options

Option	Command Line Parameter	Description
Select the vault for which a recovery log will be created	<*VaultName*>	Click **Browse** and select the vault to create a recovery log for.
Create rendition log	/RENDITIONS	Select this option to create a recovery log for the document renditions only. Clear this option to create a recovery log of the document native files only.
Incremental recovery log	/INCREMENTAL	Select this option to create a recovery log of only the documents that have been added to the vault since the last recovery log was created. Clear this option if this is the first time a recovery log has been created for this vault or to create a new, complete recovery log.

6. Click **Next**.

   The **Specify Recovery Log Location** page appears.
7. Choose between two options:

- Type a path and file name.
- To choose a location:
    a. Click **Browse**.
    b. Select a path.
    c. Type a file name to store the recovery log.
    d. Click **Save**.

Select the vault's `Backup` folder so that the recovery logs will be backed up along with the vault backup files.

Give the recovery log a descriptive name, such as `MyVault Full Recovery Log.bat`. When creating incremental recovery logs, use a name such as `MyVault Incremental Recovery Log.bat`. These names will make identifying the logs easier.

8. Click **Next**.

   The **When to Create Recovery Log** page appears.

9. Choose between two options:
    - Select **Now** to create the recovery log immediately upon finishing the wizard.
    - To schedule a job to run at a later time:
        a. Select **Later**.
        b. Type a user ID and password for the job to run as.

           We recommend that you specify a user account with a password that never expires. If the user account is removed or the password either expires or is changed, the scheduled task will fail and recovery logs will not be created.
        c. Click **OK**.
        d. Click **Set Schedule** to modify the job's schedule in the new dialog that appears.

           By default, the job will be repeated daily at the current time.
        e. Select options on the **Schedule** page to coordinate the job with other tasks running on the computer and the time when regular system backups occur.
        f. Click **OK**.

           A new job is created for the Windows Task Scheduler that may be modified with the normal Windows administration tools. For more information about Task Scheduler, refer to the Windows documentation.

10. Click **Next**.

    The **Configure Recovery Log Cleanup** page appears.

11. Click options or type values using the descriptions in the following table.

Recovery log cleanup options

Option	Command Line Parameter	Description
Do not automatically remove old log files		All existing incremental recover log files are retained when the program runs.
Automatically remove log files older than	/DAYSTOKEEP=n	Existing incremental recovery log files older than the number of days specified for `n` are purged.

12. Click **Next**.

    The **Completing the Create Recovery Log Wizard** page appears.

13. Click **Finish**.

    The recovery log is created immediately or at the scheduled time.

Create a Recovery Log with a Command Line

To create a recovery log with a command line:

- Run the program `AMRecLog.exe` with the following syntax and the parameters described in the preceding tables.

  ```
  AMRecLog.exe ["M:<ServerName>"] "<VaultName>" "<RecoveryLogfile name>" [/INCREMENTAL] [/DAYSTOKEEP=n]] [/RENDITIONS]
  ```

  The parameter names are case-sensitive and must be specified in upper case.

  By default, the program is located in the folder `C:\Program Files\BC-Meridian\Program`.

Recover Documents

Documents can be recovered from a vault that is unavailable by executing some or all of a recovery log created by the **Create Recovery Log Wizard**. Executing a recovery log exports the latest revisions of documents or renditions from their streams folders to a location of your choice outside the vault. The documents can then be used normally until they can be replaced in the vault.

The following task describes how to recover document files that exist in the stream folders where they were managed by Meridian Enterprise. To recover files from stream folders copied to backup media, they must first be restored to disk in the original location and then this task must be used to recover the document files to another location with their original file names.

Recover All Documents in Vault

To recover all of the document files in an entire vault:

- Locate and run the most recent full recovery log file.

  If incremental recovery log files also exist, run each file in the order in which they were created.

Recover Individual Documents in Vault

To recover individual document files from a vault:

1. Determine which recovery log file contains information about the files you want to recover.

   Compare the dates of the recovery log files with the date that the files were added to the vault (if known). If the files are known to exist in the vault prior to the earliest recovery log file, choose that recovery log file. Otherwise, choose the first recovery log file that was created after the files were added to the vault. If the dates that the files were added to the vault are unknown, begin with the earliest recovery log file and repeat this procedure with each recovery log file until the files are successfully recovered.

   If the files that you want to recover were added to the vault after the last recovery log was created, the files cannot be recovered until the vault is operational again.
2. On the Meridian application server, open a command-line window.
3. Make the folder containing the Meridian executables the current folder.

   By default, they are located in the folder `C:\Program Files\BC-Meridian\Program`.

4. Create an environment variable named **RECOVERDIR** and set it to the folder name where you want the files recovered, as in the following example:

   ```
   Set RECOVERDIR=C:\Temp
   ```

   Leave the command-line window open.

5. On the Meridian application server, open the recovery log file in a text editor.
6. Search the file for the file name of the first document that you want to recover (for example, `B9823 Specification.doc`).

   You should find a line in the recovery log file similar to the following example:

   ```
   AMRecover %recoverdir% "\\?\C:\BC-
   Vaults\Demo\Mechanical\8FA0\546EE97A\40A311D6\7295C800\CONT.3D2" "\*" "\Projects\2002\Universal
   Joint\0564-02-0001\B9823 Specification.doc
   ```

   The stream file names of renditions are REND instead of CONT. The file names of recovered renditions have the text **Rendition** appended to them, for example, B9823 Specification.doc.Rendition. The format of the recovered rendition file is the same as when the rendition was created (for example, PDF) even though this is not reflected in the file name or extension.

7. Copy the entire line to the Clipboard.
8. Paste the copied line at the command prompt.
9. Run the command.

   The stream file is recovered to the folder name specified by the RECOVERDIR environment variable. The vault path of the file is re-created in this folder. If the document was in a workflow in the vault at the time that the recovery log was created, the vault path that is created begins with a folder named the same as the user ID of the user to whom the document was assigned.

10. Repeat steps 6 through 9 for each file you want to recover.

Recover Prior Revisions From Backup

Under rare circumstances, it might be necessary to restore from backup a document file that has since been modified in the Meridian vault. Examples of such circumstances include:

- The vault is configured to not retain history. A prior revision of a document may be recovered by restoring older stream files that were copied to backup media before the latest revision was released.
- A document was accidentally deleted and purged. The document may be recovered by restoring stream files that were copied to backup media before the document was purged.

If a document is simply deleted in the vault and not purged, it can be recovered with the **Undelete** command as described in *Delete And Undelete Documents And Folders* in the *Meridian Enterprise User's Guide*.

To recover a prior revision from backup:

1. Determine the stream file name of the document that you want to recover. This can be done in one of two ways:
   - Search a recovery log file for the document name:
     a. On the Meridian application server, open the recovery log file in a text editor.
     b. Search the file for the file name of the document that you want to recover (for example, `B9823 Specification.doc`).

        The stream file to recover is the first file in the line containing the document name, similar to the following example:

        ```
        AMRecover %recoverdir% "\\?\C:\BC-Meridian
        Vaults\Demo\Mechanical\8FA0\546EE97A\40A311D6\7295C800\
        CONT.3D2"
        "\*" "\Projects\2002\Universal Joint\0564-02-0001\B9823
        Specification.doc"
        ```

        In this example, the stream file to recover is `C:\BC-Meridian Vaults\Demo\Mechanical\8FA0\546EE97A\40A311D6\7295C800\CONT.3D2`.
   - Find the value of the **Content** property of the document in the vault:

a. Find the document in the vault.

b. Click the document icon on the **Document** tab in PowerUser.

   The **Advanced Document Information** dialog box appears on which the **Content** property can be found.

   You must have the **Advanced Document Properties** privilege in the vault in order to view this dialog.

2. Find the stream file in your backup media.

   The file to recover must be dated prior to the date that the file was overwritten or purged in the Meridian vault.

3. Restore the file from the backup media using the software that was used to create the backup.

   The file can be restored to its original location or to an alternative location (recommended) where it can be examined for the correct contents.

Archive Documents

Meridian allows archiving of documents and metadata to a location outside of the vault. The files can then be copied to an offline media or imported into a different system.

Archiving documents can be useful:

- To create long-term storage copies of completed projects for future reference or auditing purposes
- To remove old revisions of documents that are no longer required
- To reclaim disk space occupied by unused documents. However, the database size will not change appreciably after archiving.

Archiving is performed by the **Vault Archive Wizard** in the Meridian Enterprise Administrator. The wizard gives you control over:

- Which documents are archived.
- Where to create the archive files.
- Which of several standard formats in which to store the metadata.
- Which revisions are archived.
- What data is removed from the vault for archived documents, if any.
- When the archive process will occur, immediately or at a scheduled time.

The following topics describe how to archive documents and the various options available.

Run the Vault Archive Wizard

The **Vault Archive Wizard** should be run on the Meridian application server for the best performance.

If a scheduled task will be created for archiving, it will be helpful to know when other tasks are scheduled on the same computer so that this task can be scheduled to not interfere with those processes and vice versa.

We recommend that this task be scheduled to occur after the day's Prepare for Backup, recovery log, and regular system backups occur. Archiving can require considerable system resources depending on the options chosen and should be scheduled to not occur during production hours.

To run the **Vault Archive Wizard**:

1. Open the Administrator tool and select **EDM Server** in the left pane.

   The list of active vaults appears in the right pane.
2. Select the vault containing the documents that you want to archive in the right pane.
3. On the **Action** menu, point to **All Tasks** and select **Vault Archive Wizard**.

   The **Vault Archive Wizard** appears.
4. Click **Next**.

   The **What to Archive** page appears.
5. For **Select a vault to archive**, select the vault name containing the documents that you want to archive from the list or click **Browse** and select a vault.
6. For **Select the folder within the vault to archive**, click **Browse** and select the folder containing the documents that you want to archive.

   All subfolders of the chosen folder will also be archived.
7. Click **Next**.

   The **Archive Location** page appears.
8. For **Create the archive in folder**, click **Browse** and select a destination folder for the archive files.

   The document files and subfolders will be exported to this folder as described in Vault Archive Wizard Results.

9. For **Format of the archive database**, select a format for the archive database from the list.

   The properties of archived documents will be output in this format to the archive location. The file will be named the same as the vault, for example, `<VaultName>.xls` if the Excel format is selected.

   - If the Excel format is desired, Microsoft Excel 64-bit must be installed on the server.
   - The names of the properties to be archived can be selected in the Configurator tool as described in *Configure Column Layouts* in the *Meridian Enterprise Configuration Guide*.

10. Click **Next**.

    The **Archiving Options** page appears.

11. Select an option to specify which revisions to archive using the descriptions in the following table.

    If the chosen folder has been archived before, the date and time it was last archived will also be shown for reference.

12. Click **Next**.

    A second **Archiving Options** page appears.

13. Specify what data, if any, you want to remove from the vault after the archive has completed.

    Select an option using the descriptions in the following table.

    New revisions currently in workflows are not archived by the **Vault Archive Wizard**.

14. Click **Next**.

    A third **Archiving Options** page appears.

15. Specify what additional data to include in the archive using the descriptions in the following table.

Options

Option Type	Option	Description
Revisions	Archive (export) the current revision of the documents	Archives only the latest released revision of the documents residing in the selected folder and its sub-folders. Prior revisions are not exported.

Option Type	Option	Description
Revisions	Archive all outdated revisions of the documents	Archives all but the latest released revision of the documents residing in the selected folder and its sub-folders. New revisions currently in workflows are not exported.
Revisions	Number of revisions to keep	Select the number of most recent revisions to omit. All prior revisions will be archived. For example, selecting **3** will omit the most recent three revisions of each document in the vault and archive all prior revisions.
Revisions	Age in days of revisions to keep	Select a number of days within which to skip all revisions that were released during that period. All revisions released prior to that period will be archived. For example, selecting 365 will archive all revisions more than one year old.
Revisions	Archive both in-progress current and older revisions of the documents	Includes the latest released revision and all prior revisions in the archive database.
Archived document removal	Completely remove archived revisions from database	Removes both the vault database record, including all revisions, properties, redlines, and history; and removes all stream files. Only use this option if you are confident the archive operation will succeed and produce the results you require.
Archived document removal	Only remove the document content of archived revisions	Removes only the document stream file and leaves the metadata record in the database. This option is useful for reducing disk storage space consumed by large files while keeping the database record available for searches and references. To restore the document content at a later date, drag the archived stream file from the archive location, drop it onto the document in the vault, and select the **Replace Content** option.
Archived document removal	Don't remove any information	Leaves the metadata and stream files intact. This option is useful for exporting large folders from the vault for sending to other sites, vendors, contractors, or systems while maintaining the existing information. We recommend that you use this option while practicing archiving procedures and refining the output property set configuration before selecting one of the other options.

Option Type	Option	Description
Additional data	Do not copy content, only include stream locations	Excludes document files from the export but includes their vault paths in a column in the archive database.
Additional data	Include project/folder properties and their hierarchy	Includes folder properties in the archive database.
Additional data	Include reference information	Includes the Meridian reference data for each document in the archive database.

16. Click **Next**.

    The **When to Archive** page appears.

17. Choose between two options:

    - Select **Now** to create the archive files immediately upon finishing the wizard.
    - To schedule a job to run at a later time:

        a. Select **Later**.

        b. Type a user ID and password for the job to run as and click **OK**.

        By default, the job will be repeated daily at the current time.

        We recommend that you specify a user account with a password that never expires. If the user account is removed, or the password either expires or is changed, the scheduled task will fail and archive files will not be created.

        c. Click **Set Schedule** to modify the job's schedule in the new dialog that appears.

        Select options on the **Schedule** page to coordinate the job with other tasks running on the computer and the time when regular system backups occur.

        d. Click **OK**.

        A new job is created for the Windows Task Scheduler that may be modified with the normal Windows administration tools. For more information about Task Scheduler, refer to the Windows documentation.

18. Click **Next**.

    The **Completing the Archive Wizard** page appears.

19. Click **Finish**.

The archive files are created immediately or at the scheduled time. If any documents could not be archived, a warning is shown that errors may be found in the archive log file described in Vault Archive Wizard Results.

Vault Archive Wizard Results

After the **Vault Archive Wizard** has completed, a number of files and sub-folders will have been created in the output folder that you selected:

- **Documents**: Archive copies of the documents residing in the selected vault source folder.
- **Sub-folders**: If no prior revisions were archived, the sub-folder structure of the archive source folder is reproduced to contain archived copies of each sub-folder's contents.

If prior revisions of documents were archived, sub-folders with names containing year and month numbers are created and contain sub-folders with names containing date numbers. These dates are the dates that one or more revisions were started (not released).

The files in these folders have the source document names appended with **.Rev X** where **X** is the revision number that was started on the date indicated by the folder names. Thus, the prior revisions for any particular document do not reside all in one folder, but may reside in several folders, each named for the start date of the corresponding revision.

- *<VaultName>*.ini: A mapping of vault property names to exported field names. Not all of the vault property names are valid for all of the available output formats so the field names are simplified to Field_0, Field_1, and so on.
- *<VaultName>*.log: A log of all archive activity performed. Review this file for errors if documents or metadata are missing.
- *<VaultName>*.met: A vault configuration file is generated so that the vault that was the source of the archived documents may be re-created, if necessary.
- *<VaultName >.<FileExtension>*: Document property data file of the archived documents in the format selected in the **Vault Archive Wizard**. The properties included in this file are specified in Configurator. Cross-reference these names with the vault property names listed in the **[AMFieldMap]** section in *<VaultName>*.ini.
- *<VaultName>*.reference.*<FileExtension>*: Reference property data file of the archived documents in the format selected in the **Vault Archive Wizard**.
- *<VaultName>*.folder.*<FileExtension>*: Folder property data file of the archived documents in the format selected in the **Vault Archive Wizard**. Cross-reference these names with the vault property names listed in the **[AMFieldMap2]** section in *<VaultName>*.ini.

Content Indexing

Meridian Enterprise features full-text searching of vault documents and memo properties by the various Meridian client applications. This makes finding documents extremely easy and versatile. The feature uses the Windows Search service that is included with the Windows operating systems and relies on IFilters provided by Microsoft and other software companies. The IFilters are necessary to extract the readable text from the different file formats that are stored in the vault. A specific IFilter is required fore each file type that you want to be searchable in Meridian. No configuration of the Meridian clients is necessary to enable full-text searching, it is detected automatically.

If your Meridian application server uses the Windows Search service, that service detects document changes and manages the text extraction and indexing process automatically and the configuration is simpler. If your server uses the older Indexing Service, it does not perform text extraction automatically and so this must be configured separately. Meridian provides a program named AMFTFilter to perform the extraction and that can be scheduled as a Windows task to keep the content indexes up to date with the latest document changes. AMFTFilter is not necessary with the Windows Search service.

AMFTFilter stores the extracted text in XML files with the file extension `.ami` in a duplicate folder structure to the document content files. By default, these folders and files are located at `C:\BC-Meridian Vaults\<Vault Name>\fti`. These files are then indexed by the server into a specific catalog for each vault. After the initial indexing is done, the AMFTFilter program can be scheduled to run periodically to update the catalog with new or changed document text.

The following table is a checklist for confirming that the related tasks of configuring content indexing have been performed. The tasks are listed in the order in which they should be performed. Use the hyperlinks in the checklist to find the configuration information for each task. Track your progress by printing this checklist and placing a check mark in the **Done** column as you finish each task.

Content indexing configuration checklist

Done	Task	Topic References
	Select the **Windows Search integration** or the **BC Indexing Search** component during Meridian server installation. Only the component that is compatible with your server is available for selection.	Install the Server Components
	Confirm that the content indexing service of the operating system (Windows Search or Indexing Service) has been installed on the server and is working.	Meridian Servers

Done	Task	Topic References
	In Windows Server Manager, temporarily stop and disable whichever service is used while you perform the IFilter configuration steps.	See the documentation for your version of Windows.
	Install any IFilters that you require.	See the documentation for the IFilter.
	In Windows Server Manager, enable and start the content indexing service that you stopped previously.	See the documentation for your version of Windows.
	Configure content indexing for each vault that requires full-text search functionality.	Configure Content Indexing
	In the **Indexing Options** applet of Windows Control Panel, enable indexing of the file types that require full-text search functionality.	See the documentation for your version of Windows.
	In the **Indexing Options** applet of Windows Control Panel, rebuild the content indexes.	See the documentation for your version of Windows.
	Restart the Meridian server.	See the documentation for your version of Windows.
	In Windows Explorer, test that the IFilters are working correctly by searching for text in one of the file types that you configured. The results of this test are the same as you can expect in Meridian Enterprise.	See the documentation for your version of Windows.
	If full-text searches do not produce results, repair the installation.	Troubleshoot Content Indexing

This checklist is not necessarily complete for every deployment scenario. Additional tasks may be required depending on your requirements and system configuration.

Configure Content Indexing

Content indexing is configurable on a per-vault basis. This task assumes that the vault will use the Windows content indexing component that is running on the Meridian application server. For other deployment options, see Deployment Strategies.

Notes about functionality

- If a scheduled task will be created for maintaining content indexing, it's helpful to know when other tasks are scheduled on the same computer so that this task can be scheduled to not interfere with those processes. We recommend that this task be scheduled to occur after the day's Prepare for Backup, recovery log, and regular system backup tasks occur.
- Content index files can be re-created relatively easily in the case of loss and do not need to be backed up.
- Although the Windows content indexing components run at a lower priority than other applications on the server and can be run during production hours, we recommend that they be scheduled to not run during production hours in order to maximize Meridian performance.
- After upgrading to Windows Server 2016 from a prior operating system version:
    1. Disable vault content indexing as described in this topic.
    2. Use Windows Control Panel to rebuild the Windows Search indexes.
    3. Restart vault content indexing.
- Text searching from the Meridian client applications may be performed after the catalog is complete and available.
- If the vault content files are located on a device other than the Meridian Enterprise application server (for example, a SAN device or file server), the filtered text files must reside on the same server as the indexing service or they will not be added to the indexing catalog. To accomplish this, set the **FullTextInLocalDataPath** registry value described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores.
- If a vault has a name longer than 40 characters, the corresponding catalog name will be abbreviated. The Indexing Service does not allow catalogs to have names longer than 40 characters. If you want to set a different catalog name than the default, set the **FullTextCatalog** registry value described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<vaultname>.

- To disable content indexing, clear the **Enable content indexing for documents and memos** option, remove the existing catalog, and delete the filtered text files.
- The full-text indexes that are used by Meridian Enterprise are subject to any limitations of the full-text search capabilities of the database management system in which the vault is stored. Following are examples of known limitations with Microsoft SQL Server:
  - Searching for document names that contain only numbers will yield no results.
  - Searching for terms that include numbers will not find plain text files.
  - Searching for single-digit numbers in AutoCAD drawings will yield no results.

Manage IFilters

You can add specific **ClassIDs** to the Meridian indexing service configuration to enable full-text indexing for Office documents and other formats. This provides greater flexibility for indexing in your specific environment, including support for Windows Server 2022 IFilters.

Due to technical restrictions in the **Windows Search Indexer**, a Meridian DLL must be patched with these **ClassIDs** to integrate with Windows Search. If you need to add **ClassIDs** to solve indexing issues or support new formats, contact Accruent Support for assistance with this configuration.

Procedures

To configure content indexing for a vault:

1. Open the Meridian Enterprise Administrator and click **EDM Server** in the left pane.

   The list of active vaults appears in the right pane.
2. Select the vault that you want to configure in the right pane.
3. On the **Action** menu, select **Properties**.

   The vault's **Properties** dialog box appears.
4. Click the **Content Indexing** tab.

   The **Content Indexing** page appears.
5. Select **Enable content indexing for documents and memos**.

   If the server uses Windows Search, content indexing will be enabled and begin if you click **Apply** or **OK**. However, if the server uses the Indexing Service, the initial filtered text files and indexing catalog will not be created until the task is run manually or on a schedule.
6. Select the appropriate content indexing option for your server: **Use Windows Search** or **Use Indexing Service**.

   If you selected **Use Indexing Service**:

a. Click **Set Schedule** to schedule a task to create and maintain the indexing catalog after production hours.

b. Type a user account name and password for the job to run as and click **OK**.

   For information on the security permissions that are required for the account, see Index Securely. The **Meridian Vault Indexing Task** dialog box appears.

c. Select options on the **Schedule** page to coordinate the job with other tasks running on the computer and the time when regular system backups occur.

d. Click **OK**.

   A new job is created for the Windows Task Scheduler that may be modified with the normal Windows administration tools. For more information about Task Scheduler, refer to the Windows documentation.

7. To clear the date that the content indexing catalog was last updated so that a new catalog will be built, click the **Clear** button.

   For example, if you may want to do this after restoring a vault, refer to Restore a Vault That Has Been Indexed.

8. Click **OK**.

Build and Maintain a Content Index

If your Meridian server uses the Indexing Service instead of Windows Search, a content index is created the first time AMFTFilter processes a vault. The index is updated with new and changed documents each time AMFTFilter runs thereafter. If you created a scheduled task for the vault when you configured content indexing as described in Configure Content Indexing, the task will maintain the index.

However, if this is an existing vault containing many documents, building a new catalog may take a long time. Depending on the server hardware, the type of files being indexed, and the IFilter used, it will take approximately one hour to index every 10,000 documents. This might require more time than is available between the time the scheduled task starts and production vault access next begins. This means that the search catalog will still be processing, impairing the performance of the Meridian application server and, conversely, any production activity will impair the performance of catalog processing, thus delaying its completion. Therefore, we recommend that you build the new catalog when there will be plenty of time for the catalog to process before production hours begin, for example, during a weekend.

To build a content index:

1. When you want the process to begin, open **Task Scheduler** in the **Administrative Tools** folder of **Control Panel**.
2. Right-click the scheduled indexing task for the catalog and choose **Run**.

   The task will start if the account under which the task is run can be authenticated.

Accelerate Content Index Creation

To accelerate the creation of a new content index catalog, you can temporarily increase the priority of the Indexing Service (`cisvc.exe` and one `cidaemon.exe` process per vault) or Windows Search (`SearchIndexer.exe`).

You must have administrative permissions on the computer to perform this procedure.

To increase the priority of a process:

1. Open Windows Task Manager and click the **Processes** tab.

   The list of active processes appears.

2. Right-click the process name to accelerate, point to **Set Priority**, and select **Realtime**.

   This will cause the processes to run at the same priority as normal applications, greatly reducing the time required to build content indexes. Raising the priority of other processes will adversely affect Meridian performance and should only be done after production hours.

3. When the catalog is complete, restore the process priorities to resume normal operation.

Filter Out Text Noise

Some words are not useful for full-text searching, for example, single-letter words such as “a”, numbers, and common words such as “the” and “and.” Windows Search and the Indexing Service feature a configurable “noise” blacklist. This is a text file containing words or strings that will be excluded from searches performed by users.

By modifying this file, you can control how users search in the vault and prevent them from creating search queries that will return a lot of results, which may in turn result in poor server performance.

To view or modify the noise blacklist file:

1. On the Meridian server that is running the indexing service, navigate to `C:\Windows\System32`.
2. Look for a file named `noise.dat` or `noise.<LanguageAbbreviation>` where *<LanguageAbbreviation>* matches the correct language for the text to be filtered.

   There is a separate file for each supported language. For example, the English language file is named `noise.eng`.
3. Open the file in a text editor.
4. Add or remove words or strings and save the file.

Restore a Vault That Has Been Indexed

You may need to restore a vault that had content indexing enabled when the backup was made. If your Meridian server uses the Indexing Service instead of Windows Search, when you restore the vault, it is important to know that the scheduled task to run `AMFTFilter.exe` will not also be restored even though the **Enable content indexing for documents and memos** option will be enabled for the restored vault.

If the scheduled task does not already exist, you will need to re-create it as described in Configure Content Indexing. Also clear the **Last run** date as described in Configure Content Indexing. It is not necessary to restore the filtered text files (`*.ami`) or the indexing service catalog files located at `C:\BC-Meridian Vaults\<VaultName>\catalog.wci`.

Index Securely

If your Meridian server uses the Indexing Service instead of Windows Search, then for the content index update task to succeed, it is critical that the user account used to run `AMFTFilter.exe` have access to all folders in the vault. If not, documents that reside in folders that `AMFTFilter.exe` cannot access will not be indexed and users will not be able to search on content in these folders. The user account must also have full access to the file system on the computer where `AMFTFilter.exe` runs. The program will copy the document content (stream) files to the local disk before it filters the files.

For these reasons, we recommend that you configure the task to run under the local SYSTEM account (no password required), which will filter all documents in the vault regardless of the vault security. If this is not permissible under your organization's security policy, choose an account that:

- Is a member of the local Administrators group
- Has read access to the vaults' stream folders located at `C:\BC-Meridian Vaults\<VaultName>`
- Full access to the file system on the computer where the `AMFTFilter.exe` is run.

We recommend that you specify a user account with a password that never expires. If the user account is removed, or the password either expires or is changed, the scheduled content index update task will fail, content index files will begin to age, and text searches will fail unexpectedly.

The **AMFTFilter** console window that is open when the program is running and that shows the filtering progress will not be visible if you are logged on to the computer with one account but AMFTFilter is running as a different account name. The only way to see that AMFTFilter is running in this situation is to open Task Manager, enable **Show processes from all users** on the **Processes** tab, and monitor the **AMFTFilter** process.

Troubleshoot Content Indexing

The following are solutions to common content indexing problems with Windows Search (not Indexing Service). These can be attempted after you have completed the configuration checklist in Content Indexing and you have allowed sufficient time for the search catalog to be built. If none of these solutions resolves your problem, contact Accruent Technical Support or your Accruent Partner.

Inconsistent Search Results

If full-text searches produce inconsistent results, you can try the following solution that adjusts the way the Meridian adds text to the content index catalog. Depending on the specific text in your documents, this solution might produce better results for very long documents or when searching for sub-strings in unique words. This solution optimizes results for technical limitations in Windows Search itself.

Set the Meridian word breaker mode

To set the Meridian Word Breaker mode:

1. Disable the content indexing service.
2. Create the following Windows registry key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
   Meridian\CurrentVersion\Content Indexing
   ```

3. Create a DWORD value named **ICEDM_WB_mode** in the key and set it to one of the values in the following table.
4. Close the Windows registry.
5. Restart the content indexing service.

Word breaker modes

Value	Description
0	Meridian does not generate the content indexes. Searches from within Meridian work the same as from Windows. This mode produces the smallest content index for each document but it does not support sub-string searches or fuzzy searches.

Value	Description
1	Meridian generates a **contains** operator content index only. Sub-string searches are not supported and the content index will be larger for each document, which can result in not all of the text in very long documents getting indexed.
2	Meridian generates an **exact** operator content index only. Fuzzy searches are not supported and **Contains** operator searches may not produce the desired results.
3	Meridian generates a combined **contains** and **exact** operator content index. This is the default mode and produces the largest content index for each document. All of the text in very long documents may not be indexed but **Contains** operator searches should produce some results.

No Search Results

If full-text searches do not produce any results, you can try the following solutions.

Reinstall Windows Search

To reinstall windows search:

1. In the Meridian Enterprise Administrator, disable the option **Enable content indexing for documents and memos** for all vaults.
2. Uninstall Windows Search.
3. Reboot the server.
4. Reinstall Windows Search.
5. Reboot the server, if necessary.
6. Repeat the steps in the configuration checklist in Content Indexing beginning with starting the content indexing service.

Verify the Windows registry values

To verify your windows registry values:

1. Disable the content indexing service.
2. Open the Windows registry to the following key:

   ```
   HKEY_LOCAL_
   MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex\Language
   ```

3. Locate the language sub-key under which Meridian was installed.

4. Add permission to the users for the key.
5. (Indexing Service only) Find the following key:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex`
6. Change the **MaxCharacterization** value from **0** to **140**.
7. Close the Windows registry.
8. Reboot the server.
9. Repeat the steps in the configuration checklist in Content Indexing beginning with starting the content indexing service.

Verify Windows Search Integration Component is Installed

Important!
We highly recommend that you perform a system backup before performing this task. For more information, see Backups And Recovery.

To verify the Windows Search Integration component is installed:

1. Verify that the content indexing service is enabled.
2. In Windows Control Panel, start the **Meridian Enterprise Server** setup program.
3. Select the **Modify** option and on the **Select Features** page, verify that the **Windows Search Integration** component is selected and installed.
4. Finish the wizard to apply any changes that you made or cancel it to keep the system as-is.
5. Repeat the steps in the configuration checklist in Content Indexing beginning with starting the content indexing service.

Repair the Meridian Enterprise Installation

Important!
We highly recommend that you perform a system backup before performing this task. For more information, see Backups And Recovery.

To repair the Meridian Enterprise installation:

1. Verify that the content indexing service is enabled.
2. In Windows Control Panel, start the **Meridian Enterprise Server** setup program.
3. Select the **Repair** option and finish the wizard.
4. Repeat the steps in the configuration checklist in Content Indexing beginning with starting the content indexing service.

Optimize Performance

How a Meridian system performs depends on many different factors. The following topics describe the most relevant factors and recommend configurations and settings for maximum performance of the Meridian application server and client computers.

> **Note:**
> For optimum performance with multiple large vaults or many smaller vaults, multiple Meridian application servers may be necessary. The settings and recommendations in the following topics that refer to the Meridian application server should be applied to each computer running the AutoManager EDM Server service.

Hypercache

> **Note:**
> The following applies to Meridian 64-bit editions when run on a Windows 64-bit operating system only.

Because the 64-bit platform provides a vastly larger memory address space and server computers with large amounts (16 GB or more) of physical memory are readily available and affordable, Meridian performance and scalability can be improved with an optimal configuration called HyperCache. HyperCache is the default configuration for the Meridian Enterprise 64-bit platform.

In the HyperCache configuration, vaults are loaded entirely into memory. This maximizes the performance of these vaults, which typically serve larger numbers of users and higher quantities of documents. The contents of the HyperCache are saved in Hypertrieve databases between service shutdowns and startups for the fastest possible loading. The vault contents are replicated to repositories hosted by SQL Server or Oracle where they can be accessed with the Meridian Explorer client or standard reporting tools such as SQL Reporting Server and Crystal Reports. For more information about this replication, see Data Library.

Performance tests in simulated customer environments have shown that HyperCache can improve performance significantly. Stress tests have shown that Meridian Enterprise 64-bit with HyperCache can manage 1.5 million documents (not counting revisions) and over 200 concurrent users while still providing good performance.

Earlier versions of Meridian Enterprise have been used mostly with up to 0.5 million documents (not counting revisions) and up to 100 concurrent users.

> **Note:**
> While these tests have been executed on hardware and software configurations that resemble typical customer environments, they are not representative of any particular customer environment. Therefore, in cases of more than 0.5 million documents (not counting revisions) and/or more than 100 concurrent users, we strongly recommend having the hardware and software configuration reviewed by Accruent or your Accruent Partner.

We recommend HyperCache configuration for all customers, but particularly for those with the following scenarios:

- Existing systems with performance or scalability problems.
- Customers planning to significantly expand their number of users or documents in the near future.

Implementing HyperCache requires:

- 64-bit CPU server computer
- Adequate physical memory (greater than the sum of the sizes of all vaults stored in Hypertrieve)
- Microsoft Windows Server 2008, 2012, 2016, or 2019 (partial support: no full-text search is available)
- Additional requirements as listed in Meridian Application Server Requirements
- Meridian Enterprise 2018 or higher
- No new system administration tasks

To calculate the amount of physical memory required for existing Hypertrieve vaults, add the size of all vault database files together and round up to the next largest memory configuration available for the server computer. To calculate this amount for existing SQL Server or Oracle vaults, add half the size of all vault database files and round up.

Hypertrieve example

Memory Pool	Size (MB)
Windows Server operating system	2000
Meridian services	200
Meridian user sessions (25 MB/user * 50 users)	1250
Work In Progress vault	266
As-Built vault	789
Archive vault	1584
Min. Server Memory	**6089**

Assuming the closest available memory configurations for the server are 6 GB and 8 GB, select the 8 GB configuration at a minimum.

SQL Server or Oracle example

Memory Pool	Size (MB)
Windows Server operating system	2000
Meridian services	200

Memory Pool	Size (MB)
Meridian user sessions (25 MB/user * 100 users)	2500
Work In Progress vault	1902/2=951
As-Built vault	3048/2=1524
Archive vault	6692/2=3346
Min. Server Memory	**10521**

Assuming the closest available memory configurations for the server are 8 GB and 12 GB, select the 12 GB configuration at a minimum.

Configuring HyperCache is described in the following topic.

Configure Hypercache

Configuring a Meridian Enterprise application server with HyperCache is quite easy.

> **Note:**
> When HyperCache is enabled, it overrides the **MaximumCacheSize**, and **RelativeCacheSize** settings.

To create a HyperCache configuration:

1. In the Meridian Enterprise Administrator, click **EDM Server** in the left pane.

   The active vaults are listed in the right pane.
2. Select the vault that you want to configure in the right pane.
3. On the **Action** menu, select **Properties**.

   The vault's **Properties** dialog box appears. Many of the options that are accessible from this dialog are the options that were set when the vault was created.
4. On the **Vault** tab, click the **Advanced** button.

   The **Advanced Vault Properties** dialog box appears.
5. Enable **Use HyperCache**.

   You may also set the vault's **HyperCache** registry value to **1** as described in:

   HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<vaultname>\CompoundItemService.

Optimize Server Hardware

Optimizing the Meridian application server hardware involves taking into account:

- The number of users
- The number of vaults on each server
- The number of documents in each vault
- The business processes used
- The database engine used: Hypertrieve, SQL Server, or Oracle
- Many other factors

All have an influence on the performance of the server. The following topics provide some general recommendations.

Dedicated Server

A Meridian application server can potentially use all of a server's hardware resources at one time. In reality, resource usage will vary during the day depending on the different actions taken by its users. Typically, usage is heaviest in the morning when work begins and again after the mid-day break. Actions like importing documents, executing large or complex searches, building reports, and more, may put a heavy workload on the server during these times. If the server is also used for other applications, the total system workload can rise until performance becomes unacceptable. A server dedicated to Meridian will be better able to handle these heavy workload periods and is therefore recommended.

Virtualization Software

Virtualization software such as VMware is designed to be transparent to the software that they host and not impose special requirements. However, Meridian systems deployed on virtual machines might have issues related to performance and communication with peripheral devices, other hardware components, networking, and security.

Regarding performance, running Meridian in a virtual environment is likely to result in increased CPU utilization or other hardware resource consumption. Because of this increase, total system workload capacity might be reduced and Meridian response times might increase. Considering this and assuming that the virtual machine is configured per Meridian requirements, Accruent supports deployments of all Meridian products on VMware, unless otherwise noted. However, in a virtual environment, Accruent might not be able to resolve issues related to system performance or issues that Accruent suspects are related to communication with peripheral devices and other hardware components such as network cards and disk controllers.

If Accruent suspects a particular issue is specific to virtualization technologies (such as performance or communication with peripheral and hardware components), Accruent might require that the customer reproduce the issue in a non-virtual configuration before Accruent Technical Support will assist in troubleshooting these issues. Due to the nature of virtualization technologies, Accruent cannot guarantee resolutions to issues that are caused because a deployment is virtualized. If virtualization technology is used in combination with our software, we require that this be mentioned when contacting support for assistance.

Additionally, it is the customer's responsibility to ensure that other associated third-party software is supported to run in the specified virtualized environment such as application servers, databases, and operating systems by the original vendor of that software. Because virtual environments use more computer resources than non-virtual environments, Accruent strongly recommends you gather baseline performance statistics from both types of environments and compare the results with a Accruent Solutions Partner or Accruent Technical Support before making any decisions about virtualized environments.

For the latest information about Accruent support for virtualization software, see the Operating Systems section of the *Supported Software* document for this release of Meridian.

CPU

The dominant factor affecting Meridian application server responsiveness, assuming that sufficient physical and virtual memory is available, is the server's CPU. Upgrading the CPU to a faster clock speed resolves most performance problems. However, it should not be considered a cure-all, and the other areas described in this guide should also be optimized for peak performance. When you are selecting a new Meridian application server computer, the fastest available CPU (one or more) provides the greatest value.

> **Note:**
> To determine if the server's CPU is limiting performance, monitor the **AMEDMW** instance of the **Process** object with Performance Monitor as described in Configuring the Windows Performance Monitor.

> **Note:**
> Consider using the multi-threaded database engines described in Hypertrieve Database Engine. We do not recommend setting the **Processor Affinity** of the Meridian service processes on multiprocessor servers, which can decrease overall performance. Windows symmetric multiprocessing performs better processor load balancing.

In environments where SQL Server or Oracle is used as the Meridian DBMS or multiple large Hypertrieve vaults are frequently accessed by users, it is possible to improve overall performance by hosting Meridian on a server with more processor cores. Although Meridian cannot directly take advantage of more than one core, due to Windows symmetric multiprocessing ability, Windows will assign SQL Server or Oracle processes to the other cores. Windows can also assign individual Meridian vault database engines to the other cores if the Meridian CopyDLL option is enabled as described in Configure the CopyDLL Setting. With system processes divided among the available processors, overall processing throughput is increased.

Physical Memory

Adequate physical memory also affects server responsiveness, but to a lesser degree than the CPU, and has a greater effect on the ability of a Meridian application server to handle large numbers of users and many documents.

The amount of total memory used by the Meridian EDM Server process depends primarily on the following factors:

- The number of simultaneous users connected to the server computer via the client software applications. On average, 12–25 MB of RAM will be used by each user, depending on the **ObjectsCacheDepth** setting (the number of objects to cache for each user) and the configuration of the vaults to which the users are connected (the number of objects required for users to perform their tasks). This memory contains navigation view data, collection data, search results data, and cached vault objects.
- The total of all **Maximum Cache Size** settings of all active vaults on the server computer. More vaults, even inactive ones, consume more memory. The **Maximum Cache Size** setting affects the amount of memory used for the database cache of each vault and therefore will affect the amount of memory consumed by the EDM Server process.

After a Meridian application server boots and all applications are loaded, there are only two memory pools that are variable in size, the user sessions pool and the database caches. Without enough physical memory for either of these, performance will begin to suffer. It is also at that point that virtual memory performance becomes a major factor, as described in Virtual Memory.

There are no size recommendations for these pools that apply to every configuration. Each limits the maximum size of the other. More users can be accommodated by fewer and smaller vaults, more and larger vaults can only accommodate fewer users. But the approximate size of each can be calculated with the following formulas:

- User sessions pool size = # users X 25 MB. This is an approximate maximum. The actual amount used is also determined by the **ObjectsCacheDepth** setting described in Configure the ObjectsCacheDepth Setting.
- Database caches pool size = The sum of the size of all vault caches as described in Configure the MaximumCacheSize Setting.

  Calculating the size of the cache for a vault that doesn't exist yet, is more complicated. The approximate size can be predicted by the following formula:

  Hypertrieve database file size = # documents X # avg. revisions per document X (# avg. properties per document X avg. property size)

Following is an example calculation:

50,000 documents X 3 avg. revisions per document X (75 avg. properties per document X 4 Bytes) = 45 MB

If the desired number of users and vaults cannot be accommodated with these constraints, you should consider moving other applications (for example, SQL Server) and services (for example, Task Server) to a different server to free up more memory.

For recommended configurations for various ranges of users and database sizes, see Deployment Strategies.

Disk Subsystems

Meridian does not require a particular disk subsystem type, the only requirement is that Windows supports the hardware and the account under which the EDM Server service is run can access the device. This means that Meridian can take advantage of disk storage space on a single local drive, multiple local drives, a separate file server, network attached storage (NAS) devices, or storage area network (SAN) devices. However, disk compression and data encryption are not recommended for Meridian.

Redundant array of inexpensive disks (RAID) systems are typically chosen primarily for data protection purposes and provide a minimal performance increase to Meridian. If you choose to use a software-based RAID system, the Meridian performance will most likely decrease. If you want to implement a RAID system, choose a hardware-based RAID system.

Optimize the Server Operating System

The way the operating system hosting Meridian is configured affects performance by allowing it to address larger amounts of physical memory and to lessen the processing overhead imposed on the CPU. The following topics describe recommended settings for optimizing an operating system for best Meridian performance.

Configure Application Response

The Windows operating systems can be configured to give higher priority to foreground applications versus background services with the **Application response** option. Because the Meridian application server programs run as background services, this option should always be set to give them the higher priority in order to maximize performance.

To configure the **Application response** option:

1. In Windows Explorer, right-click **Computer** and select **Properties**.
2. Click **Advanced system settings** in the **Task** list.

   The **System Properties** dialog box appears with the **Advanced** property page shown.
3. Click the **Settings** button in the **Performance** group.

   The **Performance Options** dialog box appears.
4. Click the **Advanced** tab.

   The **Processor scheduling** and **Virtual memory** options are shown.
5. Select **Background services**.
6. Click **OK**.

Virtual Memory

For the best performance, the Meridian application server needs to allocate sufficient memory for two purposes:

- A database cache for each active vault on the server
- Session data for each active user connected to a vault on the server.

If there is not sufficient physical memory for these purposes, together with all of the other applications running on the server, virtual memory is used to store the data temporarily on disk, which is much slower than physical memory and reduces system performance. This is why we recommend a server dedicated for use by Meridian as described in Dedicated Server.

To optimize virtual memory usage, there are several things you can do:

- Ensure that the Windows page file is large enough to meet the needs of all applications running on the server. We recommend that it be at least as large as the installed physical RAM on the server. We highly recommend that you assign the page file to a different drive than the drive where the Meridian vaults are located.
- Determine how much actual virtual memory is requested by Meridian by monitoring the **AMEDMW** instance of the **Virtual Bytes** counter of the **Process** object with Performance Monitor as described in Configuring the Windows Performance Monitor. Also monitor the **Available Mbytes** counter of the **Memory** object.
- If the amount of virtual memory used by Meridian approaches the amount of physical memory before the maximum expected number of users is reached, reduce the amount of memory allocated to database caches so that it can be used to accommodate more users.

  To adjust the database caches:

  1. Start using the system with a conservative number of users. Use Performance Monitor as described in step 2 to monitor the amount of virtual memory requested by Meridian during peak production hours.
  2. If **Available Mbytes** drops below 300 MB before the maximum virtual memory consumption is reached, reduce the **Maximum Cache Size**option of one or more vaults to free memory as described in Configure the MaximumCacheSize Setting.
  3. Monitor the amount of virtual memory used as additional users are allowed access to the system.
  4. Repeat steps a through c until all users are connected to vaults.

     If reducing the cache sizes causes the performance to become unacceptable, you should consider switching to a newer version or different edition of Windows Server, if possible, to access additional physical and virtual memory.

Note:
Restarting the AutoManager EDM Server service will free any unused virtual memory. If the virtual memory usage measured in step 2 cannot be lowered by reducing the cache sizes without adversely affecting performance, we recommend restarting the service after business hours, daily if necessary, as a last resort to providing additional virtual memory.

Multiple Network Adapters

If the Meridian application server is configured with multiple network adapters, it is considered a multi-homed server. There are several known issues with the DCOM protocol when used on a multi-homed server or client computer. Because the Meridian software uses the DCOM protocol extensively, it is important to configure the network adapter that the client computers will use as the first one in the server's network connections list. If it is not, users may experience a delay (by default, 30 seconds) induced by DCOM while Meridian waits for a response from the first network adapter. When no response is received, it attempts the next network connection in the list, and so on, until either a response is received or no response is received from all of the network connections. Making the correct adapter the first network connection prevents any delays.

The procedure for configuring the priority of network connections is different among the Windows operating systems. Refer to the Windows documentation for your version for specific instructions.

Multiple Network Protocols

If the Meridian application server is configured with multiple network protocols, the TCP/IP protocol should be the first one in the binding order for the network connection used by the Meridian application server computers. The only protocol the Meridian software uses to communicate with its clients is the TCP/IP protocol. Unused network protocols should be uninstalled from the Meridian application server.

Software Disk Compression

The disk subsystem used by Meridian should be as fast as possible. Third-party programs and Windows itself support compressing folder contents to save disk space. However, software disk compression adds overhead to the server CPUs that will reduce Meridian performance.

Overall bad performance can result if vault database files or streams are stored on a disk or in folders with software disk compression enabled or stored on a logical disk created with Windows disk striping (software RAID).

For best performance, do not use software compression of any kind on any of the Meridian database or streams folders, and do not locate the `BC-Meridian Vaults` folder on a Windows striped volume (software RAID).

Software Data Encryption

The disk subsystems used by Meridian should be as fast as possible. Third-party programs and Windows itself (BitLocker, for example) support data encryption for additional security. However, software data encryption adds overhead to the computer CPUs that will reduce Meridian performance. When Meridian application server security is properly configured as described elsewhere in this guide, direct access to the Meridian stream files (document content) is only permitted for server administrators, the same persons who would administer the data encryption software and have access to unencrypted files. Casual misuse of the Meridian stream files is also obstructed by the fact that the stream folders have 4- or 8-character hexadecimal names, for example, `3D0C` or `1FF20BD3`, and the document content files all use the same counterintuitive file name with variable 3-character hexadecimal file extensions, for example, `CONT.3D2`.

All other access to vault documents is only possible through authentication by the Meridian client software and application of the vault security roles. The same is true for the Meridian vault metadata stored in Hypertrieve, SQL Server, or Oracle. Therefore, software data encryption provides no useful additional security and should not be used on folders containing the Meridian database or stream files.

> **Note:**
> If Local Workspace is enabled, working copies of documents also reside there on the client computers and these principles and guidelines also apply.

Meridian is not routinely tested with software encryption products. However, if software data encryption is a system requirement, it can be accomplished by following these guidelines:

- Configure the EDM Server service to run under the same account as the account whose Encrypting File System (EFS) certificate is used to encrypt the files. Or vice versa: use the EFS certificate of the EDM Server service account to encrypt the files. Otherwise, security of the documents will not work correctly.
- Add the EFS certificates of any other accounts under which Meridian services or administrative applications access the files, for example, the tools in the Vault Consistency Toolkit, vault recovery tool, and so on. Otherwise, the documents may not be accessible, particularly in the case of a critical system failure.
- Exclude the vault database files from encryption. Rely on the security of the database management system instead.
- Ensure that passwords for the encryption accounts either are not changed or are updated immediately in the properties of the services that access the files.
- Back up the EFS certificates that are used to encrypt the files in a safe place. If a certificate is lost or becomes corrupted, access to documents will be lost.

Optimize the Meridian Server Software

Many aspects of Meridian performance can be altered by changing registry settings on the Meridian application server. Consider the following settings carefully and only make changes that you are confident may improve performance under your circumstances, or changes recommended by your Accruent Partner or a Accruent technical support representative. Document the changes you make in case they do not improve performance so that you can restore the original settings. If possible, test changes on a non-production server before implementing them in a production environment.

Not all of the following registry keys are created when Meridian is installed on the server. If a key does not exist, its default value is used. To modify the value, create the registry key and set the appropriate value. Unless otherwise specified, all registry keys mentioned in this document are of the type DWORD and the values for these keys are in decimal form.

Note:
After editing the registry, stop and restart the AutoManager EDM Server service for the setting to take effect.

Important!
Improper use or improper modification of the registry on a computer might lead to unwanted results and might even lead to a total stop of the server. If you do not feel comfortable with making changes to the registry, please contact someone who is or contact Accruent Support.

Configure the EDM Server Service

You can optimize some aspects of the **EDM Server** service, which manages the data for all vaults on the same server. Temporarily changing these settings is useful when performing special operations such as importing large quantities of documents or running the **Vault Consistency Wizard**.

To configure the **EDM Server** service:

1. In the Meridian Enterprise Administrator, select **EDM Server** in the left pane.
2. On the **Action** menu, select **Properties**.

   The **EDM Server Properties** dialog box appears.
3. Click the **Engine** tab.

   The service's options that can be configured in the Administrator tool appear. Other options can be configured by registry settings and are described elsewhere in this guide.
4. Click options or type values using the descriptions in the following table.
5. Restart the **EDM Server** service to make your changes take effect.

EDM Server service options

Option	Description
Performance	Select **Optimize for best multi-user performance** (default) for normal operation. Select **Optimize for best single-user performance** when performing server-intensive administration tasks after production hours when no users are connected to the server.
Security role assignments	Select an option from which to assign security roles in all vaults managed by this server. The options are listed in order of their impact on performance with those that have more negative effect on performance appearing at the top of the list. We recommend **Meridian groups** in environments where domain security authentication negatively effects performance such as large domains, multiple domains, or remote Primary Domain Controllers. **Note:** If the EDM Server Service is configured to use Meridian groups, the BC service account should either have a role with all privileges or use a backdoor account. This is required to allow full functionality with Tags.
<DatabaseEngine>SQL.dll	This option appears only if the SQL Server database driver is installed. For information on configuring this option, see Configure the SQL Server Account Used By Meridian.

Configure the BatchCallThreshold Setting

One user performing a large batch operation, such as submitting hundreds of documents or building a report based on thousands of documents, can seriously impact server responsiveness for other users. By default, such batch operations are pre-empted by the server after a configurable number of actions so that actions by other users may also be processed, which greatly improves multi-user responsiveness. The **BatchCallThreshold** setting determines the maximum number of actions allowed at one time. The default value is **500**.

If server performance degrades when users perform large batch operations and such operations are expected to continue, we recommend reducing this value in steps of 100 and monitoring the performance experienced by both the users performing the batch operations and other users until an acceptable compromise is reached. This setting should not be reduced below **200**.

The DWORD registry key to adjust the **BatchCallThreshold** setting is located at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
Meridian\CurrentVersion\Hypertrieve\BatchCallThreshold
```

Configure the ObjectsCacheDepth Setting

Some vault data that is retrieved by users is cached in server memory to accelerate subsequent accesses by the same user in the same session. This data includes Navigation views, collections, search results, and commonly used vault objects. The **ObjectsCacheDepth** setting determines how many objects per user are kept in memory and can have a significant effect on overall memory consumption and performance of the server. The default value is **200**.

To reduce server memory consumption with little effect on performance for general use, particularly for systems with more than 50 users, we recommend reducing this value to **25**. This can make approximately 1 MB more server memory per user available without causing memory errors. The additional memory can be used to accommodate additional users.

Reducing the setting further can have a significant negative effect on performance even with fewer users. Likewise, for intensive single-user operations that affect large numbers of vault objects, a value of **25** can negatively effect performance and a higher value (for example, **2048**) should be used. Examples of such operations are: importing a large vault configuration file, importing many documents, processing many folders or folders with many documents.

> **Note:**
> Changes to this setting take effect the next time a user opens a vault. Restarting the AutoManager EDM Server service is not necessary.

The DWORD registry key to adjust the **ObjectsCacheDepth** setting is located at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
Meridian\CurrentVersion\OML
```

Configure the BrowseForGlobalGroups Setting

If all security roles within all vaults hosted by a Meridian application server are assigned to Meridian server local groups or local user accounts, you can configure the Meridian application server to not query the network domain controller for information about global groups. This can reduce the amount of information the Meridian application server needs to cache and process for user actions, thereby improving performance of the Meridian application server.

> **Note:**
> The security policies of many organizations prevent or discourage the use of local groups. However, the Meridian server local groups can consist of domain global groups, thereby relinquishing the processing of global group memberships to Windows, achieving the best of both worlds. Users' group memberships can be managed centrally with domain global groups, but Meridian does not need to query the network domain controller for the groups' memberships.
>
> The default value of this setting is **0** (cleared) and set during Meridian installation. If your system currently uses domain groups exclusively and this setting is enabled (**1**), we strongly recommend that you consider using local groups and disable this option to improve performance.

To configure the **BrowseForGlobalGroups** setting:

1. In the Meridian Enterprise Administrator, right-click **EDM Server** in the left pane and select **Properties**.

   The **EDM Server Properties** page appears.
2. Click the **Engine** tab.

   The **Engine** options appear.
3. Select one of the **Groups** options and click **OK**.

The DWORD registry key to adjust the **BrowseForGlobalGroups** setting is located at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
Meridian\CurrentVersion\OML
```

Configure the CopyDLL Setting

By default, Meridian uses one database engine (process) for all vaults on the same server that use the same DBMS (Hypertrieve, SQL Server, or Oracle). If your Meridian server has multiple CPUs and hosts multiple vaults that are frequently accessed by users, it is possible to improve overall performance with the **CopyDLL** setting. Configuring this setting to **1** dedicates one database engine (process) to each vault. Windows may, in turn, assign each process to a different CPU as each CPU becomes completely utilized, which can improve performance when multiple vaults are accessed at the same time.

Create or edit the DWORD value **CopyDLL** located at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
Meridian\CurrentVersion\OML
```

> **Note:**
> The setting has been correctly enabled if in each vault folder you find a new DLL file that has the same name as the vault.

Optimize the Vault Configuration

A vault's configuration and the way it is used can have a dramatic effect on performance. The major configuration factors and recommendations are described in the following topics.

Folders

The number of folders at each level of a vault's folder structure has an effect on various Meridian functions such as displaying folders in views and operations on subfolders. We recommend that you configure vaults in a hierarchical folder structure that organizes documents in such a way that the minimum number of folders is required at any one level.

Folder Levels

The number of levels of folders in a vault, possibly controlled by the Field-Path definition, can also affect performance. While folder structure usability from the user's perspective decreases with as few as 4 folder levels, we recommend not more than 10 folder levels. In addition, try to organize the folders so that there are fewer top-level folders, each of which contains more subfolders, rather than having many top-level folders.

Files Per Folder

A large number of documents per folder can adversely influence the performance of Meridian. We recommend a maximum of 2000.

Multiple Vaults

Every vault hosted by a Meridian application server will consume system resources (memory and CPU) for overhead even when not frequently used. Wherever possible, reduce the number of vaults on one server. The maximum number of vaults on a single Meridian application server is limited to 64 to prevent system stability issues. However, the practical number of vaults per Meridian server is limited by the number of CPUs and available memory.

In any case, we do not recommend more than 10–15 vaults (depending on their size and the number of concurrent users) per Meridian application server. If the number of vaults on one server and the number of users accessing that server begin to require more application virtual memory than can be provided by the operating system, consider moving one or more of the vaults to an additional Meridian application server. If the server only hosts one large vault and sufficient application virtual memory cannot be made available through other optimizations (including upgrading the server hardware, operating system, and Meridian software), consider dividing the vault into two or more smaller vaults only as a last resort.

> **Note:**
> Temporarily disable vaults that are seldom used or reduce their **MaximumCacheSize** setting to make more memory available for active vaults. For assistance in temporarily disabling vaults, contact Accruent Technical Support.

Custom Properties

Depending on your overall computing environment, using many custom properties can cause poor system performance, particularly when application links are enabled. By default, Meridian Enterprise synchronizes an empty custom property only if it contained a value and a user deleted that value. Each such property requires multiple operations to find the previous value of the property. If a document uses many custom properties, these operations can negatively affect system performance, particularly if network performance is not optimal or for batch operations with many documents.

To optimize the performance of application links with empty properties, see the description of the **CheckBlankPropertiesAssigned** setting in *Configure Empty Property Synchronization* in the *Meridian Enterprise Configuration Guide* and the following registry values that **CheckBlankPropertiesAssigned** overrides:

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMLink\Settings

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMDocUpdateUtl\Settings

Security Role Assignments

The quantity of security role assignments on each vault folder has a direct effect on performance. The more roles that are assigned, the more time is required for Meridian to validate each user's actions. For best performance, assign Accruent groups to roles instead of assigning network groups or individual users to roles. If you choose to assign network groups, use local groups and avoid using global groups. For more information on security role assignments, see Configure the EDM Server Service.

Document Type Security

Enabling a vault's **Use document type security** option has an adverse impact on performance. The reason for this is that the Meridian application server then has more security privileges to evaluate for each user action on a document. When you enable **Use document type security**, the current number of document type privileges is multiplied by the number of document types configured in the vault so that each document type will have its own privileges that you can assign. With **Use document type security** cleared, there is only one set of privileges for all document types. We recommend that you not use this option unless it is required for business reasons.

Sequence Numbers

Server performance and stability problems can result if many number sequences are stored in a vault. The quantity of numbers produced by each sequence has no affect on performance or stability. You can define any number of custom number sequences in Meridian Enterprise using VBScript methods like **NextSequenceNumber**. Each number sequence can be accessed by name and produces one series of numbers that can be used in automatically generated document names and similar purposes.

When many number sequences are defined in one database, much information needs to be stored in the database (method of numbering, current number, numbering formula, and so on). This is true for all types of databases, not just Meridian Enterprise and is a logical result of using sequences in general. Using more than approximately 500 number sequences should be avoided. If more number sequences are necessary, other solutions are often possible by reviewing the system design. For example, it may be possible to use a single custom property with 500 values and one sequence number, rather than 500 sequence numbers.

When solutions to reduce the quantity of number sequences are not practical, alternatives that will not affect performance include:

- Store the number sequences in their own vault
- Store the number sequences in an external database table.

For information on using number sequences with VBScript, see the *Create And Edit Sequence Numbers* article in the *Meridian Enterprise Configuration Guide* and the *Sequence Object* article in the *Meridian Enterprise VBScript API Reference*.

Optimize Vault Performance

When designing a large Meridian Enterprise system, distributing the data among multiple smaller vaults can produce up to four times better performance than containing it all in one or more larger vaults.

Each Meridian vault can be tuned for optimal performance based on its size and the amount of activity it gets. The major configuration factors and recommendations are described in the following topics.

If a vault is configured to use HyperCache, its performance is already optimized and the following topics do not apply.

Configure the MaximumCacheSize Setting

The AutoManager EDM Server service caches each vault's database in memory to optimize performance. The more memory that is available, the more data (up to the entire database) can be cached and the better the performance will be. The default setting of 750 MB is only an example. For optimal performance of Hypertrieve vaults, the database cache size should equal the database file size. At least 20 MB will be used in all cases.

> **Note:**
> This cache is in addition to the caching performed by SQL Server or Oracle if either program is used.

The **MaximumCacheSize** setting is used by the system to determine the maximum amount of server memory (in MB) that should be used for the database cache. It ensures that the vault's cache size does not grow so large that it consumes memory that is needed for user sessions and the operating system, which could result in **Out of memory** errors.

If a single vault is used, the general recommendation is to set **MaximumCacheSize** to the size of the vault database file if Hypertrieve is used or the maximum available application memory on the server, whichever is smaller. For SQL Server vaults, the database cache size should be at most 50% of the database file size. For Oracle vaults, the database cache size should be 100% of the database file size. If multiple vaults are used, the available server memory should be divided between the caches of all vaults according to their database file size. This setting should be adjusted upward for the expected annual vault growth, if memory is available. In all cases, however, the total size of all vault caches should leave sufficient memory available for user session data. For more information about user session data, see Virtual Memory.

If the amount of installed RAM on the server cannot accommodate optimum cache sizes for all vaults, we recommend installing additional memory in the server computer. If the computer has already been configured with its maximum amount of memory, we recommend that you consider the recommendations described in Optimize the Server Operating System and Optimize the Meridian Server Software.

This setting works together with the **RelativeCacheSize** setting. The system will use whichever setting results in a smaller cache size. For example, if you specify 1 GB of RAM for caching a 750 MB database file size, setting **MaximumCacheSize** to **1000** (MB) and **RelativeCacheSize** to **100** (percent) will initially result in the entire database being cached because 100 percent of 750 MB is less than 1000 MB. The **RelativeCacheSize** setting is in effect and is controlling the cache size. However, the database will grow over time with the addition of more documents, revisions, and so on and will consume more memory accordingly. When the database size exceeds 1000 MB in size, the **MaximumCacheSize** setting will come into effect and limit the cache size to 1000 MB because 100 percent of anything over 1000 MB is greater than 1000 MB. If additional memory is made available for caching, the **MaximumCacheSize** setting should be adjusted upward so that

the **RelativeCacheSize** setting becomes the effective setting again. Both settings should be considered together with the amount of installed RAM and the number of active vaults.

> **Note:**
> This setting is overridden if the **HyperCache** setting is enabled as described in Configure Hypercache.

Configure Setting in Administrator

To configure the **MaximumCacheSize** setting:

1. In the Meridian Enterprise Administrator, click **EDM Server** in the left pane.

   The active vaults are listed in the right pane.
2. Select the vault that you want to configure in the right pane.
3. Click the **Action** menu and select **Properties**.
4. Click **Advanced**.
5. Adjust the **MaximumCacheSize** setting.
6. Click **OK**.

Configure Setting using Registry Key

This setting can also be configured with the **MaximumCacheSize** registry key located at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
Meridian\CurrentVersion\Installed DataStores\
<VaultName>\CompoundItemService
```

Configure the RelativeCacheSize Setting

The AutoManager EDM Server service caches each vault's database in memory to optimize performance. The more memory that is available, the more data (up to the entire database) can be cached and the better the performance will be. The **RelativeCacheSize** setting is used by the system to determine the maximum amount of server memory (expressed as a percentage of the vault database size) that should be used for the vault's database cache. We recommend a setting of **100** (percent) if enough application memory is available but depending on the size of the vault database, it is sometimes not possible because there is not enough memory available on the server. For SQL Server vaults, the database cache size should be at most 50% of the database file size. For Oracle vaults, the database cache size should be 100% of the database file size. If multiple vaults are used, the available server memory should be divided between caches of all vaults according to their database file size.

> **Note:**
> This cache is in addition to the caching performed by SQL Server or Oracle if either program is used.

If the amount of installed RAM on the server cannot accommodate optimum cache sizes for all vaults, we recommend installing additional memory in the server computer, if possible. If the computer has already been configured with its maximum amount of memory, we recommend that you consider either reducing this setting or implementing the other recommendations described in Optimize the Server Operating System and Optimize the Meridian Server Software.

This setting works together with the **MaximumCacheSize** setting. The system will use whichever setting results in a smaller cache size. For example, if you specify 1 GB of RAM for caching a 750 MB database file size, setting **MaximumCacheSize** to **1000** (MB) and **RelativeCacheSize** to **100** (percent) will initially result in the entire database being cached because 100 percent of 750 MB is less than 1000 MB. The **RelativeCacheSize** setting is in effect and is controlling the cache size. However, the database will grow over time with the addition of more documents, revisions, and so on and will consume more memory accordingly. When the database size exceeds 1000 MB in size, the **MaximumCacheSize** setting will come into effect and limit the cache size to 1000 MB because 100 percent of anything over 1000 MB is greater than 1000 MB. If additional memory is made available for caching, the **MaximumCacheSize** setting should be adjusted upward so that the **RelativeCacheSize** setting becomes the effective setting again. Both settings should be considered together with the amount of installed RAM and the number of active vaults.

> **Note:**
> This setting is overridden if the **HyperCache** setting is enabled as described in Configure Hypercache.

Configure Setting in Administrator

To configure the **RelativeCacheSize** setting:

1. In the Meridian Enterprise Administrator, click **EDM Server** in the left pane.

   The active vaults are listed in the right pane.
2. Select the vault that you want to configure in the right pane.
3. Click the **Action** menu and select **Properties**.
4. Click **Advanced**.
5. Adjust the **RelativeCacheSize** setting.
6. Click **OK**.

Configure Setting using Registry Key

This setting can also be configured with the **RelativeCacheSize** registry key located at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
Meridian\CurrentVersion\Installed
DataStores\<VaultName>\CompoundItemService\RelativeCacheSize
```

Configure the MaximumLogSize Setting

Meridian maintains a transaction log file for each vault database (HyperCache only) that contains all changes made to the vault since the log was last committed to the database and a snapshot was created. When the size of the log reaches the value of **MaximumLogSize** (in MB) and the amount of time specified by the **MinimumSnapshotInterval** setting has elapsed, the log is committed to the database and a new snapshot is created. The **MaximumLogSize** setting can be used to limit the size of the log file so that the data is committed to the database after predictable amounts of work have been performed in the vault without adversely affecting performance.

This setting works together with the **MinimumSnapshotInterval (in minutes)** setting. For example, if **MaximumLogSize** is set to **8** (default) and **MinimumSnapshotInterval** is set to **240** (default), when the log file reaches 8 MB no snapshot will be created unless 240 minutes (4 hours) has elapsed since the last snapshot. Likewise, if 240 minutes (4 hours) has elapsed since the last snapshot, a new snapshot will not be created until the log file size is at least 8 MB. We recommend that you use the default settings under most circumstances. The **MaximumCacheSize** and **RelativeCacheSize** settings are more effective for optimizing performance.

> **Note:**
> Whenever a **Prepare for Backup** operation occurs, the log is committed to the database and a new snapshot is created.

Configure Setting in Administrator

To configure the **MaximumLogSize** setting:

1. In the Meridian Enterprise Administrator, click **EDM Server** in the left pane.

   The active vaults are listed in the right pane.
2. Select the vault that you want to configure in the right pane.
3. Click the **Action** menu and select **Properties**.
4. Click **Advanced**.
5. Adjust the **MaximumLogSize** setting (in MB).
6. Click **OK**.

Configure Setting using Registry Key

This setting can also be configured with the **MaximumLogSize** registry key located at:

HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<*VaultName*>\CompoundItemService

Temporarily Disable Snapshot Creation

To temporarily disable snapshot file creation during large batch operations:

1. Navigate to the following registry key on the Meridian application server:

   HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<*VaultName*>\CompoundItemService

2. Create a **AllowSnapShot** DWORD registry value.
3. Set **AllowSnapShot** to **0** to disable creation of new snapshots.
4. Stop the **AutoManager EDM Server** service.
5. Restart the **AutoManager EDM Server** service.
6. Begin the batch operation.
7. Wait for the batch operation to complete.
8. Navigate back to the registry key listed in step 1.
9. Set **AllowSnapShot** to **1** to enable creation of new snapshots.
10. Stop the **AutoManager EDM Server** service.
11. Restart the **AutoManager EDM Server** service.

    Normal snapshot file creation will resume.

Configure the MinimumSnapShotInterval Setting

Meridian maintains a transaction log file for each vault database that contains all changes made to the vault since the log was last committed to the database and a snapshot was created. When the amount of time specified by the **MinimumSnapshotInterval** setting has elapsed, the log is committed to the database and a new snapshot is created.

This setting works together with the **MaximumLogSize** (in MB) setting. For example, if **MaximumLogSize** is set to **8** (default) and **MinimumSnapshotInterval** is set to **240** (default), when the log file reaches 8 MB, no snapshot will be created unless 240 minutes (4 hours) has elapsed since the last snapshot. Likewise, if 240 minutes (4 hours) has elapsed since the last snapshot, a new snapshot will not be created until the log file size is at least 8 MB.

The primary purpose of **MinimumSnapshotInterval** is to allow a System Administrator to prevent a snapshot from occurring during production hours (as a result of **MaximumLogSize** being met) when an extraordinary number of changes are made to the vault (such as a batch import), which would adversely affect performance.

> **Note:**
> Whenever a Prepare for Backup operation occurs, the log is committed to the database and a new snapshot is created.

Configure Setting in Administrator

To configure the **MinimumSnapshotInterval** setting:

1. In the Meridian Enterprise Administrator, click **EDM Server** in the left pane.

   The active vaults are listed in the right pane.
2. Select the vault that you want to configure in the right pane.
3. Click the **Action** menu and select **Properties**.
4. Click **Advanced**.
5. Adjust the **MinimumSnapshotInterval** setting (in MB).
6. Click **OK**.

Configure Setting using Registry Key

This setting can also be configured with the **MinimumSnapshotInterval** registry key located at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
Meridian\CurrentVersion\Installed
DataStores\<VaultName>\CompoundItemService\MinimumSnapshotInterval
```

Temporarily Disable Snapshot Creation

To temporarily disable snapshot file creation during large batch operations:

1. Navigate to the following registry key on the Meridian application server:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
   Meridian\CurrentVersion\Installed
   DataStores\<VaultName>\CompoundItemService
   ```

2. Create a **AllowSnapShot** DWORD registry value.
3. Set **AllowSnapShot** to **0** to disable creation of new snapshots.
4. Stop the **AutoManager EDM Server** service.
5. Restart the **AutoManager EDM Server** service.
6. Begin the batch operation.
7. Wait for the batch operation to complete.
8. Navigate back to the registry key listed in step 1.
9. Set **AllowSnapShot** to **1** to enable creation of new snapshots.
10. Stop the **AutoManager EDM Server** service.
11. Restart the **AutoManager EDM Server** service.

    Normal snapshot file creation will resume.

Optimize Client Computer Performance

Although there are fewer factors that affect the performance of Meridian client computers than the Meridian application server, the configuration of client computers can also have an impact on overall Meridian system performance. The major configuration factors and recommendations are described in the following topics.

Multiple Network Providers

Meridian communicates exclusively over Windows networks. If other network providers (for example, Novell Netware) are in use, the Client for Microsoft Networks should have the highest priority for the network connection used by Meridian client computers.

Multiple Network Protocols

The only protocol the Meridian software uses to communicate with its LAN clients is the TCP/IP protocol. If other network protocols are in use, the TCP/IP protocol should be the first one in the binding order for the network connection used by the Meridian client computers. Unused network protocols should be uninstalled from the computer.

Viewer Refreshes

By default, the viewer that is used by the Meridian client applications will automatically refresh whenever the user navigates to another document regardless of whether the user actually wants to view the document or not. This is convenient for the user but it impacts network performance, and thereby, client computer performance, because uncached documents must be downloaded from the Meridian application server for viewing and the user cannot perform any other actions while the viewer is rendering the document on screen.

To improve client computer performance and reduce network traffic, users can disable automatic refreshes of the Meridian viewer on their computers. The amount of performance that can be gained depends on the number of documents viewed, the use and contents of the Local Workspace, the size of the documents, the network bandwidth, and the client computer hardware.

AutoCAD Font Files

If the AutoCAD font files used by a drawing being viewed by a user cannot be found, or if they are located on a server, performance is degraded. For best performance, store copies of the font files on each client computer and configure the Meridian viewer in the client application to find them there.

To configure the location of AutoCAD font files, see the *Configure the Acme CAD Converter Rendering Module* article in the *Meridian Enterprise Server Administrator's Guide*.

Optimize PowerWeb Performance

When you generate reports with over 10,000 documents, Meridian PowerWeb might slow down and become unavailable for all users, requiring a server restart. To maintain PowerWeb performance and prevent outages, you can create the ReportDocumentsLimit registry key on servers hosting Meridian and PowerWeb applications managed by Microsoft IIS. The registry key sets the maximum number of documents in a report.

1. Open the **Windows Registry Editor**.
2. Navigate to HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink.
3. Create a DWORD (32-bit) registry key named **ReportDocumentsLimit**.
4. Double-click the **ReportDocumentsLimit** registry key.

   The dialog opens.
5. In the **Edit DWORD (32-bit) Value** dialog that opens, under **Base**, select **Decimal**.
6. In **Value data**, enter the maximum number of documents allowed in a report.

   We recommend entering 10000 if the report template contains fewer than 100 properties. For templates with more properties, test lower limits to find the optimal value.
7. Restart the Meridian server.

Optimize Antivirus Applications

Most organizations run antivirus applications on their server and client computers as part of their standard computer configurations. The applications impose additional overhead on the computer's CPU when files are scanned for viruses.

Configure the antivirus application on servers to NOT perform real-time scanning of folders or shares used by Meridian vaults (database and stream files). If the folders are not excluded, the antivirus application will scan all files, thereby putting a very large workload on the server, which can cause errors, even to the point of making it stop functioning. If required, perform only scheduled nightly scans of the Meridian folders when they are not in use.

Avoid real-time scanning of documents on client computers, if possible, because it will degrade client computer performance. This is particularly true for the Meridian Local Workspace folders. If required, perform only scheduled nightly scans of Meridian client computers when they are not in use.

Optimize Batch Operations

Batch operations read or modify the data for many vault folders or documents in a single operation, which can require a lot of resources on both the Meridian application server and client computers.

Batch operations include such actions as:

- Importing large numbers of documents
- Running the **Vault Consistency Wizard**
- Modifying the Field-Path definition
- Changing the security of the vault

The amount of time that they require can be reduced.

To optimize performance during batch operations:

1. Perform batch operations after production hours when no users are connected to the server.
2. Reduce the **MaximumCacheSize** setting of the vault to 60 MB as described in Configure the MaximumCacheSize Setting because batch operations do not use this cache.
3. Configure the database engine for best single-user performance as described in Configure the EDM Server Service.

   This will allow the server to use the maximum amount of system resources for the operation.
4. If the Meridian FDA Module is enabled, disable the audit log by temporarily clearing the **Audit table connection string** option described in Configure the Audit Log Connection.
5. Disable other vaults as described in Disable a Vault.
6. Run the batch operation using a client application run on the server computer, if possible.
7. Remember to restore these settings after the batch process has finished.

Remote Site Caches

Because Meridian Enterprise is a centralized system, optimizing performance for remote users with modest available bandwidth can be a challenge, particularly if the users work with large files or many external references. Meridian Enterprise provides a variety of features to help meet this challenge, including Remote and Online modes for Power Desktop users and Remote mode for PowerWeb and Explorer users.

If a group of Meridian Enterprise users works in proximity to a corporate web server that is geographically closer to them than the Meridian Enterprise application server, Meridian Enterprise web server, or Meridian Explorer server, a site cache component can be installed and configured on their local web server. Site cache servers support Meridian Explorer clients and the Online and Remote modes of PowerWeb (HTTP or HTTPS) but do not support Offline mode or the PowerUser client (DCOM). They also support simultaneous connections from multiple sessions by the same user and simultaneous connections to multiple Meridian Enterprise servers.

The site cache temporarily stores documents (source or renditions) that the users work with so that they do not have to download them from the central server every time. The system response and performance to download and upload documents is greatly improved, comparable to users that are located near to a Meridian Enterprise server. The site cache service automatically synchronizes the cache with the Meridian Enterprise servers transparently in the background. Old and orphaned documents are removed from the cache (and from local workspaces) to make space for newer and active documents. Multiple site caches can be configured to serve separate groups of users that each have a local web server.

When a remote user creates new documents, the system immediately sends them to the Meridian Enterprise web server and stores them in the vault. The new documents are added to the local site cache when the remote user accesses them after import is completed.

Configuring a site cache server involves tasks on several servers as well as on the Meridian Explorer clients. The installation tasks are listed in the order in which they should be performed in the following table and are described in this guide and in other guides. Use the hyperlinks in the following checklist to find the instructions for each task. Track your installation progress by printing this checklist and placing a check mark in the **Completed** column as you finish each task.

Site cache configuration checklist

Completed	Task	Topic Reference
	If using HTTPS, Install the site cache server certificate on the Meridian Enterprise Server machine.	When using HTTPS, it is now mandatory to install a site cache server certificate on the Meridian Enterprise Server machine for each site cache server, otherwise the site cache server is marked as invalid and an error like this one is shown in the BC Application Events: Site Cache Server 'https://<pcname>/BCSiteCache' is unavailable due to these reasons: • One or more errors occurred. • An error occurred while sending the request. • The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel. • The remote certificate is invalid according to the validation procedure. To provide preload tasks with a way to query site cache servers using HTTPS, ensure site cache servers have a self-signed certificate issued to localhost.

Completed	Task	Topic Reference
	The Meridian Enterprise EDM Server service, Meridian Enterprise web application identity, Meridian Enterprise Server service, and the **BCSiteCache** web application identity must all run under the same account.	Enter an appropriate domain account during Meridian Enterprise server installation when prompted. Confirm that the account is used by each of the services. For account requirements, see Granting domain privileges with a service account.
	Integrate Meridian Enterprise with Meridian Enterprise Server and specify the correct **HOST** and **UPN** parameters for the Meridian Enterprise Server account.	Configuring the connection to Meridian Enterprise Server
	Publish the vault that contains the documents to be cached as a PowerWeb location on only one Meridian Enterprise web server.	Creating a PowerWeb location
	Confirm that the site cache server meets or exceeds the minimum system requirements.	Site cache server requirements
	Disable Compatibility view of the **BCSiteCache** URL in Internet Explorer on the PC that will be used to configure the site cache server.	Compatibility View on the MSDN website.
	Register the site cache server in Meridian Enterprise Server.	See the *Register Site Cache Servers* article in the *Meridian Enterprise Server Administrator's Guide*.
	Configure the site cache server in Meridian Enterprise Server.	See the *Configure Site Cache Servers* article in the *Meridian Enterprise Server Administrator's Guide*.
	Pre-load the site cache with documents.	See the *Pre-load site caches* article in the *Meridian Enterprise Server Administrator's Guide*.
	On the client PCs, confirm that the local workspace component of Meridian Enterprise Application Integration is installed and running (`BlueCieloECM.SiteCache.LwsClient.exe`).	

Completed	Task	Topic Reference
	On the client PCs, confirm that Meridian Enterprise Application Integration is set to **Remote** mode.	See *Work Offline or Remote* in the *Meridian Enterprise User's Guide*.
	On the client PCs, confirm that the site cache URL is set correctly.	See *Configure Local Workspace* in the *Meridian Enterprise User's Guide*. HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client
	If users will connect from a different domain or if the site cache server is behind a proxy server, advise users how to set the connection settings of the site cache client.	See *Configure a Site Cache Connection* in the *Meridian Enterprise User's Guide*.
	On the client PCs, confirm that the local workspace option **Use in Offline and Remote modes** is enabled.	See *Configure Local Workspace* in the *Meridian Enterprise User's Guide*.
	On the client PCs, if they will be used in Remote mode with application links and large assemblies, consider enabling the **EnableRemoteDocumentCache** setting.	HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMLink\Settings

Integrate Meridian Enterprise with Meridian Portal

Meridian Cloud is a SaaS solution offered by Accruent that can be integrated with Meridian Enterprise. Meridian Cloud has three main modules: Portal, PowerWeb, and Explorer. The Cloud-based versions of PowerWeb and Explorer are similar to those offered in Meridian Enterprise.

Meridian Portal can be integrated with Meridian Enterprise so that documents can be sent from Meridian Enterprise project folders to Meridian Portal projects (standard projects, not packages-only projects) for revision, review, approval, and handover back to Meridian Enterprise. This workflow is shown in Workflow Actions. When documents are approved, they can be imported back into the Meridian Enterprise project folders. This can be done in one of two ways:

1. Documents can be sent back to Meridian Enterprise by the **Document Controller** using the **Send to Meridian** issue reason. After this process is complete, the documents in the package have the status **In Meridian** and are locked in Portal.

   This process can be automated for documents submitted by a contractor.
2. Released documents can be sent back to Meridian Enterprise by the **Document Controller** using the **For Handover** issue reason. After this process is complete, documents have the **Released** status and are locked in Portal.

To learn more about the capabilities of Meridian Portal, see the Meridian Portal documentation in the Technical Library.

What is Meridian Portal?

Meridian Portal is a web application for collaborating on engineering projects. Target users include document controllers, external engineering contractors, regulatory bodies, and other external end users.

Authorized tenant administrators maintain the configuration, and project owners create new projects and invite internal and external participants. The invited project members receive secure role-based access, and every participant has a personal landing page with an overview of “My Tasks,” “Received Packages,” and “Recent Projects.”

Within Meridian Portal, there is a personal dashboard with status reports on documents and the workflow progress of packages. Meridian Portal has a central repository for documents with text search and dynamic filtering to allow users to quickly find what they need. Views on document details can be adapted for internal and external use.

The key features of Meridian Portal include:

- Internal and external collaboration in a secure cloud-based project portal
- An easy-to-use task-based user interface for engineering contractors

- Formal and informal exchange of information in work packages
- Collaborative document review and approval processes
- Automated document compliance and completeness checks
- Full audit and history log on actions performed by internal and external participants

Learn more about which Meridian Enterprise features are supported in Meridian Portal.

Prerequisites for the Integration

The following section outlines requirements you must meet before implementing the Meridian Portal integration.

Subscription

Before you can configure the Meridian Portal integration, you must first purchase a paid subscription for Meridian Cloud. There are three subscription levels: **Meridian Cloud Project**, **Meridian Cloud Business**, and **Meridian Cloud for Life Sciences**.

> **Note:**
> The **Meridian Cloud Project** subscription level is sufficient for the Meridian Portal integration but may not include all the features you want to use in Cloud. Learn what is included with each subscription level.

After you have purchased a paid subscription, your Accruent representative will create a Meridian Cloud tenancy for you. Your tenancy is your specific instance of Meridian Cloud. Your Accruent representative will provide you with the information you need to configure your tenancy's integration with Meridian Enterprise.

Additionally, you must also have a Meridian Enterprise license for the Advanced Project Workflow Module. This module is not part of the base licenses for Meridian Enterprise. To learn more about the Advanced Project Workflow Module, see *Advanced Project Workflow Module* in the *Meridian Enterprise Configuration Guide*.

Contact your Accruent representative if you are interested in purchasing a Meridian Cloud subscription, or if you need to purchase an additional license for the Advanced Project Workflow Module.

Technical requirements

Additionally, you must meet the following technical requirements:

1. You must be using a currently supported version of Meridian Enterprise.

   To learn which versions of Meridian Enterprise are currently supported, see the *Current Support Life Cycle Status* page in the *Meridian Enterprise Supported Software* document.
2. You must implement TLS 1.2.

Set up the Integration

This section outlines the minimum requirements necessary for enabling an integration with Meridian Portal.

Configure the Connection To Meridian Enterprise Server

Register the Meridian Enterprise Vault you want to integrate with Portal

To learn how to register the Meridian Enterprise vault you want to integrate with Portal, see *Register a Meridian Enterprise Vault* in the *Meridian Enterprise Server Administrator's Guide*.

Vault Configuration

For each vault that will be connected with Meridian Portal, you must configure the following properties in the Administrator.

Vault properties required for integration

Tab	Setting	Value
Advanced Features	Enable Advanced Project Workflow Module	Enabled

Tab	Setting	Value
Advanced Features	Enable Meridian Publisher extension	Enabled
Advanced Features	Enable packages support	Enabled
Advanced Features	Repository Name	Enter the name of the Meridian Explorer repository from which the packages are made. This option is required to enable the **Export Packages** and **Import Packages** pages in PowerWeb when it is integrated with Meridian Portal.

Create a Folder Type and Project Definition to use with Portal

In the Configurator, create at least one folder type with the **Can be linked to Meridian Portal projects** setting enabled. After creating a folder type with this setting enabled, the **ProjectFolderPropertySet** property set is created automatically.

Once you have created your folder type, create a project definition that uses this folder type.

To learn how to create a folder type, see the *Create And Edit Folder Types* article in the *Meridian Enterprise Configuration Guide*.

To learn how to create a project definition, see the *Create a Project Definition* article in the *Meridian Enterprise Configuration Guide*.

Configure Scopes

Ensure that the **Link to Meridian Portal** and **Send to Portal** commands are enabled for the appropriate scopes. You can find these commands on the **Command Filter** tab.

To learn how to configure scopes, see the *Create And Edit Scopes* article in the *Meridian Enterprise Configuration Guide*.

Connect Meridian Cloud tenancy in Administration Console

To learn how to connect the Meridian Cloud tenancy in the Administration Console, see the *Change Tenancy settings* procedures in the *View And Edit the Connectivity Settings* article in the *Meridian Enterprise Server Administrator's Guide*.

Repository Settings

You must perform the following tasks related to repositories:

1. Create an Explorer repository. The repository name must differ from your Meridian tenancy name, otherwise the **Validate Synchronization** task fails with the **The selected job is not valid for this operation** error.

   Only documents synchronized to this repository will be available in Portal.

2. Configure the repository.

   To learn how to configure an Explorer repository, see *Configure a Meridian Explorer Repository* in the *Meridian Enterprise Server Administrator's Guide*.

3. Set the following values in the Vault Overview Options in the Administration Console:

   To learn more about these settings, see *Manage a Meridian Enterprise Vault* in the *Meridian Enterprise Server Administrator's Guide*.

   - **Document number property**: Set this value to any custom property
   - **Project number property**: Set this value to **ProjectFolderPropertySet.ProjectNumber**

   > **Important!**
   > If there are multiple vaults registered in Enterprise Server, your vaults must be configured to ensure that the values of **ProjectFolderPropertySet.ProjectNumber** are unique across all your vaults.
   >
   > How project numbers are calculated depends on your configuration. Usually a VBscript function is used to calculate them.
   >
   > A simple way to keep project numbers unique is to give them a vault-specific prefix. For example, if you have a vault for Unit 1, Unit 2, and Unit 3, then the script used for Unit 1 can use **U1-** as a prefix.
   >
   > If this is not feasible, you can also use a central SQL database and use SQL queries to generate unique numbers.
   >
   > Another approach is to generate sequence numbers using `Vault.Sequence("MySeq").Next` in one of the vaults and use `Vault.CallRemote` in the other vaults to access this sequence.

Create a Repository Synchronization Job

Next, you must create a repository synchronization job. A synchronization job reads data from the Meridian Enterprise source vault and exports it to one or more intermediate data (not document content) files. To learn more about repository synchronization jobs, see *Repository Synchronization Jobs* in the *Meridian Enterprise Server Administrator's Guide*.

Note:
If there is more than one repository synchronization job, the **Send to Portal** action may fail. To learn more about the **Send to Portal** action, see *Send Documents To Meridian Portal* in the *Meridian Enterprise User's Guide*.

To create a repository synchronization job, see the following articles in the *Meridian Enterprise Server Administrator's Guide*:

1. *Create a Publishing Job*
2. *Configure a Publishing Job*
3. *Configure Synchronization Options*

Create a Package Export Job

A **Package Export** job is a publishing job which defines a destination for exporting packages. There should be only one Package Export job per Explorer repository.

To create a package export job, see the following articles in the *Meridian Enterprise Server Administrator's Guide*:

1. *Create a Publishing Job*
    - In step 3 of the *Create a Publishing Job* procedures, select **Package Export** as the job type.
    - In step 10 of the *Create a Publishing Job* procedures, select **Meridian Portal** as the destination system.
2. *Configure a Publishing Job*

Create and Configure Import Profile

Next, you will need to create an import profile. To learn how to create an import profile, see the *Create an Import Profile* article in the *Meridian Enterprise Server Administrator's Guide*. The settings in the table below are specific to the integration.

Important!
There should only be one import profile that has the **Use Meridian Portal** setting enabled per vault.

Import Profile settings specific to integration

Group	Setting	Value
General	Use Meridian Portal	Enabled
Destination repository	Destination repository	The destination vault for the items that are imported from packages to which you assign this import profile. Only the projects in this vault are valid destinations.
Administrative Permissions	Import	Everyone
Administrative Permissions	Close, reopen, delete	Everyone

Configure VBScript to Assign Document Numbers to New Documents

You can modify the following VBScript and add it to the Configurator to assign document numbers to new documents submitted in packages by external business partners. By default, the documents are assigned GUID values as temporary document numbers. To learn more about working with VBScript, see the *Meridian Enterprise VBScript API Reference Guide*.

```
Sub ImportPackage_AfterImportedFromPortal()

    Document.psGeneral_DocumentNr = Document.psGeneral_Discipline & Right ("00000" & Vault.Sequence
(Document.psGeneral_Discipline).Next, 5)

    Document.ApplyPropertyValues 'To save the update

End Sub
```

Show Export Package and Import Package Property Pages in PowerWeb

You can modify the following VBScript and add it to the Configurator to configure the display of the **Export Package** and **Import Package** property pages in PowerWeb. To learn more about working with VBScript, see the *Meridian Enterprise VBScript API Reference Guide*, and to learn more about property pages, see the *Property Pages* article in the *Meridian Enterprise User's Guide*.

```
Function ExportPackagesPage_IsVisible()
    If Not Document Is Nothing Then
        'Add your code for document objects
        ExportPackagesPage_IsVisible = True
    ElseIf Not Folder Is Nothing Then
        'Add your code for folder objects
    End If
End Function

Function ImportPackagesPage_IsVisible()
    If Not Document Is Nothing Then
        'Add your code for document objects
        ImportPackagesPage_IsVisible = True
    ElseIf Not Folder Is Nothing Then
        'Add your code for folder objects
    End If
End Function
```

Configure Package Scanning Options

In the *Change Tenancy Settings* procedures in the *View And Edit the Connectivity Settings* article in the *Meridian Enterprise Server Administrator's Guide*, there are two options related to package scanning.

- **Package scanning interval**: The interval in minutes to scan for new packages. The default is 5 minutes. This option is only available after a Meridian Portal tenancy has been registered.
- **Import scanned packages**: If enabled, packages that are successfully scanned are imported automatically and do not need to be imported manually as described in *Import an Import Package* in the *Meridian Enterprise Server Administrator's Guide*. This option is intended for use with packages sent from Meridian Portal.

Save Temporary Package Files

To save temporary package files:

1. Navigate to **C:\ProgramData\BlueCieloECM\EnterpriseServices\PublishingCapability.dat**.

   Learn more about the settings in this file by reviewing the *PublishingCapability.dat* article in the *Meridian Enterprise Server Administrator's Guide*.
2. Edit the file in a text editor.

3. Set the **KeepPackageTempFiles** setting to **true**.
4. Save your changes.

   Your import and export package files can now be viewed in the following folders:

   - C:\ProgramData\BlueCieloECM\EnterpriseServices\Meridian360\import
   - C:\ProgramData\BlueCieloECM\EnterpriseServices\Meridian360\Export

Cloud Connector

The Meridian Cloud Connector is a set of components for use with the Meridian Cloud applications PowerWeb, Portal, and Explorer. The components manage a local workspace on your PC where files are downloaded when you update them.

> **Important!**
> Google does not support Google Authentication in Internet Explorer. If you want to use Google Authentication for the Cloud Connector, switch your default browser to Google Chrome or Microsoft Edge.

If you are a Meridian Cloud user who needs any of these benefits, then you should install the Meridian Cloud Connector:

- View a document in the file's source application
- Export documents or metadata
- Work with batches of documents, referenced documents, hybrid parts, and redlines
- Automatic title block synchronization and reference management
- Access Meridian Cloud from within your desktop application
- Use a Meridian site cache to access documents faster.

  To learn more about site caches, see *Configure a Site Cache Connection* in the *Meridian Enterprise User's Guide*.

The Meridian Cloud Connector is convenient because it:

- Fully supports application integration with the AutoCAD, MicroStation, and Office links. Optional settings are available in Cloud Connector Installation and through Meridian Power Settings.

  These settings can be used for troubleshooting purposes.
- Does not require administrator permissions on the PC to install (includes SQLite)
- Automatically configures itself to connect to your Meridian Cloud account

You can download the Meridian Cloud Connector from the Meridian Cloud home page.

End-User Documentation

To learn more about the end-user functionality for this integration, see the following articles in the *Meridian Enterprise User's Guide*:

- *Link Folders To Meridian Portal*
- *Send Documents To Meridian Portal*

Meridian Cloud Subscription Levels

This table describes the features and services available at each Meridian Cloud subscription level.

Meridian Cloud Features per Subscription Level

Feature / Service	Meridian Cloud Project	Meridian Cloud Business	Meridian Cloud for Life Sciences
Premium Support	Included	Included	Included
Academy E-Learning	Included	Included	Included
Meridian Cloud API	Optional	Optional	Optional
Meridian Portal	Included	Included	Included
Meridian PowerWeb		Included	Included
Meridian Explorer		Included	Included
Meridian Mobile		Included	Included
Meridian for Life Sciences			Included

Cloud Connector Installation

By default, when you download the Meridian Cloud Connector installation package, it can be run immediately without any configuration on your part and will connect the client to your Meridian Cloud tenancy automatically. Alternatively, the package can be manually configured to install the components and to connect to an on-premises Meridian Enterprise deployment.

This client is for Internet use only, not for LAN users. All communication with the Meridian EDM Server will go through the Meridian web server.

The package requires:

- Windows x64 operating system
- .NET Framework
- SQL Compact or MS Jet are NOT required

The package can be configured by creating or editing the file **Meridian Cloud Connector.ini** located in the same location as **Meridian Cloud Connector.msi**. The file should include the settings in the **INI Settings** and **Features** sections described below.

> **Important!**
> Google does not support Google Authentication in Internet Explorer. If you want to use Google Authentication for the Cloud Connector, switch your default browser to Google Chrome or Microsoft Edge.

Enable Users to Change the Site Cache URL

Users cannot change the Site Cache URL using the Cloud Connector unless you have enabled access to the setting.

To enable users to change the Site Cache URL:

- Set the **RemoteOnly** registry key value to **0**.

  This setting is located in the HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion registry key.

Setting this value will enable the site cache options for the Accruent Application Integration, which can be accessed from the icon in the system tray. *However*, this value also enables other options that you may not want users to access. Review the linked documentation for more information.

Once this setting has been enabled, users can change their site cache URL by following these procedures.

INI Settings

The package can also be installed from a command line with the parameters listed in the **Command Line Parameters** column below.

Options Settings

INI Setting Name	Command Line Parameter	Description
N/A	ALLUSERS=2	Set to **2** to install the client separately for each user of the machine instead of for all users of the machine (default). The ADDLOCAL parameter must only be set to WEBCLIENT and no other features. The MSIINSTALLPERUSER parameter must be set to **1**.
LANDINGPAGEURL	LANDINGPAGEURL	The installer will add a desktop shortcut to this URL, which should be the landing page for the Meridian Cloud tenancy. For example, https://<TenancyName>.meridiancloud.net.
SITECACHEURL	SCURL	URL of the site cache server to be used
LWSFOLDER	LWSFOLDER	Local workspace folder location
TENANTURL	TENANTNAME	URL of your tenancy at the domain specified by **M360DOMAIN**. Used only for external authentication by an OpenID provider. For example, https://<TenancyName>.meridian360.com.
ISSUERURI	ISSUERURI	**https://auth-prd.meridiancloud.net/auth**. Used only for external authentication by an OpenID provider.
M360DOMAIN	M360DOMAIN	**meridian360.com** for customers in North America, **meridian360.eu** for customers in Europe. Used only for external authentication by an OpenID provider.
N/A	MSIINSTALLPERUSER	Set to **1** to install the client separately for each user of the machine instead of for all users of the machine (default). The ADDLOCAL parameter must only be set to WEBCLIENT and no other features. The ALLUSERS parameter must be set to **2**.

INI Setting Name	Command Line Parameter	Description
SKIPUI	SKIPUI	Controls display of the setup wizard dialog pages: 0 - Even if all parameters are specified in the .ini file, will display all pages so that the user can modify them. 1 - Pages will not be displayed, only settings in the .ini file will be used.
USEOPENID	USEOPENID	Authentication method: 0 - Active Directory for on-premises users 1 - External authentication by an OpenID provider using the settings above.

Features Section

The **Features** section contains settings to install the application links, which can be any of the following:

- AMHook (generic Application Integration)
- AutoCAD
- Inventor
- SolidWorks
- Revit
- MicroStation
- Office

Setting the feature to **1** installs the link, **0** skips link installation.

Following are example .ini file contents.

```
[Options]
                    LANDINGPAGEURL=https://MyOrganization.meridiancloud.net
                    SITECACHEURL=https://MyWebServer/BCSiteCache
                    LWSFOLDER=c:\bc-cache
                    TENANTURL=https://MyOrganization.meridian360.com
                    ISSUERURI=https://auth-prd.meridiancloud.net/auth
                    M360DOMAIN=meridian360.com
                    SKIPUI=0
```

```
USEOPENID=0
[Features]
AMHook=1
AutoCAD=1
Inventor=1
SolidWorks=0
Revit=1
MicroStation=1
Office=1
```

Install Package from a Command Line

To install the package from a command line, use the Command Line Parameter settings described in the INI Settings section above.

Example

In this example, the package is installed silently:

```
msiexec /i "Meridian Cloud Connector.msi" INSTALLDIR="C:\MeridianCloudConnector\"
INSTALLDIR32="C:\Program Files (x86)\MeridianCloudConnector32\"
ADDLOCAL="WebClient,AMHook,Revit,Office,AutoCAD" SCURL="https://MyWebServer/BCSiteCache"
LANDINGPAGEURL="https://MyOrganization.meridiancloud.net"
TENANTNAME="https://MyOrganization.meridian360.com" ISSUERURI="https://auth-
prd.meridiancloud.net/auth" M360DOMAIN="meridian360.com" LWSFOLDER="C:\cache" USEOPENID=1 /quiet
```

Integrate Meridian With SQL Server

The installation and maintenance of a Meridian system based on the Hypertrieve database engine is quite simple when compared to a system based on SQL Server. When SQL Server is used, additional considerations apply to configuring and administering the system. This section explains how Meridian works with SQL Server and the major considerations when administering the system.

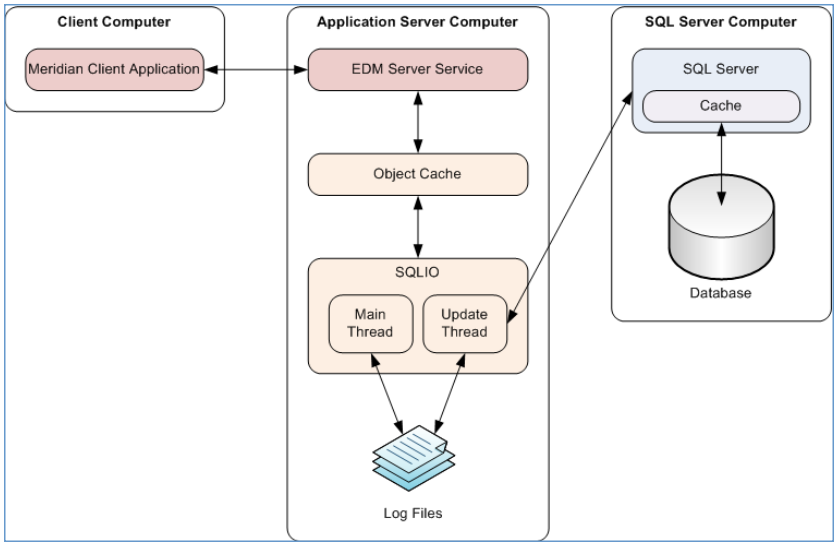
For the supported SQL Server versions see the *Database Management Systems* article in the *Meridian Enterprise Supported Software*document.

How Meridian Works With SQL Server

Meridian works with SQL Server using two intermediate Meridian components:

- Object cache (`<DatabaseEngine>SQL.dll`): A database-dependent cache that optimizes queries to SQL Server.
- Accruent SQLIO (`HTSQLIO.dll`): A SQL Server-specific component that interfaces between the object cache and SQL Server.

The relationships between these components are illustrated in the following figure.



When a Meridian client sends or requests data from the Meridian application server, the EDM Server service communicates with its object cache, which in turn communicates with Accruent SQLIO, which then communicates with SQL Server on the SQL Server computer.

Important!
Do not change the properties of a SQL Server database that is used by Meridian. Especially do not clear the **Unrestricted file growth** options for **Maximum file size** for either the data files or the transaction log. When the maximum size of the log file is reached, SQL Server cannot write to the database any more, as it is full.

Accruent SQLIO

Accruent SQLIO (not to be confused with Microsoft SQLIO) is a SQL Server-specific component that interfaces between the Meridian object cache and SQL Server. Every data change inside Meridian needs to be committed to the SQL Server database as soon as possible. Due to loads that may be placed on SQL Server by other applications and latency induced by the network between the Meridian application server and the SQL Server computer, it can take a significant amount of time for SQL Server to commit data changes, which can lead to poor performance. To avoid this bottleneck, Accruent SQLIO uses a write-ahead log mechanism as illustrated in How Meridian Works With SQL Server.

Instead of directly committing data to SQL Server, Accruent SQLIO's main thread commits data to log files (not to be confused with the SQL Server database log) stored on the Meridian application server. At this point in time, the data is considered by Meridian as committed and it can continue its work and the user will experience good responsiveness. A second thread in Accruent SQLIO reads the log files and updates the SQL Server database.

The write-ahead log mechanism maintains the integrity of the data. For example, when data needs to be retrieved by the Meridian application server, it requests the data from the object cache. If the data is not cached, it requests the data from Accruent SQLIO, which first checks whether this data is in the write-ahead log, and only if it is not found does Accruent SQLIO request the data from SQL Server.

If a lot of data is changed over a sustained period of time (for example, as the result of a batch import), the number of Accruent SQLIO log files will grow because they cannot be processed by SQL Server as fast as they are created by the Accruent SQLIO driver. This does not have a detrimental effect on the system performance, but the disk could run out of space if the number of log files keeps growing indefinitely. The maximum amount of space used for all log files can be configured with the **LoggingLimit** setting as described in Prepare the Meridian Server and Vault Configuration.

SQL Server stops processing the Accruent SQLIO log files when the vault is closed after the last client closes its connection to the server. Log files that have not been processed by that time will remain until the vault is reopened and the processing starts again. This is not a serious performance issue because Meridian allows for vaults to become available immediately after reopening them; users do not have to wait for the existing log files to be processed.

Accruent SQLIO uses a service account to communicate with SQL Server. Regardless of the number of users of the system, it uses only one connection to the database.

Create the Vault Database Manually

By default, Meridian creates the SQL Server database for a vault automatically during vault creation as described in Create a New Vault. If this is impractical for your organization, a database administrator can create the database in advance of creating the vault.

To create a vault database manually:

1. Direct a database administrator to create a new SQL Server database with the following requirements:
   - The database name must be the same as the expected vault name and can contain any valid characters.
   - The **INDEX_FILES** filegroup must exist in the database.
   - The `.mdf` file must be named *<VaultName>*`_Data.mdf`.
   - The `.ndf` file must be named *<VaultName>*`_Index.ndf` and must be created in the filegroup **INDEX_FILES**.
   - The `.ldf` file must be named *<VaultName>*`_Log.ldf`.
2. If the default backup location will be used, create a sub-folder named `Backup` in the database folder.
3. Proceed by creating the vault as described in Create a New Vault and specify the same name for the vault as was used to create the database in step 1.
4. Make sure you select the **Database exists** option.

Vault Cache Memory

When a Meridian vault is stored in SQL Server, two levels of caching are in effect instead of just one as when Hypertrieve is used; the Meridian object cache and the SQL Server buffer. For information on configuring the Meridian object cache size, see Configure the MaximumCacheSize Setting and Configure the RelativeCacheSize Setting.

Similarly, we recommend 15 percent of the database size for the size of the SQL Server buffer as a rule of thumb. For information on configuring the SQL Server buffer size, see the SQL Server documentation. When physical memory is scarce, it is best to give priority to the Meridian object cache. This will ensure that queries remain responsive, although the update throughput will be diminished if the SQL Server buffer is smaller than recommended.

Managing SQL Server memory consumption may need special attention. SQL Server is quite aggressive in requesting memory from Windows, and can push the Meridian object cache out of physical memory (if they are both running on the same computer), which will degrade performance and can cause **Out of Memory** errors. To prevent this, limit the maximum amount of memory SQL Server can use. You can set this limit in the SQL Server Enterprise Manager on the **Memory** property page of the SQL Server integrated with Meridian. When calculating this limit, remember that it is for the whole server, including all vaults and other applications using the server.

SQL Server Vault Backups

To back up a SQL Server vault database, use the **Prepare for Backup Wizard** the same as a Hypertrieve vault database as explained in Prepare For Backups. With SQL Server as the database engine, Accruent SQLIO uses the SQL Server backup functions to create the backup files in the vault's `Backup` folder. You can then back up the files in the `Backup` folder with standard backup software.

> **Important!**
> Do not create vault database backups directly with SQL Server Enterprise Manager. The **Prepare for Backup Wizard** in the Meridian Enterprise Administrator must be used in order to first commit the transaction logs that the EDM Server service generates. These are required for a complete backup.

To restore a backup of a SQL Server vault database, restore the backed up files from the backup media to the `Backup` folder and then use the **Restart After Restore Wizard** as described in Restore Backups. This ensures the integrity and compatibility of the database with the host computer.

Integrate With a Separate SQL Server Computer

Meridian can be integrated with a SQL Server installation on the computer where Meridian is also installed or on a separate computer. SQL Server installations on the Meridian computer are detected by the Meridian setup program as described in Install the Server Components.

Note:

- Document content (stream) files are typically stored on the Meridian application server regardless of where the database is located.
- If the network connection between the Meridian application server and the SQL Server computer is interrupted for any reason (for example, SQL Server is restarted), errors can occur. Any pending transactions will not be committed to the database. To resume proper operation, restart the EDM Server service.

To integrate Meridian with SQL Server installed on a separate computer:

1. Set up the Meridian application server as described in Install the Server Components if you have not done so already.
2. For new vaults, create the vault that you want to use with SQL Server as described in Create a New Vault.

   For existing vaults, proceed as described in Migrate a Hypertrieve Vault To SQL Server.
3. Create a subfolder named **Backup** on the SQL Server computer in the path typed for the **Path for Database Files** option in step 2.

   If this subfolder is not created, the backup will fail for this vault.

Configure the Windows Account Used By Meridian

Meridian can use either a Windows account or a SQL Server account to access SQL Server. This account will apply to all vaults that use SQL Server. The type of account used is controlled by the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
Meridian\CurrentVersion\Installed DataStores\MSSQL_<ServerName>_
WindowsAuthenticationMode
```

Where *<ServerName>* is the name of the computer running SQL Server. If the value of **MSSQL_*<ServerName>*_WindowsAuthenticationMode** is **1**, then the account must be a local user account (if SQL Server must be installed on the Meridian server) or a domain user account (if SQL Server is installed on a separate server, for example, DOMAIN\Administrator). If **MSSQL_*<ServerName>*_WindowsAuthenticationMode** is **0**, the account name must be a SQL Server account (for example, **sa**).

> **Important!**
> In an Active Directory domain, this account must be configured as described in Grant Domain Privileges With a Service Account.

By default, Meridian will attempt to access SQL Server using the SQL Server account name **sa** and assumes no password is set for the account. Depending on which type of account you want to use, different methods are required to change the account and its password.

> **Note:**
> Changing the password through the Meridian Enterprise Administrator does not also change the password wherever the account is defined, on the local computer or the domain. If the password of the Windows account must be changed, change it first in on the local computer or the domain and then change it in the Meridian Enterprise Administrator.

To configure a SQL Server account name to be used by Meridian to access SQL Server, see Configure the SQL Server Account Used By Meridian.

To change the Windows account name that is used by Meridian to access SQL Server:

1. In the Meridian Enterprise Administrator, click **EDM Server** in the left pane.

   The active vaults are listed in the right pane.

2. On the **Action** menu and select **Properties**.

   The **EDM Server Properties** dialog box appears.

3. Click the **Engine** tab.

   If the SQL Server database driver was installed during Meridian installation, the ***<DatabaseEngine>*SQL.dll** option appears.

4. Click the **Set Password** button.

   The **Task Account Information** dialog box appears.
5. Type a local or domain user account in **User name**.
6. Type the account password in **Password**.
7. Type the account's domain in **Domain**.
8. Click **OK**.

Create a SQL Server Account For Use By Meridian

Ideally, the SQL Server account used by Meridian should have the **dbcreator** server role. If your organization's security policy prohibits this, you can create an account with the necessary permissions.

> **Note:**
> A custom SQL Server account for use by Meridian may only be created and assigned after the SQL Server database has been created by Meridian as described in Configure the SQL Server Account Used By Meridian.

If you use Meridian Enterprise Server Clusters, the Publisher local user account must also be added to the SQL Server security logins on the Publisher Server PC node. The user should have the same server roles and securables permissions as the SQL Server account used by Meridian. However, if you have configured Enterprise Server to not run as a service on this PC, then the SQL Server account used by Publisher must have a user mapping to the configuration database with the **dbowner** database membership role.

To learn more about these topics, see the following articles in the *Meridian Enterprise Server Administrator's Guide*.

- *Meridian Enterprise Server Clusters*
- *Create the Configuration Database*
- *Configure Meridian Enterprise Server To Not Run As a Service*

To create a SQL Server account for use by Meridian:

1. In SQL Server Enterprise Manager, create a new database user.
2. In the **SQL Server Login Properties** dialog, on the **General** page select **SQL Server Authentication** and the vault database as the default database from the **Database** list.
3. In the **SQL Server Login Properties** dialog, on the **User Mapping** page, select the user and assign the **db_owner** role to the user.
4. In the **SQL Server Login Properties** dialog, on the **Securables** page, select the server you want to configure.
5. Select **Grant** for the following permissions:
    - Alter Any Database
    - Connect Any Database
    - Connect SQL
    - Create Any Database

- External Access Assembly
- View Any Database

6. Configure Meridian to use the new account name as described in Configure the SQL Server Account Used By Meridian.

Configure the SQL Server Account Used By Meridian

Meridian can use either a Windows account or a SQL Server account to access SQL Server. This account will apply to all vaults using SQL Server.

> **Note:**
> SQL Server must be configured with the Mixed Security or Standard Security modes to use a SQL Server account.

Configure the type of account used by Meridian

The type of account used by Meridian is controlled by the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
Meridian\CurrentVersion\Installed DataStores\MSSQL_<ServerName>_
WindowsAuthenticationMode
```

Where *<ServerName>* is the name of the computer running SQL Server. If the value of **MSSQL_*<ServerName>*_WindowsAuthenticationMode** is **1,** then the account must be a local or domain user account (for example, DOMAIN\Administrator). If **MSSQL_*<ServerName>*_WindowsAuthenticationMode** is **0** (default), the account name must be a SQL Server account (for example, **sa**).

By default, Meridian will attempt to access SQL Server using the SQL Server account name **sa** and assumes no password is set for the account. Depending on which type of account you want to use, different methods are required to change the account and its password.

> **Note:**
> SQL Server credentials *cannot* be set with the **Account** property and **Set Password** button present in the **EDM Server Properties** dialog in the Meridian Enterprise Administrator as described in Configure the Windows Account Used By Meridian.

To configure a Windows account name to be used by Meridian to access SQL Server, see Configure the Windows Account Used By Meridian. To configure a SQL Server account name to be used by Meridian to access SQL Server, modify or create (if necessary) registry values in the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
Meridian\CurrentVersion\Installed DataStores
```

The values are described in the following table:

SQL Server account registry values

Value	Type	Description
MSSQL_*<ServerName>*_ WindowsAuthenticationMode	DWORD	If this value is **1**, then the account must be a local or domain user account. If this value is **0** (default), the account name must be a SQL Server account.
MSSQL_*<ServerName>*_ AccountName	STRING	Account name to access SQL Server. Must be of the account type specified by **MSSQL_<ServerName>_ WindowsAuthenticationMode.**
MSSQL_*<ServerName>*_ Password	BINARY	Password for the account specified by **MSSQL_ <ServerName>_AccountName**.

Formatting the registry values

Review the following notes about formatting the registry values:

- If SQL Server is located on the Meridian application server, *<ServerName>* may be omitted, so the values look like: **MSSQL__WindowsAuthenticationMode**, **MSSQL__AccountName**, and **MSSQL__Password**.
- When *<ServerName>* is omitted, the value names must still contain two underscores.
- The value of *<ServerName>* may be specified in any format accepted by SQL Server, for example, **MyServer**, **\\MyServer**, **.\MyInstance**, or **tcp:MyServer\MyInstance,1433.**
- When no vaults yet exist on a separate SQL Server computer, the **sa** account must be used to create the initial vault. If the **sa** account has been deleted by a System Administrator to comply with your organization's security policy, the easiest way to create the initial vault is to temporarily create the **sa** account (with no password) on both the SQL Server computer and the EDM Server computer until after the initial vault has been created and then the account name changed and the **sa** account deleted again.
- The value for **MSSQL_*<ServerName>*_Password** can be either a binary value (default) or a plain-text string value. You can secure a plain-text password by applying permissions to the `Installed DataStores` key with Registry Editor. Be aware that the account that the AutoManager EDM Server service is running under (SYSTEM, by default) must have full access to this value.

Migrate a Hypertrieve Vault To SQL Server

To migrate an existing Hypertrieve vault to SQL Server:

1. Create a new vault as described in Create a New Vault using the options described in the following table.
2. Confirm the migration was successful by checking the new vault for:
    - Total number of documents equal to the source vault
    - Existence of prior revisions
    - Correct status of work in progress documents
    - Documents are visible in the Meridian viewer
    - Custom configuration items
3. To prevent users from accessing the old Hypertrieve vault instead of the new SQL Server vault, delete the Hypertrieve vault in the Meridian Enterprise Administrator.

Vault migration options

Option	Value
Database engine	Microsoft-SQL
Import contents from another vault	Enable
Source Vault	Select the Hypertrieve vault
Copy stream files	Enable
SQL Server computer	Type a SQL Server computer name

After the migration is done, the new vault is ready for use.

The migration can take a significant amount of time, depending on the size of the Hypertrieve database and the number and size of the stream files. The size of the resulting SQL Server database will be about 2.5 times the size of the source Hypertrieve database and can be seen in Windows Explorer in the location specified for the **Path for database files** property of the vault.

Move a SQL Server Vault To a Different Folder

A Meridian vault can be moved to a different folder on the same computer or on another computer (for example, a new hard drive) by importing it into a new vault.

To move a SQL Server vault to a different folder:

- Create a new vault as described in Migrate a Hypertrieve Vault To SQL Server and specify the new location for the vault on the **Configure database engine** page.

To restore a SQL Server vault into a different server and folder:

1. After you install Meridian, update the registry key DefaultDataPath in the following location to point to the new server path, including drive and folder, that you want to use as the default for all vaults:

   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores
2. Restore the vault.

Monitor SQL Server Vault Performance

Because SQL Server is a general purpose DBMS, its performance can vary widely depending on how it is configured. This can have a dramatic effect on the performance of Meridian vaults that use SQL Server. Meridian integrates with SQL Server through its own cache, so monitoring the performance of that cache can provide valuable information to help with tuning SQL Server to work the most effectively with Meridian. Detailed SQL Server monitoring and performance tuning are beyond the scope of this guide. Refer to the SQL Server documentation for more information.

The Meridian cache can be monitored with several performance counters in the **AM HT Page cache** group in the Windows Performance Monitor. The most important ones are:

- **Memory, Kbytes**: The current amount of memory claimed by the cache.
- **Memory Peak, Kbytes**: The peak amount of memory claimed by the cache.

Besides these statistics, also monitor SQL Server memory consumption to detect problems.

When performance problems arise that are not indicated by the counters above, make a Windows Performance Monitor log file with the following counter groups selected and send it to AccruentTechnical Support for analysis:

- AutoManager EDM Server
- AM HT Page cache
- Memory
- Physical Disk
- Process
- Processor
- SQL Server: Buffer Manager
- SQL Server: SQL Statistics
- System

We recommend that you log data for an entire workday, at an interval of 2–5 minutes. We can then analyze the data for known problems and suggest solutions.

Meridian requests large amounts of memory from the operating system. When there is not enough physical memory, Windows will start swapping data to virtual memory. If this happens, performance will drop sharply. You can detect when the system starts swapping by monitoring the **Pages/sec** counter of the **Memory** object.

Minimize SQL Server Log File Size

Depending on the configuration of SQL Server, the SQL Server database log file (`.LDF` file, not to be confused with the Meridian write-ahead `.LOG` files) of a Meridian vault can become very large (up to 100 GB). The reason for this is that the default recovery method of SQL Server is set to Full. If your organization allows the use of the Simple recovery mode, you can truncate the SQL Server log file to optimize performance.

> **Important!**
> Do not change the properties of a SQL Server database that is used by Meridian. Especially do not clear the **Unrestricted file growth** options for **Maximum file size** for either the data files or the transaction log because when the maximum size of the log file is reached, SQL Server cannot write to the database any more, as it is full.

To minimize the SQL Server log file size:

1. Perform a Prepare for Backup operation for every SQL Server vault as described in Prepare For Backups.
2. Open the SQL Query Analyzer included with SQL Server and connect to the SQL Server that is integrated with Meridian.
3. Paste this script into the editor and replace *<DatabaseName>* with the name of the database used by the vault:

   ```
   BACKUP LOG <DatabaseName> WITH TRUNCATE_ONLY
   DBCC SHRINKDATABASE (<DatabaseName>, TRUNCATEONLY)
   ```

   This compresses the `.LDF` file. You can now change the recovery mode to prevent the log from growing again in the future.

   Query the current recovery mode by pasting this script into the editor and replacing *<DatabaseName>* with the same database name you used above:

   ```
   SELECT DATABASEPROPERTY('<DatabaseName>', 'ISTRUNCLOG')
   SELECT DATABASEPROPERTYEX('<DatabaseName>', 'RECOVERY')
   ```

4. If it reports that it is in Full recovery mode, change the recovery mode to Simple by pasting this script into the editor and replacing *<DatabaseName>* with the same database name you used above:

   ```
   ALTER DATABASE <DatabaseName> SET RECOVERY SIMPLE
   ```

If the log file continues to grow after you've implemented these changes, consult a SQL Server database administrator to determine whether other SQL Server settings need to be modified to correct this behavior.

Integrate Meridian With Oracle

The installation and maintenance of a Meridian system based on the embedded Hypertrieve database engine is quite simple when compared to a system based on Oracle. When Oracle is used, additional considerations apply to configuring and administering the system. This section explains how Meridian works with Oracle and the major considerations when administering the system.

> **Note:**
> If the network connection between the Meridian application server and the Oracle computer is interrupted for any reason (for example, Oracle is restarted), errors can occur. Any pending transactions will not be committed to the database. To resume proper operation, restart the EDM Server service.

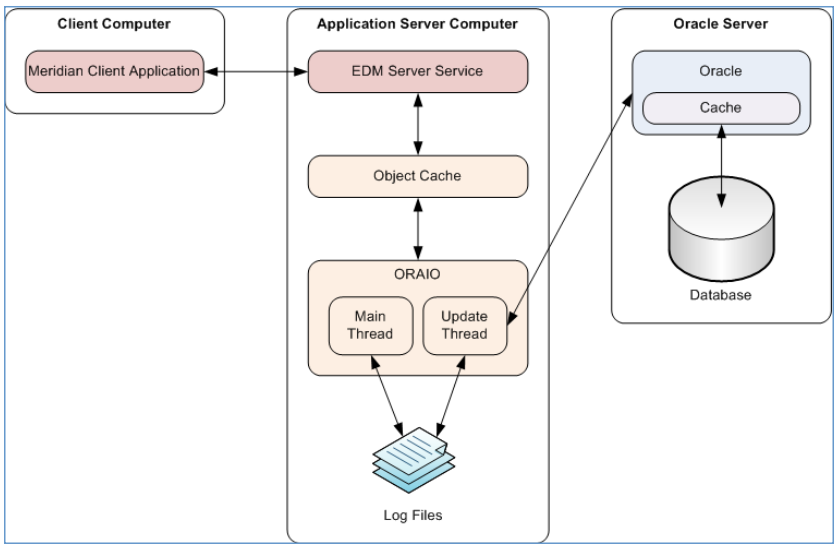
For the Oracle versions supported, see the *Database Management Systems* article in the *Meridian Enterprise Supported Software* document.

How Meridian Works With Oracle

Meridian works with Oracle using two intermediate Meridian components:

- Object cache (`<DatabaseEngine>ORA.dll`): A database-dependent cache that optimizes queries to Oracle.
- ORAIO driver (`HTORAIO.dll`): An Oracle-specific component that interfaces between the object cache and Oracle.

The relationships between these components are illustrated in the following figure.



When a Meridian client sends or requests data from the Meridian application server, the EDM Server service communicates with the object cache , which in turn communicates with ORAIO, which then communicates with Oracle on the Oracle server.

Accruent ORAIO

ORAIO is an Oracle-specific driver that interfaces between the Meridian object cache and Oracle. Every data change inside Meridian needs to be committed to the Oracle database as soon as possible. Due to loads that may be placed on Oracle by other applications and latency induced by the network between the Meridian application server and the SQL Server computer, it can take a significant amount of time for Oracle to commit data changes, which can lead to poor performance. To avoid this bottleneck, ORAIO uses a write-ahead log mechanism illustrated in the figure in How Meridian Works With Oracle.

Instead of directly committing data to Oracle, ORAIO's main thread commits data to log files (not to be confused with the Oracle database log) stored on the Meridian application server. At this point, the data is considered by Meridian as committed; it can continue its work and the user will experience good responsiveness. A second thread in ORAIO reads the log files and updates the Oracle database.

The actual time to process an ORAIO log file is the time it takes to transport its contents to the Oracle server, after which the log file is deleted. If the connection between the EDM Server and the Oracle driver is lost, no transactions are lost; the EDM Server detects the situation, closes down the database driver (all users will get **Database engine unavailable** errors), and leaves the last one or two log files in the log folder. After the EDM Server is restarted and connected to the Oracle database again, it will continue copying the transaction logs to the Oracle server. The only way one or more transactions can be lost is if the EDM Server computer physically crashes; a hard disk stops responding, for example.

> **Note:**
> An EDM Server service transaction is different from an Oracle transaction. Each ORAIO log file equals one EDM Server transaction.

The write-ahead log mechanism maintains the integrity of the data. For example, when data needs to be retrieved by the Meridian application server, it requests the data from the object cache. If the data is not cached, it requests the data from ORAIO, which first checks whether this data is in the write-ahead log, and only if it is not found does ORAIO request the data from Oracle.

If a lot of data is changed over a sustained period of time (for example, as the result of a batch import), the number of ORAIO log files will grow because they cannot be processed by Oracle as fast as they are created by the ORAIO driver. This does not have a detrimental effect on the system performance, but the disk could run out of space if the number of log files keeps growing indefinitely. The maximum amount of space used for all log files can be configured with the **LoggingLimit** settings as described in Prepare the Meridian Server and Vault Configuration. If the total size of all ORAIO log files reaches this limit, performance will drop because new changes will then be committed to the log files only as fast as the existing log files are processed by Oracle. Performance will continue to be affected until the workload of the system diminishes and Oracle

can process the backlog of pending log files. There is one exception to this situation: When the EDM Server places an internal recovery point, log files are not processed by Oracle until the last EDM Server transaction has been committed successfully. This allows the EDM Server to roll back the entire update to the last known good state. For example, this happens when a new Field-Path definition is applied.

Oracle stops processing the ORAIO log files when the the last client closes its connection to the server. Log files that have not been processed by that time will remain until the vault is reopened and the processing starts again. This is not a serious performance issue because Meridian allows for vaults to become available immediately after reopening them; users do not have to wait for the existing log files to be processed.

ORAIO uses an Oracle account to communicate with Oracle. Regardless of the number of users on the system, it uses only one connection to the database.

Vault Cache Memory

When a Meridian vault is stored in Oracle, two levels of caching are in effect instead of just one as when Hypertrieve is used; the Meridian object cache and the Oracle cache. For information on configuring the Meridian cache size, see Configure the MaximumCacheSize Setting and Configure the RelativeCacheSize Setting.

Similarly, we recommend 15 percent of the database size as a rule of thumb for the size of the Oracle cache. For information on configuring the Oracle cache size, see the Oracle documentation. When physical memory is scarce, it is best to give priority to the Meridian object cache . This will ensure that queries remain responsive, although the update throughput will be diminished if the Oracle cache is smaller than recommended.

Oracle Vault Backups

There are many ways to create database backups using Oracle, and it is normally the responsibility of an Oracle database administrator to configure the backups to best meet the organization's requirements.

> **Important!**
> Do not create vault database backups with the Oracle tools without first running the **Prepare for Backup Wizard** in the Meridian Enterprise Administrator, either interactively or as a scheduled task. The **Prepare for Backup Wizard** must be used in order to first commit the transaction logs that the EDM Server service generates. These are required for a complete backup.

We recommend the following procedure for backing up Oracle vaults:

1. Set the **UseCompatibleBackup** registry value as described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<vaultname>\CompoundItemService depending on whether or not you will use the Oracle tools to create a snapshot of the vault data.
2. Choose between two options:
   - If **UseCompatibleBackup** is set to **0**:

     Use the **Prepare for Backup Wizard** the same as for a Hypertrieve vault database as explained in Prepare For Backups. You can then back up the files in the `Backup` folder with standard backup software.
   - If **UseCompatibleBackup** is set to **1**:
     a. Run the **Prepare for Backup Wizard** either interactively or as a scheduled task.
     b. Disable and stop the **EDM Server** service with one of the following methods:
        - Microsoft Management Console (MMC)
        - The **EDM Server** properties in the Meridian Enterprise Administrator
        - A command line window or batch file (preserve all spaces shown below):

          ```
          sc \\. config EDM_SERVICE start= disabled
          net stop EDM_SERVICE
          ```

     c. Back up the Oracle database with the Oracle tools.
     d. Back up the contents of the vault's `Backup` folder, the Oracle backup files, and the vault stream files to backup media with standard backup software.
     e. Restart the EDM Server services that were stopped in step b using one of the methods listed in step b.

To restore a backup of an Oracle vault database, restore the backed up files from the backup media to the `Backup` folder, restore the Oracle database, and then use the **Restart After Restore Wizard** as described in Restore Backups.

EDM Server Service Account Requirements For Oracle

Meridian uses a specific Oracle account to create the first vault in an Oracle instance. The account name must be **MERIDIAN** (upper case) and the initial password must be **MANAGER** (upper case).

> **Note:**
> The release of Oracle 11g introduced new password policies. Oracle passwords are case-sensitive by default. A new Oracle option **SEC_CASE_SENSITIVE_LOGON** can be used to change this behavior. For more information about this, see the Oracle documentation. Passwords also expire after 180 days by default and a 90 day grace period.

The minimal privileges for this account are:

- **Create Procedure**
- **Create Sequence**
- **Create Session**
- **Create Table**
- **Unlimited Tablespace**

The Oracle roles that include these privileges are **DBA** and **CONNECT**. Although **Unlimited Tablespace** can be replaced with a quota, this can potentially be dangerous. If Meridian runs out of table space, the vault will be corrupted and must be restored from backup, potentially losing valuable data. The MERIDIAN account should always be able to store data in the Oracle database. To make sure that there is always enough space for MERIDIAN to store data in Oracle, do not use space limits on the data files or use large values for the **Initial** and **Next** size. It should be the responsibility of an Oracle database administrator to ensure that the MERIDIAN user in Oracle always has enough space to store data.

The EDM Server service will always use the account MERIDIAN to create the tables needed to store the vault metadata. The user MERIDIAN is therefore also the owner of these tables and should not be removed from the database.

When Oracle and Meridian are located on separate computers, the computer running the EDM Server service must be able to access the remote Oracle instance. You can do this either with the Net Configuration Assistant or editing the `tnsnames.ora` file directly. Refer to the Oracle documentation for more information.

After an Oracle instance has been created, a Meridian vault can be created in it. This is done in the usual way as described in Create a New Vault. After the creation of the first Oracle vault, you can change the password for the user MERIDIAN in the Meridian Enterprise Administrator. This will change the password in Oracle as well.

Configure the Oracle Account Used By Meridian

Meridian must use the MERIDIAN account to create the first vault in an Oracle instance. Afterward, the account name and/or password may be changed, if necessary to comply with your organization's security policies. We recommend that you set it to the account described in Grant Domain Privileges With a Service Account.

To change the Oracle account name or password used by Meridian to access Oracle, modify or create (if necessary) registry values in the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
Meridian\CurrentVersion\Installed DataStores
```

The values are described in the following table:

Oracle account registry values

Value	Type	Description
ORA_ *<InstanceName>*_ AccountName	STRING	Account name to access Oracle.
ORA_ *<InstanceName>* _ Password	BINARY	Password for the account specified by **ORA_*<InstanceName>*_ AccountName**

If Oracle is located on the Meridian application server, *<InstanceName>* may be omitted, so the values look like: **ORA__AccountName**, and **ORA__Password**. When *<InstanceName>* is omitted, the value names still contain two underscores.

> **Note:**
> The value for **ORA_*<InstanceName>*_Password** can be either a binary value (default) or a plain text string value. You can secure a plain-text password by applying permissions to the **Installed DataStores** key with Registry Editor. The account that the Accruent EDM Server service is running under (SYSTEM, by default) must have full access to this key.

Configure ODAC for Oracle

If you use an ODAC version newer than version 12, you will need to follow the procedures below. The reason is because newer versions of ODAC do not automatically register their own provider in the Global Assembly Cache (GAC). If you do not follow these procedures, even some of the most basic Meridian functionality will not work.

Prerequisites

To successfully complete these procedures, you must first download the following files:

- the .NET Framework Software Development Kit (SDK) for the version of .NET you want to use
- an Oracle ODAC version between version 11.2 and 12.2
- If you want to use a newer ODAC version (18 or higher), you can also download that version. However, you **must** have a version between 11.2 and 12.2 for Meridian Enterprise to function properly.

  We recommend you download the XCopy ODAC packages, because you will also need the ODP.NET components. The ODP.NET (Oracle.DataAccess) installation should be compatible with the client. For instance, the latest **64-bit Unmanaged ODP.NET 19.10**, download includes the Oracle Instant Client. See the readme documentation included with the download. More than one Oracle client can be installed and configured to use by different executables on the same machine.

Configuration

To configure ODAC for Oracle:

1. Install the .NET Framework Software Development Kit (SDK) using the Windows SDK installation.

   You will use the Global Assembly Cache tool (gacutil.exe) from this SDK file.
2. Add the following values to your system PATH environment variable, separated by semicolons:
   - **c:\Oracle**

     This assumes that you will install ODAC to c:\Oracle.
   - **c:\Oracle\bin**

- **%SystemRoot%\system32**
- **c:\Program Files (x86)\Microsoft SDKs\Windows\v10.0A\bin\NETFX 4.6.1 Tools**

  Use the proper location of your Windows SDK tools.
- **c:\Program Files (x86)\Microsoft SDKs\Windows\v10.0A\bin\NETFX 4.6.1 Tools\x64**

  Use the proper location of your Windows SDK tools.

3. Create a folder named **temp** in your **C** drive.
4. Create a folder named **oratemp** in the **temp** folder you created in the previous step.
5. Unzip the ODAC zip file to **C:\temp\oratemp**.
6. Open a Windows command prompt window.
7. Change your current working directory using the following command:

```
cd c:\Temp\oratemp
```

8. Execute a command using the below syntax:

```
install.bat [Oracle Data Provider for .NET 4] [Your installation directory path] odac true
```

The `odac` argument is the Oracle Home Name that is used for the registry keys, and the `true` argument communicates the dependency with the Oracle Instant Client. A properly formatted example appears below:

```
install.bat odp.net4 c:\oracle odac true
```

9. Change your current working directory using the following command:

```
cd c:\Oracle\odp.net\bin\4
```

10. Execute the following command:

```
OraProvCfg /action:gac /providerpath:"c:\Oracle\odp.net\bin\4\Oracle.DataAccess.dll"
```

11. Change your current working directory using the following command:

```
cd c:\Oracle\odp.net\PublisherPolicy\4
```

12. Execute the following command:

```
gacutil /i "c:\Oracle\odp.net\PublisherPolicy\4\Policy.4.112.Oracle.DataAccess.dll"
```

The 4.112 publisher policy is used to redirect the GAC to use the latest installed version of ODP.NET.

13. Check that your Global Assembly Cache (GAC) appears in the following locations:
    - c:\Windows\Microsoft.NET\assembly\GAC_64\Oracle.DataAccess\v4.0_4.122.19.1__89b483f429c47342\oracle.dataaccess.dll
    - c:\Windows\Microsoft.NET\assembly\GAC_64\Policy.4.122.Oracle.DataAccess\v4.0_4.122.19.1__89b483f429c47342\Policy.4.122.Oracle.DataAccess.config
    - c:\Windows\Microsoft.NET\assembly\GAC_64\Policy.4.122.Oracle.DataAccess\v4.0_4.122.19.1__89b483f429c47342\Policy.4.122.Oracle.DataAccess.dll
14. Check that the following registry keys have been created:
    - HKLM\SOFTWARE\Oracle\KEY_odac
    - HKLM\SOFTWARE\Oracle\ODP.NET\4.122.19.1
15. Restart your PC.
16. Use the Windows Process Explorer to confirm that the **oracle.dataaccess.dll** file is correctly mapped to the following services:
    - BlueCieloECM.EnterpriseService.exe
    - w3wp.exe

Migrate a Hypertrieve Vault To Oracle

To migrate an existing Hypertrieve vault to Oracle:

1. Create a new vault as described in Create a New Vault using the options described in the following table.
2. Confirm that the migration was successful by checking the new vault for:
    - Total number of documents equal to the source vault
    - Existence of prior revisions
    - Correct status of work in progress documents
    - Documents are visible in the Meridian viewer
    - Custom configuration items
3. To prevent users from accessing the old Hypertrieve vault instead of the new Oracle vault, delete the Hypertrieve vault in the Meridian Enterprise Administrator.

Vault migration options

Option	Value
Database engine	Oracle
Import contents from another vault	Enable
Source Vault	Select the Hypertrieve vault
Copy stream files	Enable
Oracle instance name	Type an Oracle instance name

After the migration is done, the new vault is ready for use.

The migration can take a significant amount of time, depending on the size of the Hypertrieve database and the number and size of the stream files. The size of the resulting Oracle database will be about 2.5 times the size of the source Hypertrieve database and can be seen in Windows Explorer in the location specified for the **Path for database files** property of the vault.

Restore an Oracle Vault To Another Server

An Oracle vault can be moved to another computer (for example, as a server upgrade) by restoring a backup of the vault made on the original server so long as the vault folder names and paths remain the same.

Important!

It is not possible to move (by restoring from backup) a vault from a pre-Windows Server 2008 computer (including Windows XP, Windows Server 2000, or Windows Server 2003) to a post-Windows Server 2008 (including Windows Vista) or later computer without adverse side effects.

The possible side effects include folders and documents not being accessible, and vault corruption. The cause is Windows API functions that behave differently between pre-Windows Server 2008 and post-Windows Server 2008 operating systems.

There are two supported methods to move an existing vault from a pre-Windows Server 2008 computer to a post-Windows Server 2008 computer:

- Import the vault from the source server into a new vault on the post-Windows Server 2008 computer.
- Restore a backup of the vault from the source server onto the new server and reindex the vault with the icosnlsver tool as described in Change Operating System Versions. Migration assistance is available from Accruent Partners and Accruent Technical Support.

To restore an Oracle vault to another server:

1. On the existing Meridian server, back up the existing vault.
2. On the existing Oracle server:
    a. Back up the vault data.
    b. Check for uncommitted EDM Server transaction log files.

        There must not be any uncommitted log files before exporting the Oracle data later in this procedure. Check using one of the following methods:

        - Check the vault root folder on the Meridian server. The folder should not contain any log files
        - Check the Oracle table named <*vault name truncated to 11 characters*>_ LOGFILES.

            The table should be empty. This is the preferred method.

    c. Export the Oracle vault data.

Unfortunately, the Oracle **exp** tool does not support parameters to export triggers, sequences, and so on. Likewise, the **TABLES** parameter will not export objects like triggers, views, sequences, and so on. The only way for a dump file to contain the sequences and triggers is to export the full contents of the database or export the entire schema.

If you specify the parameter **FULL=Y** in an export, you will get all triggers, procedures, views, sequences, and so on. If you specify **OWNER=<***user name***>** as a parameter to an export, you will get all objects that are owned by that user, including triggers.

With Oracle 10*g* or later, you can choose between using the old **imp** and **exp** tools or the Datapump tools named **expdmp** and **impdmp**. These new tools introduce much-needed performance improvements, network-based exports and imports, and so on. If you use an export script, make sure you log the output to a log file. All DDL statements in the export dump will be logged. Check that the following data and structures have been exported:

- Sequences and indexes
- Tables
- **AM_DATASTORES**: Common table for all vaults belongs to the MERIDIAN schema

d. Copy the `.dmp` file to a safe location on the new server from which to import it later.

3. On the new Oracle server:

a. Create and configure the new Oracle instance, if necessary, with the Oracle Database Configuration Assistant or with scripts.

> **Note:**
> Before importing the dump file, you must first create the tablespaces. Otherwise, the import will create the corresponding data files in the same file structure as the source database, which may not be compatible with the file structure on the new system. If the folder structure for tablespaces is different on the new server, you must create the tablespaces first.

b. Create the schema for the Meridian vault with user name MERIDIAN and password MANAGER.

Following is an example script:

```
sqlplus SYS/ORATEST@ORATEST AS SYSDBA
CREATE USER "MERIDIAN" PROFILE "DEFAULT" IDENTIFIED BY
"MANAGER" DEFAULT TABLESPACE "USERS"
TEMPORARY TABLESPACE "TEMP" ACCOUNT UNLOCK
GRANT CREATE ANY PROCEDURE TO "MERIDIAN"
GRANT CREATE ANY SEQUENCE TO "MERIDIAN"
GRANT CREATE ANY TABLE TO "MERIDIAN"
GRANT CREATE SESSION TO "MERIDIAN"
```

```
GRANT UNLIMITED TABLESPACE TO "MERIDIAN"
GRANT "CONNECT" TO "MERIDIAN"
GRANT "DBA" TO "MERIDIAN"
```

c. Check that the vault-related data and structures are present in the .DMP file created in step 2.c by using the **SHOW=Y** parameter with the **imp** tool.

   This information is needed to re-create vault-related sequences after importing. Following is an example script.

```
set HOMEVAULTDIR="D:\AMM\IC-Meridian vaults"
set DUMPFILE=%HOMEVAULTDIR%\Meridian.dmp
set LOGFILE=%HOMEVAULTDIR%\ShowMeridian.log
rem Show TABLES for ALL vaults (SCHEMA)
imp USERID="""SYS/ORATEST@ORATEST as SYSDBA""" SHOW=Y
FROMUSER=MERIDIAN TOUSER=MERIDIAN
FILE="""%DUMPFILE%""" LOG="""%LOGFILE%"""
```

d. Restore vault data on the new Oracle instance using the dump file created in step 2.c.

   You need to restore:

   - The vault-related table set (18 tables for each vault). Vault-related table names have prefixes that match the vault name truncated to not more than 11 characters.
   - The **AM-DATASTORES** table. This table is common to all vaults in the schema. Each row in this table defines the table name prefix to vault name mapping for each vault.
   - Vault-related sequences and indexes.

   Following is an example script.

```
set HOMEVAULTDIR="D:\IC-Meridian Vaults"
set DUMPFILE=%HOMEVAULTDIR%\Meridian.dmp
set LOGFILE=%HOMEVAULTDIR%\ImpMeridian.log
rem Show TABLES for ONE vault ONLY
imp USERID="""SYS/ORATEST@ORATEST as SYSDBA"""
FROMUSER=MERIDIAN
TOUSER=MERIDIAN TABLES=(TESTORAVAUL%%, AM_DATASTORES)
FILE="""%DUMPFILE%""" LOG="""%LOGFILE%"""
```

e. Create, re-create, or alter the vault-related number sequences.

   Sequence numbers need to be set or reset to the value captured in the exported dump file as reported in step 3.c. Following is an example script.

```
create sequence "MERIDIAN".TESTORAVAUL_COMPARTMENTNUMBER
minvalue 1 maxvalue 999999999999999999999999999
increment by 1 start with 2041 order nocycle ;
```

4. On the existing Meridian server, change the value of the following registry key to specify the new Oracle instance:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<vaultname>\CompoundItemService\InstanceName`

   > **Note:**
   > The Oracle server name and port number can be specified in **InstanceName** in the form //<*ComputerName*>:<*Port*>/<*ServiceName*>. This is called EZCONNECT and should be configured in the `sqlnet.ora` file to work properly. This method is convenient in that you do not have to create and manage a `tnsnames.ora` file to configure the Oracle database connection.

5. Repeat this procedure for each vault to be restored.

Integrate Meridian With Meridian Enterprise Server

Meridian can be easily integrated with Publisher and Meridian Explorer to create a powerful engineering content publishing environment. For more information about the capabilities of Publisher and Meridian Explorer, see Meridian Enterprise Introduction. For more information about the architecture and requirements of such a system, see the *Meridian Enterprise Server Administrator's Guide*.

The following topics describe how Meridian can be integrated with Meridian Enterprise Server (the Publisher and Meridian Explorer application server).

Configure a Vault For Publisher

After the Publisher components have been installed during Meridian Enterprise Server setup, the vaults that will serve as source or destination systems must be configured.

See our Document Synchronization Methods Overview to learn about the three methods you can use to synchronize document contents, title blocks, and references with PowerWeb.

To configure the Meridian Enterprise application server:

1. In the Meridian Enterprise Administrator, click **EDM Server** in the left pane.

   The active vaults are listed in the right pane.
2. Select the vault that you want to configure in the right pane.
3. On the **Action** menu, select **Properties**.

   The vault's **Properties** dialog box appears.
4. Click the **Advanced Features** tab.

   The **Advanced Features** page appears.
5. Select **Enable Publisher extension**.
6. Click **OK**.
7. In Meridian Enterprise Configurator, expand **Environment** in the configuration tree and select **Vault Settings**.

   The vault's configuration pages appear.
8. Click the **Enterprise Server** tab.

   The Publisher configuration options appear.
9. Click **Edit**.

   The page becomes editable.
10. Click options or type values using the descriptions in the following table.
11. Click **OK**.
12. Grant the privileges described in *Security Permission Descriptions* in the *Meridian Enterprise Server Administrator's Guide*to the Meridian Enterprise roles that you want to allow to use the publishing commands.

    For more information on granting security privileges, see *Managing Security Roles* in the *Meridian Enterprise Configuration Guide*.

Publisher configuration options

Option	Description
Prevent duplicate registration	Ignores new publishing tasks for documents for which publishing tasks already exist in the queue. This option is not available if the Publisher database is hosted by an Oracle server. If enabled, **Fail the whole batch operation when any duplicate is found** will cause the publishing job to be revoked if duplicate documents are detected within a batch submitted using the VBScript methods of the **MeridianQueue** object described in *Registering Programmatically Without the Task Server* in the *Meridian Enterprise Server Administrator's Guide*.
Synchronize rendition lookup lists	Populates the **Rendition Page Pen Table**, **Rendition Page Size**, and **Rendition Page XOD Resolution** lookup lists with values retrieved from the Meridian Enterprise Server computer. The lookup lists are described in the following table.

Option	Description
Publisher Jobs	Select the names of publishing jobs to use for the following tasks: • **Create rendition**: Publishing job used for the **Update Rendition** action • **Write title block properties**: Publishing job used for the **Properties to File** action • **Read title block properties**: Publishing job used for the **Properties from File** action • **Synchronize references**: Publishing job used for the **References from File** action To learn more about each of these actions, see the following articles in the *Meridian Enterprise User's Guide*: • *Update Renditions* • *Synchronize File Properties* • *Synchronize References* To learn more about publishing jobs and how to configure them, see the *Publishing Jobs* section in the *Meridian Enterprise Server Administrator's Guide*. If the **Create rendition** publishing job occurs too close in time to one of the other publishing job types, a conflict can arise where one or more jobs are trying to access the same file. This may result in the rendition failing, or the rendition may not include updated title blocks or references. To ensure the title block is updated before a rendition is created, on your rendering profile, ensure that the **Update title blocks before rendering** setting is selected. To learn how to configure this setting, see the appropriate rendering profile article in *Rendering Profiles* in the *Meridian Enterprise Server Administrator's Guide*. If a file is locked during rendering, you may see an error message in the rendition process log that starts with the phrase, "no storage available". To avoid issues with a locked file preventing a rendition from being generated, increase the values of the following settings in the **C:\ProgramData\BlueCieloECM\EnterpriseServices\PublishingCapability.dat** file: • **RetryWriteRendition**: Number of times that Publisher will retry a rendition before the rendition fails • **WaitWriteRendition**: Number of seconds that Publisher will wait before a retry is attempted These settings only take effect when a file is locked, and they should not impact overall system performance. To learn more about the settings in the **PublishingCapability.dat** file, see the *PublishingCapability.dat* article in the *Meridian Enterprise Server Administrator's Guide*.

The rendition lookup lists provide values for the properties in the **Rendition Properties** property set and appear on the **Rendition** property page in the Meridian Enterprise client applications. The **Rendition** property page appears when the **Use renditions** option has been enabled for the vault

in the Meridian Enterprise PowerUser client. The lookup list values may be modified to meet specific requirements.

Rendition property set lookup lists

Name	Description
Rendition Page Color	Color depths to render to: **Color** or **Black and white**.
Rendition Page Layout	Views available within the source documents to render.
Rendition Page Orientation	Orientations of the page to render to: **Landscape** or **Portrait**.
Rendition Page Pen Table	Pen settings filenames to apply to the renditions. Applicable only if the publishing job is configured to use pen settings. Filenames are those that are available on the computer. The location of these files depends on which rendering application you use. • The Teigha files are stored in: `C:\Program Files\BC-Meridian\BC Enterprise\Teigha.net`
Rendition Page Size	Sizes of the pages to render to. Values are retrieved from the printing settings of the Meridian Enterprise Server computer when the **PublishDocumentUIExtension** extension is configured. The Microsoft default page sizes may not include the page sizes that your users need. In that scenario, you will need to set up custom page sizes on the Enterprise Server and Publisher machines. The process for setting up custom page sizes depends on which Windows features have been installed on the Servers. Our experts recommend using a tool such as Microsoft's **Print Management Console**, which is available as an optional feature for Windows. Learn how to use the Microsoft Print Management Console to add custom page sizes.
Rendition Page XOD Resolution	Resolutions at which to render documents. Lower values may lack sufficient clarity. Higher values may cause slower viewing. These values are retrieved from the rendering profile that resides in Meridian Enterprise Server when the **Synchronize rendition lookup lists** option described above is enabled. If this lookup list is empty after synchronization, scan the rendering profile as described in the *Create and edit a rendering profile* article in the *Meridian Enterprise Server Administrator's Guide* and then run the synchronization job again to repopulate the list with values.

In VBScript, use the **User.HasPrivilege** method with the **Can Publish** privilege to verify whether a user should be allowed to publish a particular document.

Create Custom Page Sizes for Meridian Enterprise

The default Microsoft page sizes may not include the page sizes that your users need. In that scenario, you will need to set up custom page sizes on the Enterprise Server and Publisher machines.

The process for setting up custom page sizes depends on which Windows features have been installed on the Servers. Our experts recommend using a tool such as **Print Management**, which is available as an optional feature for Windows.

Enable Print Management Console

To enable the **Print Management Console**:

1. Navigate to **Start** > **Settings** > **Apps** > **Optional features** > **Add a feature**.
2. Select **Print Management Console**.
3. Click **Install**.

   Once installation is complete, you can access the **Print Management Console** from the **Start** menu.

Create Custom Page Sizes

To create custom page sizes:

1. Open the **Print Management Console**.
2. Expand **Print Servers** and expand the name of the server you want to configure.

   You will need to do this process for your Enterprise Server and Publisher machines.
3. Right-click **Forms** and select **Manage Forms** from the menu that opens.

   The **Printer Server Properties** window opens.
4. Select **Create a new form**.

   The fields in the window become editable.
5. Enter the name of the page size you want to create in **Form name**.

   > **Important!**
   > The Meridian Enterprise Configurator is case-sensitive, so you will need to enter the name of the page size in Configurator exactly as how it is written in the **Form name** field.
6. Enter the dimensions of your custom page size.

7. Click **Save Form**.
8. Click **Close**.

   Your page size appears in the **Forms** section of the **Print Management Console**. To view the full list of page sizes, click **Forms** in the menu.

Add Custom Page Sizes to Configurator

You may want to remove unnecessary page sizes so that your users do not select one that is incorrect.

To add the custom page sizes you created to the Configurator:

1. In Configurator, expand **Lookup Lists** in the configuration tree to display the existing lookup lists.
2. Select the **Rendition Page Size** lookup list.

   This lookup list is automatically created when the Publisher module is enabled for the vault. The values are populated automatically the first time you connect the vault to a rendition job.
3. Click **Edit**.
4. Click the **Entries** tab.

   The existing page sizes are shown.
5. Choose between two options:
   - To add a custom page size:
     a. Click **Add Entry**.

        The **Add lookup list entry** dialog opens.
     b. Enter the name of the page size.

        The Configurator is case-sensitive, so you will need to enter the name of the page size exactly as how it was entered in the Create Custom Page Sizes procedures above.
     c. Click **OK**.
   - To remove a custom page size, click **Remove Entry**.

     The entry is removed.
6. Click **Apply**.

   Your changes are saved.

Configure the Connection To Meridian Enterprise Server

Meridian Enterprise can connect to a Meridian Enterprise Server computer to share a number of services in common:

- User and group management
- License management
- Audit log database
- Discussion comments and redlines from Meridian Explorer

This is valuable to administer both Meridian and Meridian Explorer from a single, central location, particularly if it is linked to your Microsoft Active Directory. These features are used for all vaults that are hosted by the same server.

To configure the connection to Meridian Enterprise Server:

1. In the Meridian Enterprise Administrator, select **EDM Server** in the left pane.
2. Click **Properties** on the **Action** menu.

   The **EDM Server Properties** dialog box appears.
3. Click the **Settings** tab.

   The Meridian Enterprise Server connection options appear.
4. Click options or type values using the descriptions in the following table.
5. Click **OK**.
6. Restart the **EDM Server** service.

Meridian Enterprise Server connection options

Option	Description
Computer running the Enterprise services	Specify a computer and account name using the following syntax: Host=<*ServerName*>;Port=<*Number*>;UPN=<*Domain*>\<*Account*>;Password=<*Password*> The port number and password are optional. If a password is specified, it is saved encrypted. You may also specify the port number using the syntax: <*ServerName*>:<*Port*> If any of the following are true: • Meridian Enterprise and Meridian Enterprise Server are running on the same computer • A site cache is not used • Renditions are not generated for the vault The computer name can be simplified to one of the following formats or you can click **Browse** and select the name of the Meridian Enterprise Server computer in your domain: • Simple name (**MyServer**) • Fully qualified domain name (**MyServer.MyDomain**) • IP address (**127.0.0.1**, **localhost**)
Use Enterprise Server for user management	If enabled, Meridian Enterprise security will use the groups and users that are defined in Meridian Enterprise Server Administration Console on the computer specified for the **Computer running the Enterprise services** option instead of in Meridian Enterprise Configurator. Changes to the users and groups can be made from either application. For information on managing users and groups in Meridian Enterprise Server, see *Meridian Enterprise User Administration* in the *Meridian Enterprise Server Administrator's Guide*. When this option is enabled, the reserved word **$$UserDB** cannot be used in VBScript with the **Vault.ExecSQL** method to access the Meridian Enterprise Server user database.

Option	Description
Use Enterprise Server for the audit log	If enabled, Meridian Enterprise actions will be logged to the audit log database in Meridian Enterprise Server running on the computer specified for the **Enterprise Server web server** option. The actions are combined with the Meridian Enterprise Server actions that are also logged. For information on viewing the Meridian Enterprise Server audit log, see View the Audit Log in the *Meridian Enterprise Server Administrator's Guide*. Alternatively, the audit log database can be stored in a separate, standalone database instead. The data can then be viewed using an audit log viewer web application that can be installed. For information about setting the audit trail database connection in Meridian and installing the audit log viewer web application, see Install the Audit Log Viewer.

Local Workspace

Local Workspace is the name for a folder on client computers that contains copies made by the Meridian client applications of recently accessed vault documents. The folder also contains a small database that tracks the files that are contained in the Local Workspace. As documents are checked out or viewed, they are copied to the user's Local Workspace folder for use, thus providing a local caching mechanism.

Large assemblies or other complex related documents cause a lot of network traffic when viewed or opened in their applications because all related documents must be opened before the composite document can be viewed or opened. Therefore, we always recommend implementing Local Workspace in such circumstances.

Local Workspace is enabled by default for new vaults.

When is a document copied to the Local Workspace?

A document will be copied to Local Workspace if it is accessed under the following circumstances:

- **If a document is selected for viewing.**

  This will also copy all referenced files. The files are made read-only in Local Workspace. The first time this is done, the user will see no benefit because the files are downloaded from the Meridian application or file server. However, if the user views one of these files again later, the performance will be dramatically improved because the file and all its references are retrieved from Local Workspace instead of from the Meridian application server or file server. This is particularly important when viewing large or complex 3D model files such as created by Autodesk Inventor or SolidWorks.

  > **Note:**
  > You can confirm that a document is being opened from Local Workspace by examining the **Local Copy** property on the **Document** property page of the document in PowerUser. The property will contain the modification date and time of the file.

- **If a document is checked out by a user for editing.**

  The file and its references are initially copied to Local Workspace read-only. However, when the document is opened for editing in an application, it is made writable and the document is locked in the Meridian vault against change by other users.

- **The user manually synchronizes property or reference data using the commands in PowerUser.**

When is a document copied from the Local Workspace?

Files will be copied from the Local Workspace if they do not yet exist or if the versions in Local Workspace are older than the versions in the vault.

Changed documents in the Local Workspace are synchronized with the vault in the background at a time interval set by the user. This is an important difference between Meridian and a simple manual check-out/check-in system. The synchronization is automatic, transparent to the users, and secure.

Advantages and Disadvantages

Local Workspace has the following advantages:

- There is less load on the Meridian application server or file server.
- There is much less network traffic when viewing, opening, or saving files, which increases performance.
- Larger data files such as complex assembly models open much faster.

Of course, there are also some disadvantages:

- If a conflict occurs during synchronization, user intervention is needed to take the appropriate action.
- Referenced documents cannot be found if the references do not exist in the vault.

Filepath Length Recommendations

Although the Local Workspace itself does not impose a limitation on the length of the paths to documents, other programs that might need to work with the documents (application links, viewers, and so on) may be limited to approximately 256 characters. The fully-qualified path of a document in Local Workspace comprises several elements:

*<LocalWorkspaceLocation>**<UserName>*
<Server,Datastore,ContextID,RevisionID>
*<VaultPath>**<FileName>*.*<Ext>*

For example:

```
C:\BC-Workspace\John Doe\M-MyServer,
D-Engineering,P-AMContext1,
W-b9A04B874B60FE440\Projects\P1000
\Foundation Plans\D1000201.dwg
```

For this reason, we recommend that all paths within vaults be maintained at 190 characters or less so as to not result in Local Workspace paths over 256 characters.

32-bit vs. 64-bit Configurations

By default, Meridian running on 32-bit computers uses the Microsoft Jet database engine to create and maintain the Local Workspace database. On 64-bit computers where 64-bit Microsoft Jet is not available, the Local Workspace uses SQLite. SQLite is provided as an option during client installation. Which database engine is used can be set with the **WorkSpaceDB** registry setting in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client.

Use Local Workspaces in Remote Mode

By default, users that work in PowerWeb or in PowerUser in Remote mode require and are granted read/write access to a Local Workspace location on the Meridian web server. If you move the location of the Local Workspace by setting the path in the **WorkSpaceLocation** value described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client, then you must manually grant read/write access to the **Authenticated Users** group to the new location for the application links to work correctly.

The location is only maintained by the settings described in Optimize Local Workspace Configuration for the account under which Application Integration is run on the web server. To maintain the location for all PowerWeb users, see the **WorkSpaceNoUserName** registry value described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client.

Optimize Local Workspace Configuration

The configuration of the local workspace options is done on the client computers by users as described in the *Configure local workspace* article in the *Meridian Enterprise User's Guide*. However, these options can have an adverse impact on performance under specific circumstances, in particular when the local workspace is larger than necessary. The primary options affecting overall system performance are:

- **Start synchronization every**
- **Maximum amount of disk space to use for local workspace** (the size can also be set in the **CacheSize** value described in HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMSync\Settings)

Meridian application server performance can be adversely affected when large numbers of documents are stored in users' local workspaces and synchronization is occurring at the default setting of every 30 minutes. Even with the local workspace option **Synchronize recently accessed writable documents only** enabled, the system will still verify the synchronization of every document in the local workspace folders. Verifying the synchronization of excessive numbers of documents can cause poor performance of the Meridian application server, resulting in poor client performance.

Best Practice Recommendations

We recommend that you advise users to configure their local workspace options as follows:

- Local workspace disk space should be reduced for users experiencing poor performance. Lowering the **Maximum amount of disk space to use for local workspace** setting will reduce the size of the local workspace on the user's computer and the number of documents that need to be synchronized. A size of 750 MB is usually enough.
- The **Start synchronization every** setting can be increased to a number higher than the default of 30 minutes. This will reduce the frequency of local workspace synchronization attempts with the Meridian application server, especially during periods of heavy usage when performance is most important.

Changing these settings on a client computer will take effect immediately and will not cause any active documents in the local workspace to be purged from the disk. When the **Maximum amount of disk space to use for local workspace** setting is reduced for an active local workspace, the system will only remove documents that are not under change by the user.

How Local Workspace affects disk space

The local workspace, the Windows temporary folder, and the application temporary files folder are used on Meridian Enterprise Server rendering computers but the disk space is not reclaimed automatically as it is on normal client computers.

By default, the Windows temporary files folder is specified by the Windows environment variable as `%WINDIR%\TEMP`. By default, the application temporary files folder is specified by the `%TEMP%` environment variable and is set to `C:\Users\<AccountName>\AppData\Local\Temp` where *<AccountName>* is the name of the Meridian service account.

To prevent errors caused by running out of disk space, you should periodically clean these folders with a scheduled task to run a command file, script, or third-party utility. We recommend that you also schedule a task to clean the local workspace for the Meridian service account as described in the *Cleaning the local workspace article* in the *Meridian Enterprise Server Administrator's Guide*.

Local Workspaces in Offline or Remote Mode

Local workspace performance can be affected by how Meridian synchronizes the local workspace with the application server: Online mode, Offline mode, or Remote mode as described in the *Offline mode and Remote mode* article in the *Meridian Enterprise User's Guide*.

These modes affect the following client registry values as described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client

Local Workspace mode registry values

Mode	Offline Mode	WebServicesMode	Description
Online	0	N/A	For LAN use only. Documents are stored in the Local Workspace folder, metadata is synchronized in real-time, and Local Workspace is automatically synchronized to the Meridian application server using RPC/DCOM.
Remote	1	1	For WAN or Internet use. Documents are stored in the Local Workspace folder, metadata is stored in the Local Workspace database, and both are automatically synchronized to the Meridian web server in real-time using HTTP.

Mode	Offline Mode	WebServicesMode	Description
Offline	1	0	For worst case network performance or disconnected use only. Documents are stored in the Local Workspace folder, metadata is stored in the Local Workspace database, and Local Workspace is only synchronized on demand by user commands.

Unlock Local Workspace Documents

In certain circumstances, an administrator may need to free a document that a particular user has locked because:

- The user who locked the document is not available and someone else urgently needs to work on the document.
- The user did not synchronize the document properly.
- The user wants to continue to work on the document remotely through PowerWeb.
- The user locked the document in the Local Workspace on an old workstation and needs to work on these documents on a new workstation, but the old workstation is not available anymore.

  In this scenario, if the user tries to unlock the document, they will get an error message.

In these situations, you may need to unlock the document so that the vault copy may be worked on.

Important!
Unlocking a document from a user's Local Workspace can lose changes made to the document by that user while the document resided in the Local Workspace if the document has not yet been synchronized to the vault. The original copy of the document in the vault will be unlocked and considered by Meridian to be the latest revision. For this reason, a document should only be unlocked after it has been synchronized.

Note:
The **Revoke Quick Change for Others** privilege is required to unlock Local Workspace documents.

Unlock One Document

To successfully perform this procedure, you need to open the vault using the Meridian Service Account (or your Admin account if you have sufficient workflow privileges).

To unlock one document locked in a user's Local Workspace:

1. In PowerUser, navigate to the locked document.
2. Right-click the document and select **Show Revisions**.
3. Right-click the last revision, which represents the copy locked in Local Workspace and choose **Unlock from Local Workspace**.

A dialog box opens, asking you to confirm your choice.

4. Click **Yes**.

Unlock All Documents

> **Note:**
> When the **Use Enterprise Server for user management** option is enabled as described in Configure the Connection To Meridian Enterprise Server, the **Accruent Users and Groups** branch mentioned below is hidden because the user accounts and groups are then stored in the Meridian Enterprise Server database instead. You can force the branch to appear anyway by setting the **ForceShowUserManagementNode** registry value described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMAdmin.
>
> This is typically done so that an administrator can then use the **Unlock Documents** command described in Unlock Local Workspace Documents. The branch is visible when the user accounts and groups are stored in the Meridian user database by default.

To unlock all documents that are locked in a user's Local Workspace for one vault:

1. In the Meridian Enterprise Administrator, expand **Accruent Users and Groups** in the left pane and click **Users**.
2. In the user list, click the name of the user for which you want to unlock documents.
3. On the **Action** menu, point to **All Tasks** and click **Unlock Documents**.

   The **Unlock Documents** dialog box appears.
4. Read and understand the warning.

   Proceeding to unlock documents cannot be undone.
5. In the vault list, click the name of the vault name for which you want to unlock documents.
6. Confirm that the user name is correct.

   To see how many documents are locked by the selected user:

   a. Click **Check**.

      The quantity appears in a dialog box.

   b. Click **OK**.
7. If you are certain that you want to unlock the documents, click **Finish**.

   A dialog box shows the results of the command.

   The next time that the user who had the documents locked logs on, they will be shown a Local Workspace conflict message stating **This file is modified outside the vault**. For information on resolving Local Workspace conflicts, refer to *Resolve Local Workspace Conflicts* in the *Meridian Enterprise User's Guide*.

Automatically Synchronize and Unlock Documents

When Meridian is used in an environment where users can work at different computers or where multiple users share a computer and work on the same documents (for example, in different shifts), we recommend that the documents in the local workspaces of the computers be synchronized and unlocked when the users logs off from Windows. This makes the documents able to be edited in different local workspaces (at different times) or by different users in the same local workspace.

Synchronizing the documents can be done manually by each user in PowerUser but it is easy to forget to do so before logging off. To do it automatically, you can run a tool named `BCSyncUnlock.exe`. By default, it is installed by Meridian in `C:\Program Files (x86)\BC-Meridian\Program\BCSyncUnlock`. The tool can be run in the **Logoff** script of the local or Active Directory security policy.

When `BCSyncUnlock.exe` runs, it:

1. Locates any documents in the logged-on user's To-Do list that reside in the local workspace
2. Synchronizes the content of the documents with the vault
3. Unlocks the documents from the local workspace. This is different than the **Synchronize Now** command in Application Integration, which does not unlock the documents.

By default, if AutoCAD, MicroStation, or Notepad are still open when the tool runs, the tool waits for those programs to close before synchronizing and unlocking the documents. If those programs do not close within a configurable time period, the tool stops automatically and logging off can proceed. Additional applications can also be configured to suspend the tool.

- The tool does not affect sub-assemblies and parts.
- The tool presents a graphical user interface for easier troubleshooting.
- The tool supports running under restricted permissions by the typical Meridian user who is not an administrator of their PC.

The documents that are unlocked remain on the user's To-Do list, ready to be downloaded to a different local workspace for editing by the same user. The documents can also be reassigned to a different user for editing on the same or a different computer.

`BCSyncUnlock.exe` can be configured by editing the file `BCSyncUnlock.exe.config` that resides in the same folder.

The parameters that can be configured are described in the following table.

Configurable parameters

Parameter	Description
AutoUnlockAndClose	When set to True, the tool runs immediately and closes. When set to **False** (default), the tools opens in a window and waits until you click **Start** to synchronize.
WaitFor	A comma-separated list of executables (without their file extensions) that, if running, will suspend `BCSyncUnlock.exe`. The default is **ustation,acad,notepad**.
MaxWait	The maximum time in milliseconds to wait for running applications to close before the tool stops. Setting this parameter to **0** will cause the tool to wait indefinitely. The default is **20000** (20 seconds).
WaitForMessage	The message to show while the tool is waiting for applications to close. The default is **Waiting for AutoCAD and MicroStation to be closed...**
MaxWaitMessage	The message to show when the maximum wait period has expired. The default is **Synchronization aborted. Please close AutoCAD and MicroStation and retry.**

Disable Offline Mode

By default, it is possible for users to switch between Online and Offline mode directly from the shortcut menu of the **Meridian Application Integration** icon in their system tray.

Many organizations do not want this option available to users, so it can be hidden via a server registry key. Create a new DWORD value named **DisableOfflineSwitch** in the following registry key on the client computer:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco
\AutoManager Meridian\CurrentVersion\Client
```

Set this new value to **1**. After this registry key has been added, the next time the client computers are restarted, the **Offline Mode** option will be hidden. You can also stop Meridian Application Integration with the **Close** item on its menu, and restart it from the Windows **Start** menu.

> **Note:**
> Offline mode must be enabled for the Meridian CAD application links to work remotely with PowerWeb. For more information, see Prepare the Remote Access Client Computers.

Network Administration

After Meridian is properly installed and configured in a network, administration tasks revolve primarily around the aspects of security and maintaining a high performance infrastructure upon which Meridian can run productively.

This section describes the following topics:

- Summaries of the security privileges required on each computer used by Meridian
- Guidelines for using Meridian with popular Microsoft network models
- Considerations for configuring Meridian in a mixed vendor network
- How to configure and apply Meridian security roles within vaults
- Instructions for configuring remote access to Meridian
- Explanations of the effects of network performance on Meridian

Meridian Security Requirements

The Meridian desktop applications (PowerUser, Configurator, and Administrator) authenticate users with the computer's operating system, Windows. The PowerWeb client authenticates users according to the method specified for the web application in Internet Information Services on the web server as described in Configure a PowerWeb Location.

Meridian does not rely on Windows to implement vault security. Meridian uses Windows only to authenticate users' identity. Instead, security roles are defined in the Configurator and privileges are granted or revoked from these roles. An administrator then assigns Windows users or groups to different roles for different folders with the PowerUser client application.

To work the most effectively with Meridian, Windows user accounts and groups should adhere to the following guidelines:

- Multiple users should not be allowed to log in under the same user name.
- Password synchronization between networks or systems should be consistent.
- A dedicated server for user administration is recommended.
- Users should always log on when they start working.
- Users' logon scripts should synchronize the client computer time with the Meridian application server time.

If your Meridian Enterprise system will use more than one server, the services might need to be configured to allow security delegation as described in Security Delegation.

Client Computer Privileges

All Meridian users require the following minimum privileges on their own computers:

- Membership in the Administrators group to install the Meridian software. See the following note.
- Internet Explorer security settings as described in *Configure Browser Security* in the *Meridian Enterprise User's Guide*.
- Read access to `C:\Program Files\BC-Meridian` and subfolders
- Read access to `C:\Program Files\Common Files\Cyco Shared`
- Read access to `C:\Program Files\Common Files\Autodesk Shared`
- Read access to `C:\Windows\System32`
- Read and Write access to `C:\Windows\Downloaded Program Files`. This folder is the ActiveX cache for user interface extensions that are downloaded from the Meridian server as needed. Extensions are only needed by users of vaults in which the extensions have been registered as described in *Register Custom Interface Extensions* in the *Meridian Enterprise Configuration Guide*.

  > **Note:**
  > By default, user interface extensions are installed in this folder for all users of the computer. For information about installing extensions only for a specific user, see the Meridian Enterprise .NET API Reference Guide. When user interface extensions are installed for a specific user, the extensions are placed in a sub-folder of the folder that is specified by the Windows environment variable **LocalAppData**.

- Full access to the `C:\BC-Workspace` folder. They must also have full access to the sub-folder that matches their user name.
- Modify access to the folder specified by the Windows **TEMP** system variable or if a **TEMP** user variable is defined, that folder, which overrides the system variable.

> **Note:**
> Ideally, users should be a member of either the Administrators or Power Users group of their own computer, unless read/write access has been granted for a lower group for which the user is a member. If this is prohibited by your organization's security policy, an alternate method for installing Meridian and deploying extensions must be used.
>
> Common alternatives include manual installation performed by a System Administrator or using a centralized application deployment system such as Microsoft Systems Management Server (SMS).

Meridian Server Privileges

All Meridian users require the following minimum privileges on the Meridian application server:

- All users must be members of a valid local or domain group that is granted access to the Meridian application server.
- Read access to `\Program Files\BC-Meridian\Program`
- Read access to `\BC-Meridian Extensions` (share name AMM3EXT$) and its subfolders
- No access to `\BC-Meridian Vaults`

> **Important!**
> We recommend that access to this folder be granted to members of the Administrators group and the local system accounts only. The Meridian vault database and document files are stored in this folder and its subfolders and any unauthorized modifications, movements, or deletions are extremely dangerous.
>
> The capability to modify the vault can be further secured by only installing the administration tools (**Administrator** component in the setup packages) on the computers used by authorized System Administrators.

PowerWeb Server Privileges

When using PowerWeb with a default installation of Internet Information Services, updating thumbnails, synchronizing properties and other functionality may seem to fail without any direct cause. Users may also receive **Access denied** errors.

All Meridian PowerWeb users and the IIS service account require the following minimum privileges on the server running Internet Information Services, whether it is also the Meridian application server or another server:

- Read access to `C:\Inetpub\AMM`.
- Modify access to `C:\Inetpub\AMM\AMTemp`.
- Full access to `C:\Inetpub\AMM\Profiles`.
- Full access to the folder specified by the Windows **TEMP** system variable or if a **TEMP** user variable is defined for the application pool account, that folder, which overrides the system variable.
- Full access to the local workspace folder, `C:\BC-Workspace` by default.
- Read access to `C:\Program Files\BC-Meridian\Program`.

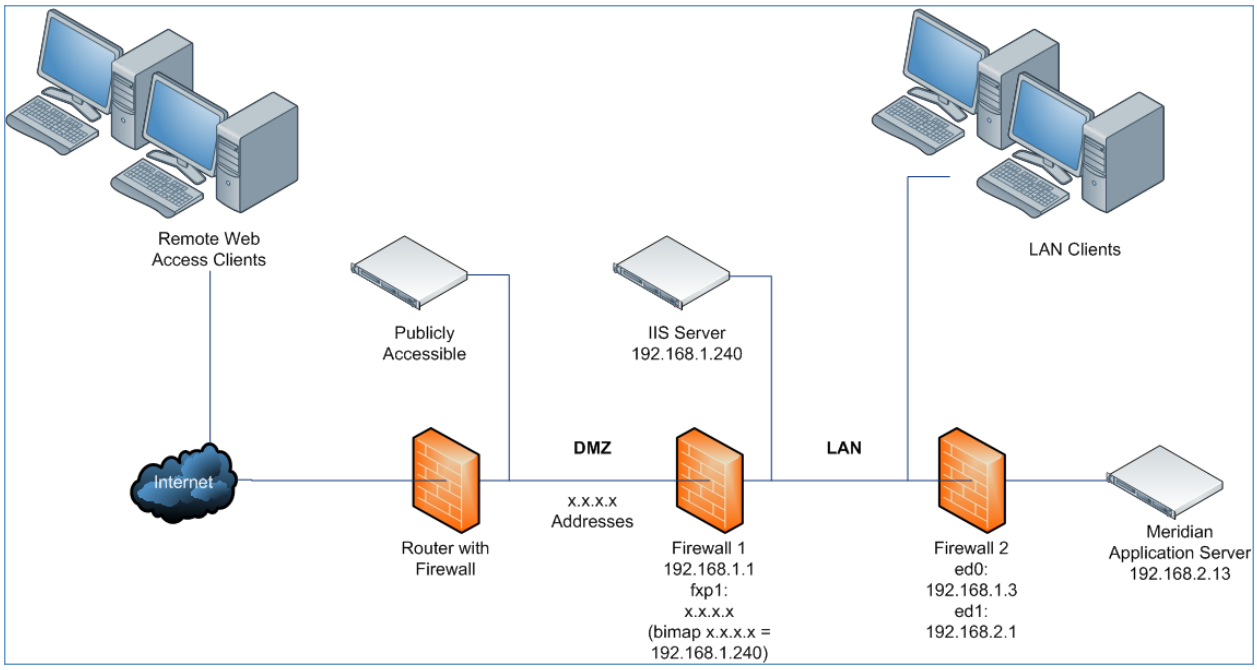
If PowerWeb will only be used on your organization's intranet, no additional configuration is necessary. PowerWeb is as secure as any other IIS website. But if you want to allow access from outside of the organization for remote users, contractors, vendors, or other business partners, we recommend that you:

- Create a separate domain in the demilitarized zone (DMZ). The DMZ is the zone between a first and second firewall. There you place computers that are accessible from the Internet (like DNS, SMTP, and IIS servers, and so on).
- Enable a one-way trust relationship between the DMZ domain and your corporate domain.

> **Note:**
> We recommend that you use the Secure Sockets Layer (SSL) for connections to PowerWeb sites from the Internet because, depending on the authentication method used, IIS may need to forward passwords to the Meridian application server. If SSL is not used, the passwords will be in clear text between the PowerWeb clients and the IIS server.

Allow PowerWeb Access Through a Firewall

If PowerWeb will only be used on your organization's intranet, no special configuration is necessary. PowerWeb is as secure as any other IIS website. But if you want to allow access from outside the organization for remote users, contractors, vendors, or other business partners, your network will need to be configured to allow access through one or more firewalls to the PowerWeb server. A description of this configuration follows and is illustrated in the following figure with example IP addresses:



This configuration is necessary because the Meridian application server communicates with PowerWeb running on the IIS server via the DCOM protocol. PowerWeb always starts a DCOM session with a request on the TCP port 135 of the Meridian application server. If a response is received, DCOM handles further communications, and determines which port will be used. The Meridian application server needs to be accessible from the IIS server on its own IP address because DCOM doesn't support Network Address Translation (NAT).

To allow PowerWeb through a firewall:

1. Install Meridian and PowerWeb on their respective computers as described in Installation.

   By default, DCOM communicates over a very wide port range (135 and 1025 to 5000 and 49152 to 65535 on Windows Vista and Windows Server 2008 and later).

2. Use the **netsh** tool on the Meridian application server to view the DCOM properties of the computer as described in this Microsoft Support article.

3. Restrict the range of TCP port numbers your computer is able to use to, for example, 135 and 4000–5000.

   It's essential to ensure that DCOM is running with TCP/IP only. If possible, delete all other protocols except TCP/IP if you are not using them. If you only have a restricted number of ports to use, refer to the Microsoft MSDN site for the current recommendation for the minimum number of ports to allocate.

4. Configure the **Meridian** IIS applications (created by PowerWeb installation) of the default website to enable SSL.

   > **Note:**
   > If the Windows firewall is used, enable **World Wide Web Services (HTTP Traffic in)** and **World Wide Web Services (HTTPS Traffic in)** in **Windows Firewall with Advanced Security**.

   In the example configuration shown in the preceding figure, a small modification is necessary in the routing table for Windows. The default gateway is 192.168.1.1, which means that the subnet of 192.168.2.0 can never normally be reached. This could be solved with two network cards, but could also be solved by adding an explicit routing to the routing table as shown in the following example:

   ```
   ROUTE –p ADD 192.168.2.0 MASK 255.255.255.0 192.168.1.3
   ```

   If errors occur from `mtx.exe`, this means that you have restricted the Meridian website to run in a separate memory space, which is not allowed.

5. Configure the firewall between the Meridian server and the IIS server to allow communications within the port range specified in step 3.

   Following are example lines to add to an `/etc/ipf.rules` file:

   ```
   #dcom connection from PowerWeb to EDM Server
   pass in quick on ed0 proto tcp from any port > 1024 to any port =
   135 flags S keep state keep frags
   #dcom connection from EDM Server to PowerWeb
   block in on ed0 proto tcp from any port > 1024 to any port > 5000
   flags S keep state keep frags
   pass in quick on ed0 proto tcp from any port > 1024 to any port >
   4000 flags S keep state keep frags
   ```

   > **Note:**
   > If the Windows firewall is used, add inbound and outbound rules in **Windows Firewall with Advanced Security** for the Meridian executable `AMEDMW.exe`.

6. When the firewall has been configured and the connection between the IIS and Meridian servers is working properly, publish a Meridian vault as described in Create a PowerWeb Location.

7. Create a simple port mapping on the firewall between the LAN and the DMZ so that the IIS server on the private LAN can be reached via the Internet using a real IP address:

   a. On the firewall computer, edit the `/etc/ipnat.rules` file as below:

      ```
      #test web client
      bimap fxp1 192.168.1.240/32 -> x.x.x.x/32
      ```

      (x.x.x.x = a real life Internet address)

   b. Edit the `/etc/ipf.rules` file as shown below:

      ```
      #test web client
      pass in quick on fxp1 proto tcp from any port > 1024 to
      192.168.1.240/32 port = 80 flags S keep state keep frags
      pass in quick on fxp1 proto tcp from any port > 1024 to
      192.168.1.240/32 port = 443 flags S keep state keep frags
      ```

      Your Meridian application server is now accessible securely via the Internet.

      The preceding steps relate to this configuration scenario only. However, the technique of using protocol levels in this way is the same for all configurations.

Security Delegation

In the typical Windows network, when a user makes a request from a service, if the service needs to connects to a different computer to fulfill the request, it connects using its own account (or application pool identity if it is a web service).

Examples are:

- Meridian Enterprise and PowerWeb running on separate servers
- Meridian Enterprise, Publisher, and Meridian Explorer running on separate servers

This has ramifications for Meridian Enterprise security. For example, the requesting service account must have all of the permissions granted to it that would be needed by any combination of potential users, document types, and areas of the vault. This makes enforcing very specific or granular security difficult if not impossible. It may also have ramifications on the metadata. For example, document properties that are modified by the request will show the service account name in the **Modified By** property or in the document log. This can make security auditing problematic.

To overcome these problems, the environment can be configured to allow security delegation, in which the service impersonates the requesting user by connecting to the other computer using the user's account to fulfill the request. The user's account credentials are delegated to the service. At first glance, delegation may seem to be the perfect solution. However, impersonation creates what is known as the double hop problem, which requires additional configuration.

By default, Meridian Enterprise Server assumes that security delegation has been configured. Delegation and impersonation can be disabled in Meridian Enterprise Server by adding the following setting to the file `C:\ProgramData\BlueCieloECM\Hyperion\WebConfigDto.dat`.

```
"DisableImpersonationForBCM":true,
```

Note:

- This setting affects changes initiated from feedback type property pages and VBScript events. Examples are users adding comments to documents from Meridian Explorer and viewing print previews when watermarks are configured to be shown. In both examples, Meridian Enterprise Server needs to connect to the Meridian Enterprise server to read or save data that can be protected by security privileges that the application pool identity might not have been granted.
- Also see the registry value **SameIISEDMAccount** in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink.

- In Meridian Enterprise Server 2012 SP5, the name of this setting is `FeedbackNoImpersonation`.

Following are some guidelines to help you determine if you need to configure security delegation.

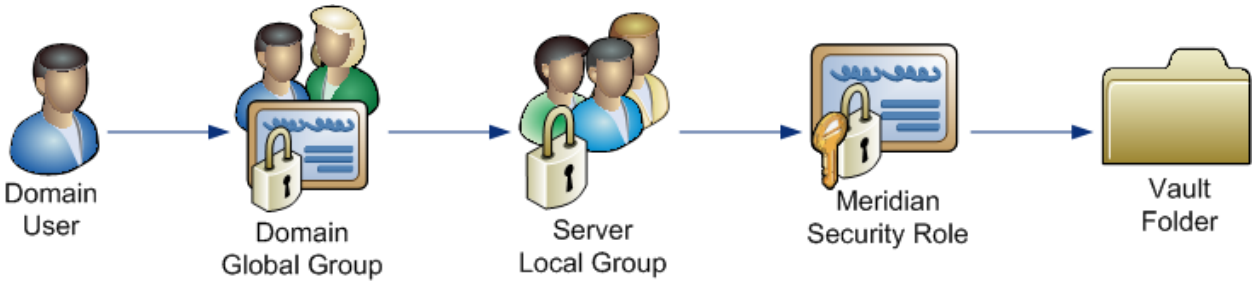
- If the system works as expected and access errors do not occur or if the services run on the same computer, delegation is not necessary and you do not need to disable impersonation.
- If the lack of security delegation is causing problems, you have two options:
  - If it's acceptable to your organization that for all Meridian Explorer users, feedback to the Meridian Enterprise vault (redlines, comments, property updates, VBScript procedures) are performed under the service account, then disabling the impersonation is an easy way to avoid the delegation issue.
  - You must resolve the double hop problem by configuring security delegation.

Following are links to resources that explain this requirement in more detail and provide configuration assistance:

- How to Configure the Server to be Trusted for Delegation on the Microsoft TechNet website
- How to configure an ASP.NET application for a delegation scenario on the Microsoft Support website
- Understanding Kerberos Double Hop on the Microsoft TechNet website

Meridian Support For Microsoft Active Directory

Meridian supports Microsoft Active Directory (AD) domain global groups. Active Directory domain local groups and universal groups are not supported. The recommended relationship between a user and the user's permission to perform a particular Meridian action within a folder looks like this:



- Domain user account assigned to a domain global group.
- Domain global group assigned to a Meridian application server (domain member server) local group.
- Meridian application server local group assigned to a Meridian role at the vault folder where the action is performed.
- Meridian role defined (in Configurator) with appropriate Meridian object-level privileges enabled.

Active Directory Security Problems

With security configured, the Meridian users and services need privileges to access the domain user account and group membership information. By default, Active Directory users and the Windows SYSTEM account do not have these privileges. Without sufficient access, Meridian security may not function and users can be denied access to documents or commands. It may seem to work at times or in certain situations, but problems can still occur.

This problem typically occurs after security is applied to a vault, resulting in all users being denied access to the vault. No folders or documents can be seen by any user. Only the vault's root folder appears in the application with a nearby lock icon indicating that the user has no access. In some cases, a subset of users is denied access to the vault even when they have appropriate privileges in the vault. In such cases, it is not uncommon for a user to be denied access, even though their group membership is identical to a user who is not denied access.

Because Meridian uses Windows domain security authentication to control security privileges in the vault, the AutoManager EDM Server service used by Meridian must have privileges to query the domain user accounts and group memberships. In Active Directory, these privileges may be granted in one of two ways:

- Granting domain privileges with a service account
- Granting domain privileges to the Meridian application server

Both of these methods rely on the Pre-Windows 2000 Compatible Access group that is available in each Active Directory domain. The group is a convenient way to grant necessary privileges to the AutoManager EDM Server service.

> **Note:**
> When Meridian users reside in multiple domains within an Active Directory forest, you have to add the service to the group in every domain where the users reside.

Meridian security will also work if the Everyone group or the Authenticated Users group is added to the Pre-Windows 2000 Compatible Access group. However, this will likely breach your organization's security policy, so you should choose one of the above solutions.

Grant Domain Privileges With a Service Account

By default, the EDM Server service runs under the SYSTEM account of the computer. This works well in simple environments.

But it does not work in more complex environments such as:

- Meridian user accounts synchronized with Active Directory
- Meridian integrated with SQL Server or Oracle hosted on other computers
- Meridian PowerWeb or stream files located on other computers
- Meridian integrated with Publisher or Meridian Explorer

In environments like these, the EDM Server service must have access to those computers, which the SYSTEM account does not. Instead, the EDM Server service must run under a different account that does have access to those computers. We recommend that you configure the EDM Server service to use a domain account with sufficient permissions to access those computers depending on the required resources. For example, to access stream files (document content) stored on a separate file server, the EDM Server service account will need Read and Write permissions to the stream folders on the file server. In addition to the particular resource requirements of the server type being accessed, the EDM Server service account needs the **Log on as a service** security policy for the domain.

This solution involves creating a dedicated account for the Meridian services to run under and granting that account the domain privileges needed. This solution is preferred by domain administrators when the privileges should be as restricted as possible.

Create Service Account

Important!
For some Meridian application servers this service account user must also be a local administrator. If Meridian Enterprise Server is configured to run as a service on the Publisher Server PC, then:

- On the **Publisher Server PC** (a node), the windows account used by Meridian must be added to the Administrator's group.
- On the **Enterprise Server PC** (a primary node), the Publisher local user account must be added to the Administrator's group.

Learn more about Meridian Enterprise Server Clusters in the *Meridian Enterprise Server Clusters* section in the *Meridian Enterprise Server Administrator's Guide*.

You can also configure Meridian Enterprise Server to not run as a service, as described in the *Configure Meridian Enterprise Server To Not Run As a Service* article in the *Meridian Enterprise Server Administrator's Guide*. If you do this, then the Publisher local user should be added to the administrator's group on the Enterprise Server PC.

See the *Non-Admin Service Accounts* section below to learn how to create non-admin service accounts and what limitations they have.

1. In Active Directory, create a new user named **BC Meridian Server Service** (or similar).

   The account should be a domain user. By default, this account is set as the rescue account as described in Create a Rescue Account For Security Administration.

2. Add the account to the following policies on the Meridian application server:
   - **Log on as a batch job**
   - **Log on as a service**
3. Give the account full control over the following folders:

   If everyone has access to a folder, you do not need to change the access for that folder.
   - \BC-Meridian Vaults
   - \BC-WorkSpace
   - \inetpub\AMM
   - \inetpub\PowerWebAPI
   - \inetpub\Tags
   - \inetpub\WhereUsed
   - \inetpub\wwwroot\BCSiteCache
   - \inetpub\wwwroot\BCSiteCacheClient
   - \inetpub\wwwroot\BCEnterprise
   - \inetpub\wwwroot\M360.Meridian
   - \BC-Meridian Extensions
   - \ProgramData\BlueCieloECM
   - \SiteCachePreloadFolder

     This is a manually created preload folder on the Site Cache server.
4. Give the account full control over the following registry branches on the Meridian application server:

- HKEY_CURRENT_USER\SOFTWARE\Cyco
- HKEY_LOCAL_MACHINE\SOFTWARE\Cyco
- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cyco

5. In Active Directory, add the account to the built-in **Pre-Windows 2000 Compatible Access** group.

   This grants the required privileges to the server's SYSTEM account. In an Active Directory environment, changing the account under which the AutoManager EDM Server service runs will also require you to add the account to the **Pre-Windows 2000 Compatible Access** group of the domain, unless the new account is also a domain administrator account.

   If the account is not a domain administrator and the account is not added to the **Pre-Windows 2000 Compatible Access** group, strange security behavior will occur in the vault because the new account will not be granted access to query domain user accounts and group membership.

   If Meridian users reside in multiple domains in an Active Directory forest, you must do this for every domain in which the users reside.

6. In Active Directory, verify that the account is a member of the **Distributed COM Users** group or of a group that is a member.

7. Choose between two options:

   - Enter this account name when prompted during Meridian Enterprise server installation as described in Install the Server Components.
   - If the Meridian Enterprise server components are already installed, in **Computer Management** on the Meridian application server, edit the properties of the **AutoManager EDM Server** service and set the logon credentials to the name and password created in step 1.

8. Restart the Meridian application server.

   We recommend that you specify this same account for all of the uses in your environment that are listed in Service Account Usage.

Non-Admin Service Accounts

It is possible to use a non-admin service account, but you must reserve specified URLs for the Meridian Service Account on the 8686 server port and the listener on the 40865 server port. This is required for all Meridian Enterprise Server services of any of the PCs in your configuration. Reserving these URLs is necessary because the Meridian Service Account is working with non-admin rights in the system.

In this scenario, the account:

- is a standard domain account
- is only a member of the Domain Users AD group
- does not belong to the Administrator's group of any of the PCs in the configuration

  If Meridian Enterprise Server is NOT started as a service on the Publisher Server PC, then the Meridian Service Account MUST be added to the Administrator group on this PC. Learn more by reviewing the *Configure Meridian Enterprise Server To Not Run As a Service* article in the *Meridian Enterprise Server Administrator's Guide*.

1. Access the Enterprise Server and Publisher Server machines.
2. Follow the *Create Service Account* procedures above.
3. Download this zip file.
4. Extract the **Reserve URL MSA.ps1** script.
5. Disable and stop the **Meridian Enterprise Server** service.
6. Navigate to **C:\Program Files\BC-Meridian\Enterprise Server** on your computer.
7. Open a command window as an administrator from the folder.
8. Type the following command in the window.

   ```
   BlueCieloECM.EnterpriseService.exe /c
   ```

9. Press **Enter** on your keyboard.

   The command processes.
10. Start **PowerShell** as an Administrator.
11. Run the **Reserve URL MSA.ps1** script you extracted in step 4.

    The parameters in this script are:

    - **MSA**: Meridian service account in format: domainname\username.
    - **Server**: Enterprise server.
    - **ESService**: All available services.
    - **UrlOFF**: Switch argument. If presented, reserved URLs will be deleted from the system.

      This argument is used when you want to roll back changes made to the system by the script.

    This script may fail for some of the services, this is a known issue.
12. To check the result of the script:

a. Type the following command in PowerShell:

```
netsh http show urlacl
```

b. Press **Enter** on your keyboard.

13. Close PowerShell.
14. Close the command window.
15. Re-enable and start the **Meridian Enterprise Server** service.
16. Restart all Meridian machines.

Grant Domain Privileges To the Meridian Server

This solution involves adding the Meridian application server computer to the **Pre-Windows 2000 Compatible Access** group in Active Directory. This solution grants the required privileges to the server's SYSTEM account.

Note:

- You must reboot the domain controllers after adding the server to the group.
- Only the computer running the AutoManager EDM Server service should be added to the **Pre-Windows 2000 Compatible Access** group.

DCOM Problems

Meridian relies heavily on the DCOM protocol for communications between its client applications and the Meridian application server as described in Interprocess Communication. Unfortunately, due to the abuse of this protocol by hackers in recent years, Microsoft has steadily increased the default security restrictions on DCOM in subsequent Windows versions, making the legitimate use of the protocol more difficult.

Improper configuration of DCOM can result in a variety of Meridian error messages. When trying to connect to a Meridian application server, a client computer may show one of the following error messages:

- Remote calls are not allowed for this process
- RPC Server not available
- Cannot create instance of AMDocumentRepository
- Access denied

The following topics describe common solutions to these error messages.

Enable DCOM

DCOM might be disabled on the Meridian application server or client computers manually by IT personnel for security reasons or by a script (or group policy) or other software that is installed on the server or client computer.

> **Note:**
> Another cause of failed DCOM communications can be a software firewall on the server, including the integrated Windows firewall. Test this possibility by temporarily disabling the firewall and testing for the client error.
>
> If access succeeds, configure the firewall to allow DCOM communication as described in Allow PowerWeb Access Through a Firewall.

Enable DCOM on Client Computers

To enable DCOM on client computers:

1. Open Registry Editor on the client computer and locate the following key:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE`

2. Change the **EnableDCOM** value to **Y**.
3. Reboot the client computer.

Enable DCOM on Meridian Server Computers

To enable DCOM on Meridian server computers:

1. Open `dcomcnfg.exe` from a command (CMD) window on the server.
2. Expand **Component Services**, expand **Computers**, right-click **My Computer**, and then click **Properties**.
3. Click the **Default Properties** tab.
4. Enable the **Enable Distributed COM on this computer** option and then click **OK**.

Configure DCOM Permissions

The Microsoft Distributed Component Object Model (DCOM) protocol facilitates communication between Meridian LAN clients and the **Meridian EDM Server** service. Grant the necessary DCOM permissions to ensure users can properly use Meridian:

1. Add the Meridian users' group as a member of the **Distributed COM Users** group on the Meridian servers.
2. Search for and open **Component Services** on the Windows search bar.
3. Expand **Component Services** > **Computers**.
4. Right-click **My Computer** and select **Properties**.
5. Click **COM Security**.
6. In **Launch and Activation Permissions**, click **Edit Limits**.
7. Click **Add**.
8. In **Enter the object name to select**, enter **Distributed COM Users** and click **OK**.
9. Select **Allow** for **Local Launch**, **Local Activation**, and **Remote Activation** permissions for the **Distributed COM Users** group.

Grant permissions in DCOM applications

In Windows **Component Services**, expand **Component Services** > **Computers** > **My Computer** > **DCOM Config** and grant permissions for DCOM Configs **BCEnterpriseServicesPS**, **BlueCielo EDM Server**, and **BlueCielo License Server**:

1. Right-click the DCOM Config, then select **Properties**.
2. Click **Security**.
3. Configure each section starting with **Launch and Activate Permissions**:
    a. Select **Customize** then click **Edit**.
    b. Click **Add**.
    c. In **Enter the object name to select**, enter **Domain Users**.
    d. Click **Check Names** then click **OK**.
    e. Select **Allow** for all permissions of the **Domain Users** group.
    f. Click **OK**.
    g. Repeat for **Access Permissions** and **Configuration Permissions**.

Configure the DCOM Identity Of Remote Services

Some web applications that are included with Meridian besides PowerWeb also need to access document metadata, for example, the document subscriptions viewer and the Meridian FDA Module audit log viewer. In environments where the audit and subscription data is stored in a separate database server from the Meridian application server, it may be necessary to configure the user account that is used by those web applications to access the data.

To configure the DCOM identity for these services:

1. Open `dcomcnfg.exe` from a command (CMD) window on the server.
2. Expand **Component Services** > **Computers** > **My Computer** > **COM+ Applications**.
3. Right-click **BlueCielo Meridian Services** and select **Properties** on the shortcut menu that appears.

   The **BlueCielo Meridian Services Properties** dialog box appears.
4. On the **Identity** tab, click **This user**.
5. Type the credentials of the account described in Grant Domain Privileges With a Service Account.
6. Click **OK**.

Use Meridian With Nested Groups

Meridian supports Active Directory nested groups when the following requirements are met:

- The Meridian application server has been configured as described in Active Directory Security Problems.
- The domain is in Native mode. For several reasons, Meridian does not support nested groups in Mixed mode.
- Meridian is configured to browse for domain global groups as described in Configure the BrowseForGlobalGroups Setting.
- Meridian is configured to browse for nested global groups with the **BrowseForNestedGlobalGroups** setting described in Windows Registry Keys.

Note:

- Using these settings might have a negative impact on performance.
- Nested groups are not supported for reserving licenses as described in Reserve Licenses.

Use Meridian With Multiple Domains

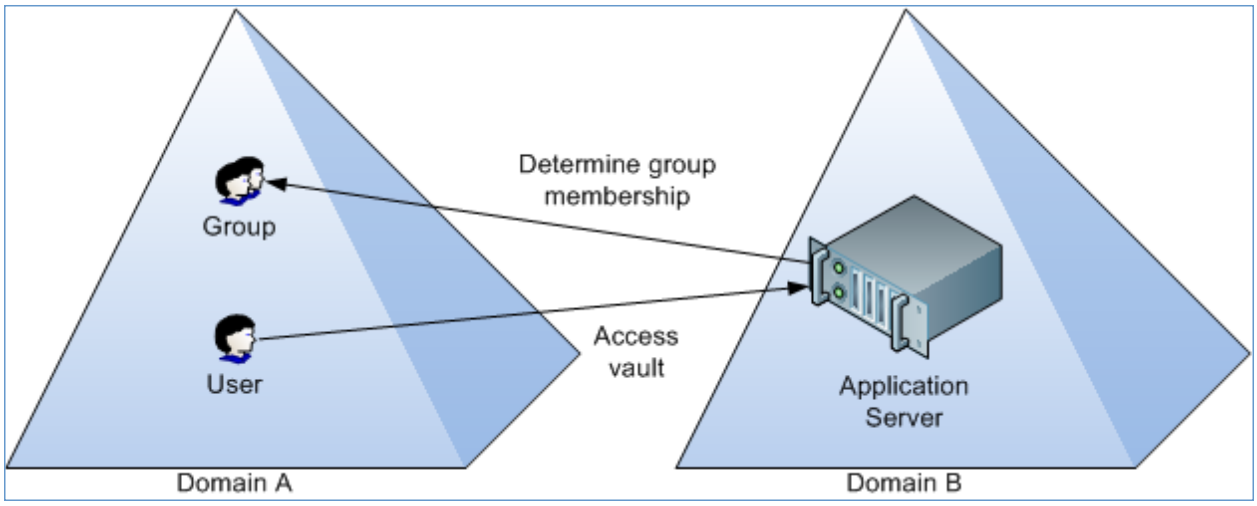
In a single-domain environment, running Meridian's AutoManager EDM Server service under a domain account as described in Active Directory Security Problems is sufficient, the service needs to be able to log on to the domain. We highly recommend that the domain account also be a member of the Meridian application server's Administrators group.

When Meridian is installed in an Active Directory environment with multiple domains, for example, one user domain and one resource domain, some additional configuration is needed to allow the vault security to function correctly. The Meridian service account needs to be able to query the domain controller for the group memberships of users. A default installation of Active Directory allows these queries by including the built-in group Authenticated Users as a member of the built-in Pre-Windows 2000 Compatible Access group.

In order to allow access to users from remote domains (other than the domain where the Meridian application server resides), the Meridian application server must first be configured as described in Active Directory Security Problems. Additional configuration may be necessary as described in the following topics.

Grant Membership Query Access

In a multiple-domain environment, Meridian security is a little more complicated than in a single-domain environment, as shown in the following figure.



A user in Domain A can access the Meridian application server in Domain B and open a vault as long as there is full trust between the two domains. But if there are Meridian security roles assigned to the folder in the vault that the user attempts to access, Meridian needs to be able to query the domain of the user to determine the user's group memberships. In order to be able to do that, the account in Domain B under which the AutoManager EDM Server service is running needs read access to the **Member Of** attribute of the user in Domain A.

To grant the service read access to the **Member Of** attribute:

1. Install the Windows Server Support Tools on the domain controller computer of the user's domain, if they are not installed already.

   The Windows Server Support Tools can be found on the Windows Server installation disc.
2. Start the ADSI Edit management console by running `ADSIEDIT.MSC`.
3. In ADSI Edit, right-click the domain's DNS folder, and select **Properties**.
4. Click the **Security** tab and add the domain account under which the Meridian services are being run.

   This should be an account in the server's domain.
5. Click the **Advanced** button.

   The **Permission Entry** dialog box appears.

6. Click the **Properties** tab and check the **Allow** column of the **Read Member Of** permission.
7. Click **OK**.

Configure Computer Name Resolution

If user access problems still occur after configuring the Meridian service account as described in Grant Membership Query Access, the problem could be caused by incorrect computer name resolution.

> **Note:**
> You can confirm this cause by testing whether vault access works for the remote domain users as long as no roles are applied in the vault. You can also test this by creating a temporary test vault. As soon as roles are applied to the vault, users in remote domains can no longer access the vault. Only users from the home domain (the domain where the Meridian application server resides) can access the vault.

If the Meridian application server is not able to find a domain controller for the remote domain, add the fully qualified remote domain to the DNS suffix list for the TCP/IP protocol of the Meridian application server's active network card.

Other conditions that can cause this behavior include:

- The remote domains are not configured as described in Active Directory Security Problems.
- Settings on firewalls between the domains.

Run Accruent License Server On a Different Computer

If the Accruent License Server service is running on a different computer than the AutoManager EDM Server service, the AutoManager EDM Server will be denied access to the license server.

To enable access in that configuration:

1. Create a new account or choose an existing account as described in Grant Domain Privileges With a Service Account
2. Assign the account to the **AutoManager EDM Server** service.
3. On the computer running the Accruent License Server service, verify that this account is a member of the **Distributed COM Users** group or a member group.

> **Note:**
> If a local account is used to run the AutoManager EDM Server service, a local account with the same username and password must also be added to the computer running the Accruent License Server service. If a domain account is used, this step is not necessary.

Meridian User Administration

Meridian user administration consists of three separate but interrelated disciplines:

- Windows user account administration as described in the topics in Network Administration.
- Meridian user account administration described in the following topics.
- Meridian vault security administration as described in the *Secure Parts Of the Vault Configuration* and *Security Roles* articles in the *Meridian Enterprise Configuration Guide*.

Meridian user accounts and user groups are used to assign security roles to specific folders in vaults and for use with workflow definitions and the project definitions of the Advanced Project Workflow module. These users and groups should not be confused with Windows users and groups or Active Directory users and groups. Although Meridian users and groups can be synchronized with their Active Directory counterparts, they are not the same things, but can work together to authorize content management activities. The Windows user accounts and groups are used solely for user authentication and security permissions outside of the Meridian vaults. For the remainder of this topic, the terms *user* and *group* refer to Meridian users and groups unless otherwise specified.

Meridian users and groups may be defined in the Meridian Enterprise Administrator tool. If Meridian Enterprise Server is also deployed, users and groups may be defined in the Meridian Enterprise Server Administration Console instead. They are then available in Meridian Enterprise if the **Use Enterprise Server for user management** option is enabled as described in Configure the Connection To Meridian Enterprise Server. Once defined, they may be used in any of the vaults managed by the same server. They can be applied to folders and workflow definitions inside the Meridian Enterprise Configurator tool as described in the *Workflow Definitions* section of the *Meridian Enterprise Configuration Guide*and the *Assign Security Roles To a Folder* article in the *Meridian Enterprise User's Guide* .

> **Note:**
> When the Meridian Enterprise Administrator tool is started before users and groups have been defined, only one user account will exist; the SYSTEM user account. No groups will exist until they have been defined by a System Administrator.

Role-Based Security

Meridian uses a role-based security system that is different from Windows domain security in a number of ways:

- Users can be organized according to their functional roles, as opposed to the domain departmental groups they may belong to.
- It does not require IT department involvement to apply roles to the vault.

Meridian security roles can be applied to different folders in vaults. This allows the flexibility for role members to have certain privileges in one folder and different privileges in another folder. Meridian security roles are defined in the Meridian Enterprise Configurator tool as described in the *Managing Security Roles* article in the *Meridian Enterprise Configuration Guide*.

Create and Edit User Accounts

> **Note:**
> If Meridian Enterprise Server is also deployed, users and groups may be defined in the Meridian Enterprise Server Administration Console instead. They are then available in Meridian Enterprise if the **Use Enterprise server for user management** option is enabled as described in Configure the Connection To Meridian Enterprise Server. If Meridian Enterprise Server is not also deployed, use the instructions in this topic.

To apply user accounts in workflow definitions, refer to the *Assign Users To a Workflow State* article in the *Meridian Enterprise Configuration Guide*.

Create an Account

To create a Meridian user account:

1. In the Meridian Enterprise Administrator, expand **Accruent Users and Groups** in the left pane and click **Users**.

   The existing user accounts appear in the right pane.

2. On the **Action** menu, point to **New** and click **User**.

   The **Create New User** dialog box appears.

3. Type a name for the new user's To-Do list.

   If this account is for an existing Meridian user, type their name as it appears in Meridian, which is their Windows user name. If this account is for a new Meridian user, this name can be different than the user's Windows user name. For example, if your organization uses employee numbers for Windows user names, you can type their personal name, which is more recognizable.

4. Click **OK**.

   The new account's **Properties** dialog box appears.

5. Click options or type values using the descriptions in the following table.

User account options

Page	Options
General	Type all known information. This information is for reference purposes only.

Page	Options
Recipient Data	Optional user information.
Member Of	Add the user to the necessary groups as described in Create and Edit User Groups.
Accounts	Add the Windows user accounts that are to be associated with this Meridian Enterprise user account: a. Click **Add**. The **New Account** dialog box appears. b. Type the user's Windows user name, regardless of the name that you typed for the user's To-Do list. c. Click **OK**. The name is added to the list of Windows accounts associated with the Meridian user. If the user is located in a different domain than the Meridian server, precede their name with the fully qualified domain name using the syntax *<Domain>\<UserName>*. d. To confirm that you typed the user name correctly, the user exists in the specified domain, and that the account information can be retrieved by the Meridian server, click **Check Name**. A dialog box will show the result. e. Add more Windows accounts if this account is for a virtual user and will be used by multiple persons or the user has multiple Windows logon accounts. f. Click the **Up** and **Down** buttons to move the primary account name to the top of the list.
Email	Add the email accounts that are to be associated with this Meridian Enterprise user account: a. Click **Add**. The **New Email Address** dialog box appears. b. Type the user's email address for receiving workflow notifications. c. Click **OK**. The address is added to the list of email addresses associated with the Meridian user. d. Type additional email addresses if this account is for a virtual user and will be used by multiple persons or the user has multiple email addresses. e. Click the **Up** and **Down** buttons to move the email address associated with the primary account name to the top of the list. Subscription notifications will only be sent to the primary account name.

Page	Options
To-Do List	This name was typed in step 3.
Manager Of	Select the names of users for whom this user will be their direct manager: a. Click **Add**. The **Select Users** dialog box appears. b. Select one or more user names. c. Click **OK**. The names are added to the list. d. Click **OK**. **Note:** If the user has already been assigned to another manager, they will be reassigned to the current user without a warning.
Active user	If selected, the user is considered active and can be selected to manage or participate in workflows. If cleared, the user is considered inactive and cannot be selected to manage or participate in workflows.
Locked user	If selected, the user's account is locked and they cannot log on to Meridian with any client application. This option can be set automatically if the Meridian FDA Module is enabled for the vault and the user exceeds the maximum number of log on retries. For more information, see *Configure Authentication* in the *Meridian Enterprise Configuration Guide*.

6. Click **OK**.
7. Repeat this task for at least every Meridian user that will participate in workflows.

   Creating a Meridian user account for every Meridian user is recommended but not required.
8. To group Meridian user accounts together, see Create and Edit User Groups.

Edit an Account

To edit an existing Meridian user account:

1. In the Meridian Enterprise Administrator, expand **Accruent Users and Groups** in the left pane and click **Users**.

   The existing user accounts appear in the right pane.
2. Choose between two options:

- Double-click the name of the user account that you want to edit.
- Click the name of the user account that you want to edit and then on the **Action** menu, click **Properties**.

  The **Properties** dialog box for the selected user appears.

3. Click options or type values using the descriptions in the preceding table.

> **Note:**
> Meridian user names can be shown in different formats as specified by the server registry setting **UserNameFormat** described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server\UserDatabase.
>
> If you change a user name, that user cannot edit their previous redlines because the redlines contain the name of the user who created them.

Create and Edit User Groups

> **Note:**
> If Meridian Enterprise Server is also deployed, users and groups may be defined in the Meridian Enterprise Server Administration Console instead. They are then available in Meridian Enterprise if the **Use Enterprise Server for user management** option is enabled as described in Configure the Connection To Meridian Enterprise Server. If Meridian Enterprise Server is not also deployed, use the instructions in this topic.

To apply user groups in workflow definitions, refer to the *Workflow Definitions* section of the *Meridian Enterprise Configuration Guide*. To synchronize the memberships of user groups with Microsoft Active Directory, see Synchronize User Groups With Active Directory.

Create User Group

To create a Meridian user group:

1. In the Meridian Enterprise Administrator, expand **Accruent Users and Groups** in the left pane and click **Groups**.
2. On the **Action** menu, point to **New** and click **Group**.

   The **New Group** dialog box appears.
3. Type a name for the new group in **Group name** and an optional description in **Description**.
4. Click **Add**.

   The **Select Users** dialog box appears.
5. Select a user name from the list.
6. Click **OK**.

   The user name is added to the **Members** list. Repeat to add all the required users to the new group. If a user does not exist, see Create and Edit User Accounts.
7. Click **Create**.
8. Repeat this task for the following groups of users:
   - Assigned to document workflow definitions
   - Assigned to project workflow definitions
   - All users if the EDM Server service is configured to use Accruent groups for security role assignments as described in Configure the EDM Server Service.

Synchronize User Groups With Active Directory

By default, the user property values and group memberships in Meridian are managed manually as described in Create and Edit User Accounts and Create and Edit User Groups. Those methods are satisfactory for small numbers of users and groups or when Microsoft Active Directory is not used extensively to manage users' privileges. However, many medium to large organizations rely on Active Directory to manage all users' access to network resources through Active Directory groups. Managing similar or identical Meridian groups separately can be inconvenient and error-prone.

Meridian Enterprise includes a program to synchronize Meridian user information and group memberships. The program allows you to map Active Directory groups to corresponding Meridian groups. The members of the mapped Active Directory groups will be synchronized with the Meridian groups and the user information for each user can also be synchronized. The program provides options that control what information is synchronized to Meridian.

The program can run in interactive mode as described in the following task. It can also be run in silent mode as a scheduled task to maintain synchronization by configuring its initialization file as described in the following topics.

Notes about functionality

- The program is installed on a computer only when the **Administrator** components are selected during Meridian installation.
- The maximum number of group mappings that can be synchronized is limited to 65520/AD group name length in characters + Accruent group name length in characters + 1. For example, given the names **ADGroup1** (8) and **BCGroup1** (8):

  8 + 8 + 1 = 17

  65520/17=3854 mappings
- User accounts in nested Active Directory groups will be synchronized with their associated Accruent user accounts but Accruent groups may not be nested.
- If Meridian Enterprise Server is also deployed, users and groups may be defined and synchronized with Active Directory in the Meridian Enterprise Server Administration Console instead.

  They are then available in Meridian Enterprise if the **Use Enterprise Server for user management** option is enabled as described in Configure the Connection To Meridian Enterprise Server. If Meridian Enterprise Server is not also deployed, use the instructions in this topic.

Procedures

To run the program interactively:

1. Run `ADSyncUsers.exe`.

   It is located at `C:\Program Files\BC-Meridian\Program` by default. The **Active Directory User Synchronizer** dialog box appears.

2. Click options or type values using the descriptions in the following table.

Configuration options

Option	Description
AD server	The IP address of the LDAP server where Active Directory information is stored.
AD admin	Account name under which to query user information from the server specified in **AD Server**.
Password	Password for the account specified in **User**.
AD groups	Names of the Active Directory groups found on the server specified in **AD Server**. To sort the names in ascending or descending order, click the corresponding button. To filter the names, type text in the **Filter** box.
Meridian groups	Names of the Meridian groups found on the Meridian Enterprise server.
Always	Updates all mapped user properties in Meridian with the information stored in Active Directory upon every synchronization.
Primary account only	Only updates the Meridian user account if the Windows account is the primary account associated with the Meridian user. For information on associating multiple Windows accounts to a single Meridian user, see Create and Edit User Accounts.
Never	Does not update user information fields from Active Directory. Only group memberships will be synchronized.
Update properties only if the user is a group member	Only updates the Meridian user properties if the user is already a member of the mapped Meridian group.

Option	Description
Rename duplicate Meridian user accounts	If a Windows account name is found associated with more than one Meridian user account, renames subsequent Meridian user accounts to match the first Meridian user account found.

3. Click **Get Groups** to retrieve the Active Directory group names and fill the **AD groups** list.
4. To create a new group mapping:
    a. Select an Active Directory group from **AD groups** that you want to map to a Meridian group.

       You may map the same AD group to multiple Meridian groups.
    b. Select a group from **Meridian groups** that you want to map to the group specified in **AD groups**.
    c. Click **Add Mapping** to create a mapping between the two selected groups.
5. To delete a group mapping, select a mapping in **Mapped groups** and click **Delete Mapping**.
6. Click **Synchronize** to begin synchronization using the current settings.
7. Click **Exit** to close the tool.

   Only the account credentials are saved. The other options can be set in the file `ADSyncUsersConfig.ini` that is located in the same folder as the program. You may edit the configuration file in any text editor.

Command Line Parameters

Besides the interactive mode described in Synchronize User Groups With Active Directory, the program can also be run from the command line in silent mode. This can be useful to incorporate the program in batch files or scheduled tasks so that it runs regularly to maintain synchronization.

To run `ADSyncUsers.exe` from the command line:

- In the batch file or scheduled task, specify the `-silent` parameter on the command line as in the following example.

  ```
  C:\Program Files\BC-Meridian\Program\ADSyncUsers.exe -silent
  ```

By default, a log file of the actions that are taken will be created in the same folder as the program. You can specify a different location and file name by also specifying the `-logpath` parameter on the command line as in the following example.

```
C:\Program Files\BC-Meridian\Program\ADSyncUsers.exe
-silent -logpath=C:\LogFiles\ADSyncUsersLog.txt
```

When run in silent mode, the program reads the configuration settings in the file `ADSyncUsersConfig.ini` that is located in the same folder as the program. You may edit the configuration file in any text editor.

> **Note:**
> The account password typed in *Password* is stored in the configuration file in encrypted form and may not be edited manually. Therefore, run the program in interactive mode to enter the password.

Map the User Properties And Groups

By default, `ADSyncUsers.exe` uses a default mapping of Active Directory user properties to Meridian user properties. You can map the Meridian properties to different Active Directory properties by specifying the property mappings in the `ADSyncUsersConfig.ini` file. No default group mappings are provided and you must specify those in the file.

Edit User Property Mapping

To edit the user property mapping:

1. Open `ADSyncUsersConfig.ini` in any text editor.

   It is located in the same folder as the program.

2. Find or create the **FieldMapping** section in the file.

   The section heading is followed by lines that each specify a Meridian user property name and its corresponding Active Directory property alias.

3. Change the Meridian property name on the left side of the line or change the Active Directory property alias on the right side of the line.

4. Save your changes and close the file.

If a Meridian property is not specified in a mapping or the name is specified incorrectly, the property will not be synchronized. If an Active Directory property alias is specified incorrectly, the default mapping will be used.

Not all of the Active Directory properties are available to be mapped. The Active Directory properties that are available to be specified in the mapping and the default mappings are listed in the following table.

Available Active Directory aliases and corresponding properties

Meridian user account property	Active Directory alias	Active Directory user object property
Account	ADPrincipalName	PrincipalName

Meridian user account property	Active Directory alias	Active Directory user object property
Address This values is the concatenation of the other address aliases (**ADStreetAddress** + **ADPostOfficeBox** + **ADCity** + **ADState** + **ADPostalCode** + **ADCountry**).	ADComputedAddress	StreetAddress + PostOfficeBox + City + State + PostalCode + Country
Description	ADDescription	Description
DisplayName	ADFullName	FullName
Email	ADEMail This value uses the format *<UserName>@<Domain>*. If mapped to **Worklist** (**Worklist=ADEmail** in `ADSyncUsersConfig.ini`), only *<UserName>* is used.	Email
Initials	ADInitials	Initials
OrgUnit	ADDepartment	Department
Title	ADPersonalTitle	Title
Worklist (To Do list)	ADAccountName	AccountName
	ADCity	City
	ADCompany	Company
	ADCountry	Country
	ADDisplayName	DisplayName
	ADJobTitle	JobTitle
	ADNT4Name	NetBIOSName
	ADPostalCode	PostalCode
	ADPostOfficeBox	PostOfficeBox
	ADState	State
	ADStreetAddress	StreetAddress

Edit User Group Mapping

To edit the user group mapping:

1. Open `ADSyncUsersConfig.ini` in any text editor.

   It is located in the same folder as the program.

2. Find or create the **GroupMapping** section in the file.

3. Add or modify the lines after the section heading to specify an Active Directory group name on the left side of the line and its corresponding Meridian group name on the right side of the line similar to the following example.

   ```
   [GroupMapping]
   Domain Admins=BCGroupAdmins
   Domain Users=MeridianUsers
   ```

4. Save your changes and close the file.

Create a Rescue Account For Security Administration

If Meridian security is incorrectly configured or assigned, even a System Administrator may not have access to a vault or its configuration. To circumvent Meridian security so that the configuration or assignment can be corrected, one Windows user account may be specified with special access to a vault that bypasses all Meridian security. By default, the account that is assigned to the **AutoManager EDM Server** service is set as the rescue (also known as a backdoor) account unless a different account is already set.

You can log on with the rescue account to temporarily grant additional privileges (for example, **Change Configuration**) to roles that are assigned in the vault or to change the role assignments (for example, the Administrator role) in the vault. This is the only way to access the system if you have locked yourself out of the vault with incorrect role settings.

To create a rescue account:

1. Open Registry Editor on the Meridian application server and locate the following registry key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Cyco
   \AutoManager Meridian\CurrentVersion\OML
   ```

2. On the **Edit** menu, point to **New**, and select **Key**.

   A new registry key named **New Key #1** appears in the left pane. Rename it to **AMServerManagerAccount**.

3. Make sure that **AMServerManagerAccount** is selected in the left pane and then double-click **(Default)** in the right pane.

   The **Edit String** dialog box appears.

4. Type the account name (for example, **BCBackDoor**) in **Value data**.
5. Click **OK**.

Secure the Rescue Account

The reason that the rescue account name is saved as the default value of the **AMServerManagerAccount** key and not as a string value is that it is possible to set security for a registry key in Windows. Doing so is highly recommended because unauthorized access to this registry key could compromise the security of your system.

To secure the rescue account:

1. Open Registry Editor on the Meridian server and locate the following registry key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager
   Meridian\CurrentVersion\OML\AMServerManagerAccount
   ```

2. On the **Edit** menu, select **Permissions**.

   The **Permissions for AMServerManagerAccount** dialog box appears.

3. Confirm that the account name typed in **AMServerManagerAccount** has **Full Control** permissions to this key, either explicitly or via group membership, along with the SYSTEM account and click **OK**.

Create an Impersonation Account for Vault Access

In some situations, a tool that uses the Meridian .NET API must impersonate a user. To enable this, set a **Security Manager Account**. When the tool runs under this account, it can impersonate other users without requiring credentials.

1. Open **Registry Editor** on the Meridian application server.
2. Locate the **HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager Meridian\CurrentVersion\OML** registry key.
3. On the **Edit** menu > **New**, select **Key**.
4. Rename the key to **AMSecurityManagerAccount**.
5. Select the **AMSecurityManagerAccount** key and double-click **Default**.
6. In the **Edit String** dialog > **Value data**, enter the account name (for example, BCBackDoor).

   The account name should not include the domain name.
7. Click **OK**.

Specify a Mail Server

The Meridian application server can be linked to an SMTP server. The SMTP server will be used to deliver workflow status messages, subscription notification messages, and to deliver documents sent via email from PowerUser. The mail server can reside inside or outside of your corporate domain.

More about configuring when notification messages are sent in *Email Notifications* of *Meridian Enterprise Configuration Guide*.

Specify One Mail Server for all Vaults

1. In the Meridian Enterprise Administrator, click **EDM Server** in the left pane.

   The active vaults are listed in the right pane.
2. From the **Action** menu, select **Properties**.

   The **EDM Server Properties** dialog appears.
3. Click **Settings**.
4. In the **Mail server** group, click the **SMTP parameters** hyperlink.

   The **SMTP Parameters** dialog appears.
5. Click options or type values using the descriptions in the SMTP server parameters table.
6. Click **OK**.

   The parameters you specified are concatenated together into a single string in the **SMTP parameters** text box.
7. Click **OK**.

SMTP server parameters

Option	Description
Host	The IP address of the SMTP server.
Port	The IP port number on which to communicate with the SMTP server. Port 25 is used by default.
SenderAddress	An optional email address of the notifications sender. This address will receive any replies to notifications. Set to the email address of the workflow manager.

Option	Description
SenderName	The optional name of the notifications sender. This should be the name of the person to whom notification replies will be sent.
Enable SSL/TLS	Select this option to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) communications with the SMTP server. SSL/TLS is not used by default. To use this option, the mail server requires TLS 1.2.
Auth Type	Specify the authentication type used by the SMTP server (such as Basic, Digest, or Password).
UserName	The user account to be used for authentication with the SMTP server. If notifications do not work with this account, the account under which the Enterprise Server service runs might need to be changed with the DCOMCNFG tool to an account that is more compatible with the SMTP server. By default, the service runs under the **Local System** account but it might need to be changed to **Network Service** or a logged on domain account, for example.
Password	The password to be used for authentication with the SMTP server.
Retries	The number of retry attempts that the Meridian Application Server will make if an email notification fails. The default value is **3**, and the maximum value is **20**. This value is stored as part of the **MailServerParameters** setting in the HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<vaultname> registry key.
Retry Delay	The interval in seconds between each retry attempt. Insert a value between 3 and 600 seconds.
Transmission interval	The time in minutes between each batch of PowerWeb email notifications. The default value is **5** minutes.
Group emails	Set to **True** to combine multiple PowerWeb notifications into a single email, sent according to the **Transmission Interval**. The default value is **False**.

Specify Different Mail Server per Vault

- Set the **MailServerParameters** registry value as described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<vaultname>.

Administer Meridian Enterprise Remotely

The Meridian Enterprise services can be administered remotely in two ways:

- Remote access software
- Meridian Enterprise Administrator program

Most IT departments use remote access software to administer servers from a central location. It can also be used to work with the Meridian Enterprise Administrator run on the Meridian Enterprise server. No special configuration is necessary.

The Meridian Enterprise Administrator tool can also be used to administer Meridian Enterprise from a client computer. This option is useful if responsibility for administering Meridian Enterprise should be specified to a user who should only have access to administer Meridian Enterprise and nothing else on the server.

To administer Meridian Enterprise from a client computer with Meridian Enterprise Administrator:

1. Install the Meridian Enterprise Administrator program on the client computer from the Meridian Enterprise installer package.
2. Open the Meridian Enterprise Administrator.

   Meridian Enterprise Administrator manages the current (**Local**) computer by default.
3. From the **Action** menu, select **Connect to Another Computer**.

   The **Select Computer** dialog box appears.
4. Select **Another computer** and either type the Meridian Enterprise server computer's name or click **Browse** and select the Meridian Enterprise server.
5. Click **Finish**.

   The connected computer's name appears in the left pane instead of the text **(Local)** and the Meridian Enterprise Administrator now affects that computer instead of the local computer.

> **Note:**
> Not all Meridian Enterprise services can be administered remotely with Meridian Enterprise Administrator, in particular, Accruent License Server and PowerWeb. However, they require minimal ongoing administration once initially configured compared to the other services, which can be administered remotely.

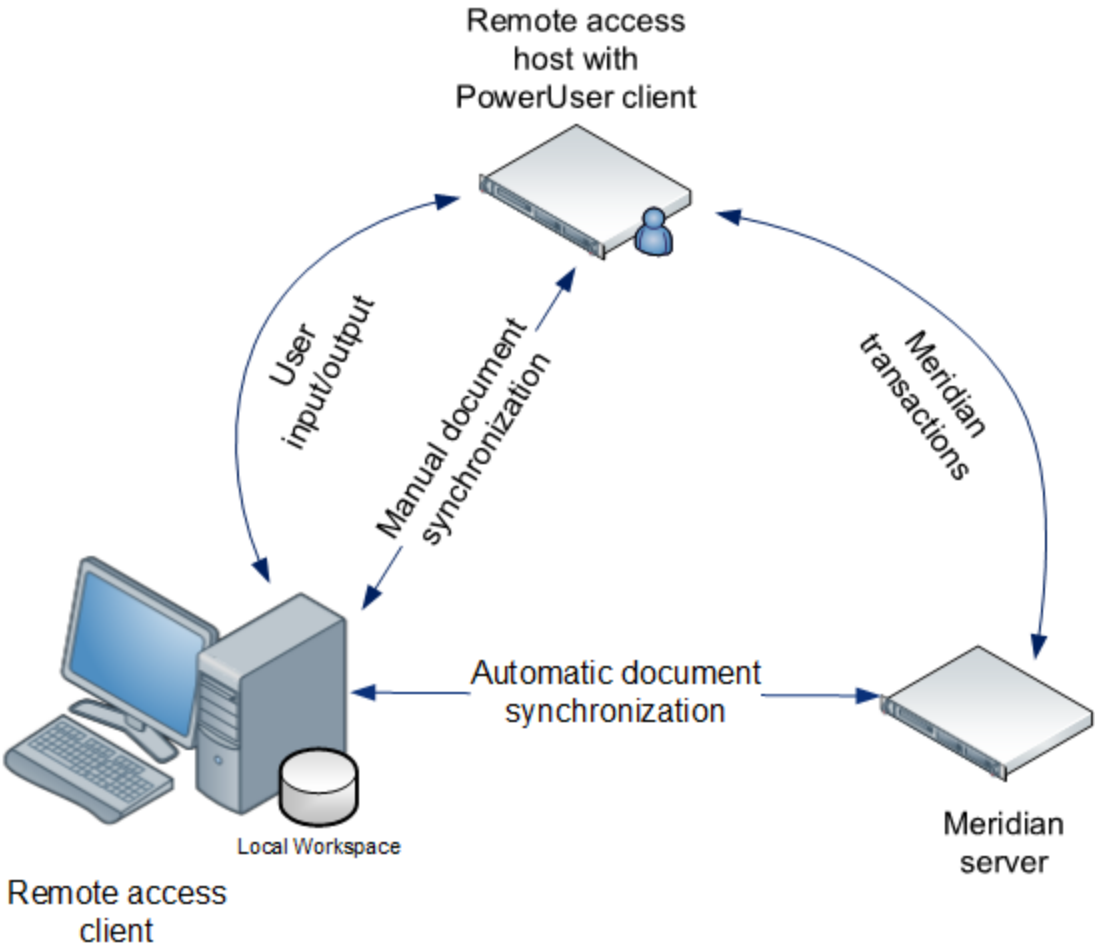
Remote Access Support

The PowerUser client application can be run remotely using popular remote access software such as Windows Terminal Server by Microsoft or Citrix Delivery Center by Citrix Systems. Support for remote access in Meridian is implemented in a generic way independent of the remote access software that is actually used. A minor limitation of this method is that it does not allow a user to automatically open documents on the remote access client computer the same as they could if they were running the PowerUser software locally. Instead, documents can be downloaded to the remote access client computer with the **Download document** or workflow commands. After downloading, the documents can be selected and opened with their native applications installed on the remote access client computer.

The key issues for supporting Meridian remote access are:

- Enabling the Meridian Offline mode commands
- Document delivery to and from the remote access client computers for editing
- Document locking
- Client licensing
- Viewing performance

Meridian remote access involves a minimum of three computers. In a remote access session, the remote access client computer connects through the remote access software to the remote access host computer where the PowerUser client application runs. The remote access host interacts with the Meridian application server as though it were a normal Meridian client except that it is configured to store documents in the remote access client computer's Local Workspace where they can be edited by the user with local applications. The relationships between the three computers are illustrated in the following figure.



Note:
Meridian supports remote access by the PowerUser client application only. The other client applications are not supported for remote access. If a different Meridian client is required, consider using PowerWeb.

Configuration of the three computers to support remote access is explained in the following topics.

Reserve Licenses For Remote Access

To ensure that a license is available for remote access, one license must be reserved for every remote access user by configuring the appropriate License Server settings as described in Reserve Licenses. Otherwise, named licenses should be assigned to the remote access users.

Prepare the Meridian Server For Remote Access

By default, the PowerUser client application uses the viewer installed on the remote access client computers. Performance in this configuration, particularly for documents with external references, is typically slow because the documents to be viewed must first be downloaded to the client computers.

Prepare the Remote Access Host Computer

The remote access host computers must be configured to display the Offline mode commands in the PowerUser client application. They should synchronize changed documents on every Offline command, but use the remote client computers' Local Workspace for storage.

If a pool of remote access host computers will be used, the Local Workspace lock ID, which normally identifies the computer where the client is run, must be set to a common value for all of the remote access host computers.

Notes about functionality

- To switch the user interface language of Meridian Enterprise to accommodate remote access users in different locales, see Install Second Language Support.
- If AutoCAD will be run over the remote connection and title blocks will be synchronized from the PowerUser client, set the registry keys accordingly that are described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AutocadLink.

Procedures

1. If documents that include external references will be edited by remote access client computers, install the documents' native application on the remote access host computer.

   This is required to resolve the external references of documents downloaded to the remote access client computers.
2. As described in Install the Client Components, install the following:
   - Meridian client applications that will be used by the remote access client computers
   - the appropriate application links
   - Application Integration components
3. Create the following values if they do not already exist and set them.

   As described in HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Client\Settings
   - OfflineMode
   - **WorkSpaceLocation**

   As described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client

- **RunRemoteApp**
- UseCICO
- **WorkSpaceDB**
- **WorkSpaceLocation**
- WorkSpaceLockID for remote PowerUser users, **CommonWorkspace** on the Meridian web server for remote PowerWeb users as described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\Published Locations\<ID>.

The preceding registry values are for 64-bit Application Integration. If only the 32-bit version of Application Integration will be used on a 64-bit PC, set the same values in the **Wow6432Node** branch as described in HKEY_LOCAL_MACHINE\Software\Wow6432Node. `AMHookTray.exe` may need to be restarted for the changes to take effect.

Prepare the Remote Access Client Computers

We recommend that the remote access client computers be configured to support integration with the third-party applications installed there and with a local workspace for best performance. The following task describes how to configure that support. If documents must be prevented from being downloaded to the remote access client computers, then this task should not be performed, in which case documents will be edited in the local workspace located on the remote access host computer instead.

The following task configures:

- Meridian to work in Offline mode
- A local workspace location on the local computer to store working copies of offline documents

To prepare the remote access client computers for remote access:

1. Install at least one of the Meridian client applications, the appropriate application links, and the Application Integration components as described in Install the Client Components.
2. Open Registry Editor on the remote access client computers and locate the following key:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager Meridian\CurrentVersion\Client`

3. Create the following values if they do not already exist and set them.

   As described in HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Client\Settings

   - **OfflineMode**
   - **WorkSpaceLocation**

   As described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client

   - **RunRemoteApp**
   - UseCICO
   - **WorkSpaceLocation**

   The preceding registry values are for 64-bit Application Integration. If only the 32-bit version of Application Integration will be used on a 64-bit PC, set the preceding values in the **Wow6432Node** branch instead as described in HKEY_LOCAL_MACHINE\Software\Wow6432Node. `AMHookTray.exe` may need to be restarted for the changes to take effect.

After the remote access client computers have been configured, they can use the Offline mode commands and functionality described in *Offline Mode And Remote Mode* in the *Meridian Enterprise User's Guide*.

Configure OpenId Connect

A standalone tool is installed with Meridian Enterprise to configure these Meridian clients to work with any OpenId compatible identity provider:

- PowerWeb
- Meridian Explorer (see the *Configure SAML Authentication* article in the *Meridian Enterprise Server Administrator's Guide*.
- Application Integration (site cache web server and site cache client)
- Remote CAD links

The tool allows you to enter and test authentication details in a simple graphical user interface and to enable or disable authentication for specific clients. You should understand how to also configure an on-premises firewall to allow inbound connections if required.

- To request the client secret and client ID that will be generated by the Meridian CloudOps Team, open a support case with the information below:
  - **IssuerUri**: https://auth-prd.meridiancloud.net/auth (change it to .eu if you have a tenant in Europe).
  - **M360Tenant**: Your Meridian Tenant unique name
  - **M360Domain**: meridian360.com (change it to .eu if you have a tenant in Europe).
  - **PowerWebAppUrl**: http://localhost/meridian

    This PowerWeb URL must be accessible externally from outside your network.
  - **ExplorerWebAppUr**: http://localhost/BCEnterprise

    This Explorer URL must be accessible from outside your network.
- To use OpenId Connect, you don't need to have the Meridian clients (PowerWeb, Explorer and Enterprise Server) accessible from outside your corporate network.

To configure authentication:

1. On the Meridian Enterprise server, run `C:\Program Files\BC-Meridian\Program\SAMLConfigurator\SAMLConfigurator.exe`.

   The tool window opens.
2. Click options or type values using the descriptions in the following table.
3. Click **Apply and Continue**.

   The Meridian Cloud logon page opens in a browser window.
4. Select an authentication provider and enter valid credentials.

5. When you have successfully configured and tested authentication, click the **Enable** button for each client for which you want to enable OpenId authentication.
6. Enter the client secret and client id provided by Support.
7. Enter the other appropriate information.
8. Click **OK**.
9. Repeat these steps until the process is complete.

   The authentication options are saved for the corresponding clients.
10. Select the **Meridian groups** option as described in Configure the EDM Server Service.
11. For more information or to manually configure authentication, click the corresponding help button (**?**) in the tool.

    Instructions will open in a new window.

OpenId configuration options

Option	Description
IssuerUri	`https://auth-ci2.meridiancloud.io/auth`
M360Tenant	Your Meridian Cloud account name
M360Domain	`meridian360.io`

Troubleshoot Server Performance and Stability

An exhaustive reference on Meridian troubleshooting is beyond the scope of this document, but the following table is a troubleshooting checklist that you can complete on your own before contacting your Accruent Partner or Accruent Technical Support for assistance. If you contact Accruent for assistance with performance or stability problems, we will assume that you have read this document and that the recommendations in this checklist have been fully implemented.

Troubleshooting server performance and stability includes steps that should be performed in the order listed in the following table. Use the hyperlinks in the following checklist to find information in the remainder of this appendix and elsewhere in this guide about performing each step. Track your progress by printing this checklist and writing a check mark in the box in the **Completed** column as you finish each step.

Server troubleshooting checklist

Completed	Step	Topic Reference
	Determine the extent of the problem. Answer the following questions, looking for patterns and shared factors: • Does the issue appear to be limited to the server or does it seem to originate on the client computers? • How many and which computers are affected? • Does it affect all vaults or only one? • Can you reproduce the problem? • When did the symptoms first occur? • Do symptoms occur consistently throughout the day or only during certain periods?	
	Configure the Windows Performance Monitor	Configuring the Windows Performance Monitor
	Verify that the affected computers meet or exceed the system requirements	Meridian Servers System Requirements For Meridian Clients

Completed	Step	Topic Reference
	Ensure that sufficient physical memory, virtual memory, and free disk space are available on both the server and client computers. For the server computer, it is very important that the `AMEDMW.exe` server process has enough memory available to prevent memory and performance issues. This also applies to virtual environments such as VMWare. Use the Windows Performance Monitor to track memory usage over time to determine the peak server load times and to monitor memory and available disk space. We recommend using Performance Monitor instead of Task Manager because the Performance Monitor is more accurate, provides much more information, and the information can be logged for further analysis.	CPU
	If the vault cache settings are set correctly and you are still experiencing performance issues, try to reproduce the issue in a new Hypertrieve vault located on the same server. Make sure that the vault has no VBScript event code configured. If the issue is not reproducible, the cause of the issue may be the configuration of the problem vault. If the database engine of the vault is SQL Server or Oracle, contact the database administrator to check the database configuration. Both SQL Server and Oracle have several settings that can affect the amount of memory consumed by a database. These can affect the amount of available memory on the server computer.	Optimize Vault Performance
	If the issue can still be reproduced at this point, the issue may be related to the network, SAN/NAS storage, or server computer hardware performance. If the vault files reside on a SAN or NAS device, see if the performance issue is resolved if the content (streams) files are relocated to the Meridian server computer.	
	As a final check, test if the issue is reproducible on a test server. From our experience, performance and stability issues can be sometimes be related to malfunctioning hardware that is difficult to diagnose.	

If none of these steps resolve the problem, contact your Accruent Partner or Accruent Technical Support for assistance.

Configure the Application Event Log Filter

Meridian invisible events are written to the Windows **Application** log. By viewing the log, you can browse for any Meridian problems.

When you're troubleshooting, you can increase the level of detail logged by using this registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager Meridian\
CurrentVersion\File System\Parameters\LogFilter
```

The hexadecimal value is a bit mask of:

Application log filter registry values

Value	Level
0x00000001	Log success
0x00000002	Log information
0x00000004	Log warnings
0x00000008	Log errors

The default is **8**, only report errors. To log warnings also, set the value to 8 + 4 = 12 (0x0C hexadecimal). Logging information and success messages is not recommended as it can seriously impact performance.

Configuring the Windows Performance Monitor

The Windows Performance Monitor is an accurate tool for measuring Meridian application server performance.

With it, you can:

- Monitor real-time and historical system performance
- Identify trends over time
- Identify bottlenecks
- Monitor effects of system configuration changes
- Determine system capacity

Some of the most relevant Performance Monitor counters are described in the following table.

Relevant Performance Monitor counters

Counter	Description
Processor Queue Length	This counter of the **System** object is an indicator of the number of outstanding requests the processor has in its queue. Each application thread requires a certain number of processor cycles. A consistent processor queue length greater than 2 may mean the processor is inadequate for the applications that it runs.
Avg. Disk Queue Length, Current Disk Queue Length	These counters of the **Logical Disk** object monitor the average number and the instantaneous number of both reads and writes queued for the selected disk. **Note:** For best performance, **Avg. Disk Queue Length** should not exceed two requests per disk drive.

Counter	Description
% Disk Time, % Disk Read Time, % Disk Write Time	These counters of the **Logical Disk** object monitor the percentage of time spent servicing the particular I/O requests during the sampling interval. Use the **% Disk Time** counter in conjunction with the **% Processor Time** counter of the **Processor** object to determine the time the system spends executing I/O requests or processing non-idle threads. Use the **% Disk Read Time** and **% Disk Write Time** counters to gain further insight into the type of I/O being performed. Your goal is to have a high percentage of time spent executing non-idle threads (high **% Processor Time**) and executing I/O (high **% Disk Time**). On a highly optimized system, these counters can be consistently over 90 percent. If one of these counters is substantially lower than the other, it is likely that the high counter indicates a bottleneck, and further investigation is necessary. With high **% Disk Time**, use the **% Disk Read Time** and **% Disk Write Time** counters to get the I/O breakdown. With high **% Processor Time**, use the **% User Time** and **% Privileged Time** to get further CPU utilization breakdown.

The data captured by Performance Monitor can be very useful for problem diagnosis and configuration analysis. You might be asked by Accruent Technical Support to log performance data and send it to Accruent for analysis.

To log Performance Monitor data:

1. Open the Performance Monitor on the Meridian application server.
2. Create a new counter log or data collector set, depending on the version of Windows.
3. Add all counters of the **AutoManager EDM Server** object.
4. Set the sample interval to between 15 and 120 seconds, depending on the duration of the problem.
5. Start the log just before reproducing the problem and run it long enough to capture a representative sampling of the problem behavior.
6. Compress the resulting log file into a ZIP file and send it together with a CAB file created as described in Create a System Status Report to Accruent Technical Support as instructed.

System Status Reporting

When troubleshooting Meridian performance or configuration issues with a Accruent Partner or Accruent Technical Support, you might be asked to provide a system status report produced by the AMRepU tool, typically for the Meridian application server only. AMRepU gathers configuration and event information from many system resources into a single file that can be sent to a remote technical support representative. The information allows the technical support representative to review the most important information about a Meridian system without requiring physical access to the system. We recommend that all technical support representatives, application engineers, and System Administrators become familiar with using this tool and the report files it produces.

AMRepU produces a CAB file that is a compressed archive that contains numerous other files generated or copied by AMRepU. The CAB file can be opened with applications like WinZIP, WinRAR, and the newer versions of Windows. Because the file is already compressed, you do not need to compress (ZIP) it before sending it via email or uploading the file to an FTP site.

If you are familiar with the information contained in an AMRepU report file, you can perform some basic system troubleshooting yourself. We recommend that you review the information contained in an AMRepU output file regularly. By examining the report results from known good systems, you will gain experience in interpreting the information. That experience will make it easier to identify and diagnose suspicious results in problem situations.

The following topics describe how to produce an AMRepU report file and to interpret the results in several of the files it contains.

Create a System Status Report

AMRep.exe (AMRepU.exe on 32-bit computers) is a command-line tool that can be run on a Meridian application server or client computer to gather configuration and status information useful for troubleshooting. Running this executable is completely safe and typically can be done during production hours because it does not interact or interfere with any Meridian components that might also be running.

AMRep.exe accepts several parameters that are described in the following table. The command-line syntax is:

AMRep <*OutputFolder*> [/ds] [/bu]

The output file will be named AMReport<*32 or 64*>_<*ComputerName*>_<*Date*>.cab where <*32 or 64*> is the 32-bit or 64-bit report, <*ComputerName*> is the name of the computer where AMRepU is being run, and <*date*> is the current date, for example, AMReport64_MyServer_10042009.CAB. The 32-bit program AMRepU.exe produces only the 32-bit report. The 64-bit program AMRep.exe produces both the 32-bit and 64-bit reports since 32-bit components are also installed.

AMRepU command-line parameters

Parameter	Description
<*OutputFolder*>	The folder in which to store the output file. The DOS shorthand characters "." (current folder) and ".." (parent folder) are accepted. This parameter is required.
/ds	Includes all vault databases (excluding stream files) in the output file. This can cause the output file to become very large. Optional. **Important!** AMRep.exe will temporarily stop the Meridian services in order to do this. Therefore, do not use this option while the server is in use. Do not use this option unless specifically asked to do so by a technical support representative.
/bu	Includes the Backup folders of all vault databases (excluding stream files) in the output file. The Meridian services will not be stopped if this switch is used. This can cause the output file to become very large. Optional. Although AMRep.exe doesn't stop any services when this switch is used, it can temporarily put a heavy load on the server, which will result in decreased performance. Do not use this option unless specifically asked to do so by a technical support representative.
/ext	Includes the contents of the extensions share in the output file. By default, these are located at C:\BC-Meridian Extensions.
/ch:<*Drive*>	Runs CHKDSK on the specified drive and includes the results in the output file.

To create a system status report:

1. Open a command-line window on the computer where you want to run the program.
2. Change the current folder to the Meridian program folder `C:\Program Files\BC-Meridian\Program`, by default.
3. Type the program name, specify the necessary parameters, and press Enter. The following example will produce a basic report file in the current folder:
   `C:\Program Files\BC-Meridian\Program>AMRep`
4. As `AMRep.exe` runs, progress messages are shown in the command-line window. Completion can take several minutes.
5. When `AMRep.exe` is finished, you can open the resulting `.cab` file to review the results.

   An `AMRep.exe` output file (`*.cab`) contains the files described in the following table.

AMRep.exe output file contents

File Name	Description
*.dat	Symantec Norton AntiVirus configuration files (files > 10 KB in size are skipped)
*.hdb	Hypertrieve database file (requires /ds parameter)
*.log	Hypertrieve database log file (requires /ds parameter)
*.log	Backup of Hypertrieve database log file (requires /bu parameter)
*.snb	Hypertrieve database snapshot backup (requires /ds parameter)
*.snp	Hypertrieve database snapshot (requires /ds parameter). Not added if `*.snb` exists
*.snp	Backup of Hypertrieve database snapshot (requires /bu parameter)
*_ALLOC.CSV	Hypertrieve allocation information
amfs.log	AMFS service log file
AMM_Installed DataStores.txt	A listing of vaults and the amount of disk space used
AMM_Installed DataStores.txt.dir	Directory listings for each vault folder
AMMamacad.ini	AutoCAD application link settings
AMRepFiles.csv	A listing of all files included in the CAB file

File Name	Description
Application Events.csv	An export of the Windows Application Event log
BLUESCRN.TXT	Dump of BlueSave
boot.ini	Windows boot configuration file.
CacheLoader.ini	Cache loader settings
CU_Cyco.txt	An export of Meridian-related registry settings under HKEY_CURRENT_USER
DataStore.ini	Settings of installed datastores
Drivers.txt	A listing of Windows drivers
HyperCache.evt	HyperCache event log
HyperTrieve.evt	Hypertrieve event log
BCME<*Version*>-Setup<*Build*>.log	Setup log files where <*Version*> is the installed Meridian version number and <*Build*> is the build number
iFilters.txt	Information about installed Indexing Service content filters
IIS_ ApplicationPools.txt	Properties of the application pools used by Meridian Enterprise and Meridian Enterprise Server.
IIS_ WebApplications.txt	Properties of the web applications installed by Meridian Enterprise and Meridian Enterprise Server.
LM-Autodesk.txt	An export of registry settings related to Autodesk software
LM_Classes_AppID.txt	An export of registry settings related to class AppIDs
LM_Cyco.txt	An export of Meridian-related registry settings under HKEY_LOCAL_MACHINE
LM_HotFix.txt	An export of registry settings related to Windows hot fixes
LM_McAfee.txt	An export of registry settings related to McAfee software
LM_Memory_ Management.txt	An export of registry settings related to Windows memory management
LM_MsOle.txt	An export of registry settings related to OLE
LM_MSSQLServer.txt	An export of registry settings related to SQL Server
LM_Services.txt	An export of registry settings related to installed services
LM_Symantec.txt	An export of registry settings related to Symantec software

File Name	Description
LM_Uninstall.txt	An export of registry settings related to uninstall information
Scheduled Jobs.txt	An export of jobs in Windows Task Scheduler
Security Events.csv	An export of the Windows Security log
SetupLog.csv	A listing of files installed by Meridian
System Events.csv	An export of the Windows Events log
System Information.txt	System information
USERS_*_Intl.txt	An export of registry settings related to the current international region from the **Default**, **LocalService**, **LocalSystem**, and **NetworkService** registry sections

Review the Server Configuration Information

To review the server configuration information in an AMRepU output file:

1. View the creation date and time of the CAB file.

   For the memory usage statistics, it is important that the CAB file was created during business hours when typical activity occurs.

2. Locate and open the CAB file generated by AMRepU with WinZIP or a similar program.
3. Locate and open the `System Information.txt` file and review the recommendations in the following table.

Server configuration recommendations

Data	Recommendation
Total physical memory	The amount should meet the requirements listed in Meridian Servers.
Available physical memory	There should be at least 300 MB of available physical memory during normal use. If there is less than 100 MB available when server performance is slow, the problem may be a lack of available memory. See Optimize the Server Operating System
Available free disk space	Each disk should have at least 15% free.
File system type	The drive where the vault-related data is stored should be NTFS.

4. Locate and open the `LM_Cyco.txt` file and review the recommendations in the following table.

   This file contains the contents of the Cyco branch of the local machine registry hive.

Registry value recommendations

Setting	Recommendation
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager Meridian\<*Version*>\PatchLevel	We are continuously improving product performance. Check that the latest version of the software is installed.

Setting	Recommendation
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\ AutoManager Meridian\ CurrentVersion\File System\Parameters\TemporaryLocation	Should point to a local NTFS drive with enough free disk space.
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\ AutoManager Meridian\ CurrentVersion\HyperTrieve\BatchCallThreshold	By default, this setting is **1F4**h (**500** decimal). See Configure the BatchCallThreshold Setting.
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\ AutoManager Meridian\ CurrentVersion\Installed DataStores\DefaultDataStore	Should point to an existing vault, preferably the most used one.
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\ AutoManager Meridian\ CurrentVersion\Installed DataStores\<vaultname>\ CompoundItemService\MaximumCacheSize	The value should always be lower than the amount of physical memory. See Configure the MaximumCacheSize Setting.
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\ AutoManager Meridian\ CurrentVersion\Installed DataStores\<vaultname>\ CompoundItemService\RelativeCacheSize	The default value is **46**h (**70** decimal). See Configure the RelativeCacheSize Setting.
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\ AutoManager Meridian\ CurrentVersion\Installed DataStores\<vaultname>\ CompoundItemService\TraceOn	Should be **0** at all times.
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\ AutoManager Meridian\ CurrentVersion\Installed DataStores\<vaultname>\ CompoundItemService\TraceName	Should be empty at all times.
HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\ AutoManager Meridian\ CurrentVersion\Installed DataStores\<vaultname>\ StreamService\RootPath	Should point to a local NTFS disk or high-performance connection to another data storage device.

5. Locate and open the `LM_services.txt` file.

   This file contains a listing of all services that are installed on the server. Review this file for any resource-intensive services. Suspicious services can include virus scanners, server management scanning tools, other server applications such as Exchange, Lotus Notes, and so on, or installable file systems.

6. Locate and open the `Drivers.txt` file.

This file contains a listing of all device drivers that are installed on the server. Review this file for any resource-intensive drivers.

Event Logs

The **AMRepU** output file contains the contents of both the System and the Application event logs. Both files are in comma-separated value (CSV) format. You can view these files in Microsoft Excel. If Excel does not recognize the comma as a column separator, then you have to make changes to your local region settings. The **Sort** and **Filter** options on the **Data** menu of Excel are very useful for analyzing trends.

The best practice is to review the server event logs on a regular basis, not only when troubleshooting problems, but even when the server is running well. Analyzing event logs from a server that is running well will give you experience with the different events. It will teach you which events are common so that you don't have to spend time on them when analyzing event logs when problems occur.

If certain events are not clear to you, visit www.eventid.net. There you can search for additional event information and best practices based on the event source and the event ID.

The following topics describe the important events to review in the System and Application event logs.

Review the System Event Log

To review the System event log:

1. Open the CAB file generated by AMRepU with WinZIP or a similar program.
2. Locate and open the `System Events.csv` file and review the recommendations in the following table.

System event log recommendations

Source	Event ID	Description	Recommendation
Application Popup	26, 50	"Application popup: Windows - Delayed Write Failed."	This is typically a false error and data is not lost at the time of the event.
Application Popup	26	"The Application Log is full."	If the event file is full, you will not get important information about your system. Change the event log settings in order to overwrite older information when the event log reaches its maximum size.
Eventlog	6008	"The previous system shutdown at <*Tme*> on <*Date*> was unexpected."	This event occurs when the server has crashed with a "stop" error (blue screen). In most cases, this error is not caused by a Meridian service. Analyzing a Windows full or mini dump file will tell you more about the cause. The creation of dump files should be enabled on the server.
Print	10, 13, 45		We strongly recommend not using the Meridian server as a print server.
Service Control Manager	7022	"The Accruent Filesystem Server service hung on starting."	Ignore this message. It is just a timeout in the system boot process.
Srv	2013	"The C: disk is at or near capacity. You may need to delete some files."	This event is raised when a hard disk has less than 15% available disk space. It is known that performance degrades when an NTFS volume is at or near capacity. The server can stop responding (blue screen) if the C: drive is full.

Review the Application Event Log

To review the Application event log:

1. Open the CAB file generated by AMRepU with WinZIP or a similar program.
2. Locate and open the `Application Events.csv` file and review the recommendations in the following table.

Application event log recommendations

Source	Event	Description	Recommendation
AutoManager OML	259	"Vault status for Datastore *<DatastoreName>*, Section *<VaultName>*: 0, 0, 0, 0, 0, 0"	If the numbers are all **0**, the vault is consistent. If any of the numbers is not **0**, see Run the Vault Consistency Wizard. The numbers are the quantity of each of the following items found in the vault: Value 1: "Ghost" documents in the **Explorer** view. The documents disappear from the **Explorer** view when selected. Value 2: Documents without document types or property values. Value 3: Garbage objects. Value 4: Documents that cannot be opened or viewed. Value 5: Documents that appear in searches, but disappear in the **Explorer** view. Value 6: Usually related to referenced documents that cannot be found.
Hypertrieve	257	"File locked (133) *<file name>*'"	Another process (for example, antivirus scanner or backup program) is locking the Meridian database files.
Hypertrieve	257	GetNamedChild, GetObjectSetViaRoute, or GetRestrictedSet and "999, Out of memory"	Out-of-memory errors appear when the EDM Server service requests more virtual memory than is available. See Optimize the Server Operating System.
AutoManager EDM Server	256	"Error 2 reported by memory manager."	See Optimize the Server Operating System.

Source	Event	Description	Recommendation
AM Compound Item Service for Database Engine	2	“The Database reported an unexpected error.”	See Optimize the Server Operating System.

Windows Registry Keys

In this section we list the registry settings created and used by the Meridian Enterprise server and client applications. Additional operating system or third-party application registry settings may have an effect on the performance or usability of Meridian Enterprise but are beyond the scope of this document and are not listed here.

The descriptions of value data and their effects are general and not guaranteed to be complete. The effects of settings may also change slightly between Meridian Enterprise versions.

The Meridian Enterprise 32-bit components run in WOW64 mode on 64-bit editions of Windows and access keys and values that are stored in the following registry sub-key:

```
HKEY_LOCAL_MACHINE\Software\WOW6432node
```

For more information, see Registry changes in x64-based versions of Windows Server 2003 and in Windows XP Professional x64 Edition on the Microsoft Support website.

> **Important!**
> Do not modify any of the following keys except as instructed elsewhere in Meridian Enterprise documentation or by your Accruent Partner or a Accruent Support representative.
>
> Making changes to the system registry can cause serious, system-wide problems that may require you to reinstall Windows to correct them. Make a backup of settings before making any modifications you are unsure about. Edit the registry at your own risk.

Server Registry Keys

The following tables list registry keys that can be found on a Meridian application server computer.

HKEY_CLASSES_ROOT\CLSID

The following table lists the registry keys of the HKEY_CLASSES_ROOT hive.

Registry values

Key Name	Value Name	Data Type	Value Data
{B34AA9A3-B4A7-11D0-A75B-002018345407}	ThreadPriority	DWORD	A number between -15 and +15 for the priority of a new thread for the Compound Item Server service. Zero (0) is the default priority. If this value is not present, the Compound Item Server service will run in the main thread.
{46115012-3B1B-11D1-B41D-002018345407}	ThreadPriority	DWORD	A number between -15 and +15 for the priority of a new thread for the Stream Server service. Zero (0) is the default priority. If this value is not present, the Stream Server service will run in the main thread.

HKEY_LOCAL_MACHINE

The following tables list the registry keys of the HKEY_LOCAL_MACHINE hive.

HKEY_LOCAL_MACHINE\Software\Cyco

Registry values

Value Name	Data Type	Value Data
Active Product	String	Internal name of the active Meridian product.
AmAcDbHost<*n*>	String	Path of the active AutoCAD database library file.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian

Registry values

Value Name	Data Type	Value Data
Path	String	Path where the application is installed.
ProgramPath	String	Path to the application executables.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\<*PatchLevel*>

Registry values

Value Name	Data Type	Value Data
PatchLevel	String	Version name of the installed Meridian application.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\File System\Connections

Registry values

Value Name	Data Type	Value Data
<*DriveLetter*>	String	Vault context assigned to <*DriveLetter*>

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\File System\Parameters

Registry values

Value Name	Data Type	Value Data
LogFilter	DWORD	See Configure the Application Event Log Filter.
NoImportFilters	String	List of file extensions and descriptions to be excluded from the vault to the location specified by TemporaryLocation. Defined in Configurator.
TemporaryLocation	String	Path of the folder to store temporary files excluded from the vault by filters defined in Configurator.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\File System\Shares

Registry values

Value Name	Data Type	Value Data
<*ShareName*>	Binary	Drive shared as <*ShareName*>

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Hypertrieve

Registry values

Value Name	Data Type	Value Data
AllowMaxProperties	DWORD	If **0** (default), property count is limited to 32,768 entries. If property count exceeds this value, the engine will be stopped. To repair the situation, it is possible to increase the limit by setting this registry entry to a non-zero value. The absolute maximum is 65,535 properties. Beyond that the vault cannot be opened anymore. Having so many properties in a vault is not normal. Usually this is caused by many different sequence names being generated in script. If this situation occurs, the use of sequences in script should be changed. If that many different sequences are needed, an alternative method should be considered, such as generating sequence numbers using a SQL database. If old sequences are not needed anymore, they can be removed from the vault using the ImportFilterFile registry setting.
BatchCallThreshold	DWORD	Number of database calls beyond which a transaction is deemed to be a batch transaction. Default = **500** No load balancing = **0** See Optimize the Meridian Server Software and Configure the BatchCallThreshold Setting.
CheckTerminated	DWORD	If this value is **1**, enables extra runtime low-level data consistency checks to be performed and reported to event log. Significantly decreases database engine performance. If this value is **0** (default), disables extra consistency checks at runtime.

Value Name	Data Type	Value Data
CreateMiniDump	DWORD	If this value is **1**, a memory dump file is generated that can be sent to Accruent Technical Support for troubleshooting. If this value is **0** (default), no file is generated.
DebugAllocation	DWORD	If this value is **1**, allocates extra memory to debug memory overwrite problems. If this value is **0**, disables extra consistency checks at runtime.
DefaultEngine	DWORD	Not used.
Disable_Double_Records_Report	DWORD	If this value is **1**, duplicate records are checked during VCW repair but not reported. If this value is **0** (default), duplicate records are reported. For internal use only.
DumpAllocation	DWORD	If this value is **1**, forces engine to dump compartment allocation information when database is closed. If this value is **0** (default), disables dump.
IgnoreShutdownFlag	DWORD	If this value is **0**, skips restore when opening a database containing inconsistencies. If this value is **1**, restores the database by executing the log file with the most recent snapshot.
OldCheckRepairAlgorithm	DWORD	If this value is **1**, uses old, slower repair algorithm during VCW repair. If **0** (default), uses new algorithm.
PageAllocationTrace	DWORD	If this value is **1**, enables page allocation tracing. If this value is **0** (default), disables tracing.
TraceControl	DWORD	If this value is >**0**, enables call logging using special SetVariant. Calls can be logged at runtime by setting any string property to **TRACE:+** or **TRACE:-** to turn it on and off. If this value is **0** (default), disables logging.
UseDatagrams	DWORD	If this value is **1**, indexes strings using datagrams, which speeds up pattern matching. If this value is **0**, does not use datagrams.

Value Name	Data Type	Value Data
VerboseEventFlags	DWORD	Controls generation of extended event log messages. The following values are supported: **0**: No extended messages are logged (default) **1**: Log extended messages when cache loader threads fail **2**: Log extended messages when DLLs are loaded and unloaded **3**: Log both types of extended messages
WaitInterval	DWORD	When a transaction exceeds the BatchCallThreshold number of database calls, it will be made to wait after each call for as much time as it has spent. The total wait is partitioned in individual waits of WaitInterval milliseconds. Default = **3**.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores

Registry values

Value Name	Data Type	Value Data
DefaultDataPath	String	Path to the root folder of all datastores.
DefaultLocation	String	Path to the root folder of all datastores.
DefaultDataStore	String	The name of the default datastore.
FullTextInLocalDataPath	DWORD	If this value is **1**, full-text indexing catalog (`catalog.wci`) will be placed in the folder specified by <*dbname*>\CompoundItemService\LocalDataPath. If this value is **0** or omitted (default), the catalog is created where streams are located.
MSSQL_<*ServerName*>_ AccountName	String	If SQL Server support is installed, account name (sa by default) used for SQL Server authentication. See Configure the Windows Account Used By Meridian.
MSSQL_<*ServerName*>_ Password	String	If SQL Server support is installed, password used for SQL Server authentication. See Configure the Windows Account Used By Meridian.
MSSQL_<*ServerName*>_ WindowsAuthenticationMode	DWORD	If SQL Server support is installed, mode of SQL Server authentication. Server name can be optional value. See Configure the Windows Account Used By Meridian.
ORA_<*InstanceName*>_ AccountName	String	If Oracle support is installed, account name (MERIDIAN by default) used for Oracle authentication. See EDM Server Service Account Requirements For Oracle.
ORA_<*InstanceName*>_ Password	String	If Oracle support is installed, password used for Oracle authentication. See EDM Server Service Account Requirements For Oracle.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<*vaultname*>

Registry values

Value Name	Data Type	Value Data
AlertNoBackup	DWORD	Number of days (**5** by default) since the last successful execution of the Prepare for Backup command on this vault, after which an alert is displayed when the Administrator tool is opened. If this value is **0**, do not display an alert for this vault. The alert is based on the LastSuccessfulPrepareForBackup value. See Backups And Recovery.
AuditConnectionString	String	Connection string to the audit log database. See Create an Audit Log Database.
CacheLoad	DWORD	If this value is not **0** or omitted (default), database cache is loaded. If this value is **0**, cache is not loaded.
DataStoreID	String	Twelve-digit hexadecimal ID used to name the streams and content indexing folders for this vault. See Content Indexing.
DefaultSection	String	The name of the default section in a datastore. If the section does not exist, it will be created.
EnableFullTextSearch	DWORD	If this value is **1**, content indexing is enabled for this vault. If this value is **0** or omitted (default), content indexing is cleared. See Content Indexing.

Value Name	Data Type	Value Data
FullTextCatalog	String	Microsoft Indexing Service catalog name for content indexing. If omitted (default), catalog name is based on the vault name preceded by “AM”. If the default name is not compatible with Indexing Service, an alternative name can be specified here. See Content Indexing.
FullTextCatLocation	String	Parent folder of the catalog.wci folder containing Indexing Service catalog files for this vault. When “*” (default), this value depends on the value of FullTextInLocalDataPath. See Content Indexing.
LastFailedPrepareForBackup	Binary	Date and time of the last failed backup attempt of this vault. See Backups And Recovery.
LastFullTextFilter	Binary	Date and time that content indexing was last updated successfully for this vault. See Content Indexing.
LastRecoveryLogCreated	Binary	Date and time that the Recovery Log command was last run successfully. See Backups And Recovery.
LastSuccessfulPrepareForBackup	Binary	Date that the Prepare for Backup command was last run successfully. See Backups And Recovery.
MaximumWorkflowLogSize	DWORD	The maximum workflow log size for a vault in bytes. By default this value is set to **0**, which means there is no maximum size. You can also configure this setting in the Administrator. If the user performs an action and the log exceeds the maximum configured size, lines are removed from the start of the log until the log is not larger than the maximum size.

Value Name	Data Type	Value Data
MailServerParameters	String	String of mail server parameters to use for notifications sent from this vault like: `Host=smtp-mail.outlook.com;Port=587; SenderAddress=MeridianMail@hotmail.com; SenderName=Meridian Mail. Account; EnableSSL=True;UserName= meridianmail@hotmail.com; Password=*********;AuthType=Basic` This setting is intended to be used only when multiple vaults should send notifications from different SMTP servers, for example, per the user's region. If all vaults should use the same SMTP server, it may be configured more simply as described in Specify a Mail Server.
NotificationsConnectionString	String	Connection string to the subscription notifications database. See Create a Subscriptions Database.
UseAMFS	DWORD	This is a legacy setting related to a Windows feature that is no longer supported. Do not change the default value of this setting, or you will encounter issues with clients being unable to access file contents.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<*vaultname*>\CompoundItemService

Registry values

Value Name	Data Type	Value Data
AllowSnapShot	DWORD	If this value is **0**, disable log file truncation during creation of new database snapshots. If this value is **1** (default), enable truncation. See Configure the MaximumLogSize Setting.
AlwaysCreateCheFile	DWORD	If this value is **1**, creates a cache file when the vault is closed by the EDM Server, even if the HyperCache setting is enabled. If this value is **0** (default), no cache file is created.
BackupLocation	String	The path used by Meridian to store the vault database backup files created by the **Prepare for Backup** command. If this value is not set, the default location `<DataPath>\Backup` will be used.
CopyOnlyBackup	DWORD	If this value is **0** (default) or is absent, the **Prepare for Backup** command performs a conventional SQL Server backup. If this value is **1**, the command creates a copy-only backup.
Databasename	String	The path of the vault database file if Hypertrieve is used.

Value Name	Data Type	Value Data
DatabaseNotCreated	DWORD	If this value is **0**, a new SQL Server database will not be created automatically when this vault is created. If this value is absent (default), a new SQL Server database will be created automatically. This value corresponds to the **Database exists** option in the **New Vault Wizard** as described in Create a New Vaultand must not be manipulated manually. Doing so could result in the loss of the vault database.
DataPath	String	Path used by SQL Server for data files used by this vault. If a remote SQL Server instance is used, type an existing path (UNC not supported) on the remote server.
Datastorename	String	If SQL Server or Oracle support is installed, this value will be used as a base name for locally generated files. It will also be used as a database name for Microsoft-SQL Server and as a source to generate table names for Oracle.
DetachRetention	DWORD	The amount of time in minutes the database cache will remain in memory after all users have logged out of the system. Only used in very specific situations. The default is **5**.
DllName	String	Name of the database engine DLL file that serves this vault. For information about upgrading the database engine and the filenames, see Upgrade Vaults To a Newer Database Engine.
ExtendedMemory_ EnableCache	DWORD	Enables the High Performance Option. Obsolete.
ExtendedMemory_BlockSize	DWORD	Size of individual extended memory blocks used by the High Performance Option. The default size is **1** KB. Obsolete.
ExtendedMemory_Blocks	DWORD	Number of individual extended memory blocks used by the High Performance Option. Obsolete.
HyperCache	DWORD	On 64-bit computers, if this value is **1** (default) or missing, vaults are loaded completely into cache memory and a cache file (.CHE) is not created between EDM Server sessions. To force the creation of cache files, use the AlwaysCreateCheFile setting. If this value is **0**, vaults are loaded into cache memory according to the vault's cache settings.

Value Name	Data Type	Value Data
IgnoreShutdownFlag	DWORD	If this value is **0** (default), when an unsuccessful database shutdown is detected, the database engine normally restores the database by playing the log file against the existing snapshot. If this value is >**0**, the engine does not restore the database from snapshot after unsuccessful shutdown and continues with the database, which probably contains inconsistencies.
IndexPath	String	Path used by SQL Server for index files used by this vault. If empty, uses DataPath value. If a remote SQL Server instance is used, type an existing path (UNC not supported) on the remote server.
InstanceName	String	Name of the Oracle server instance used by this vault.
IsLocal	DWORD	If this value is **1**, the Oracle instance is hosted on the local computer. If this value is **0**, the Oracle instance is hosted on a remote computer.
LocalDataPath	DWORD	Path to be used for locally created SQL Server files. If empty, DataPath will be used.
LoggingLimit	DWORD	Server performance option for use with SQL Server. See Integrate Meridian With SQL Server.
LogPath	String	Path used by SQL Server for transaction log files used by this vault. If empty, uses DataPath value. If a remote SQL Server instance is used, type an existing path (UNC not supported) on the remote server.
MaximumCacheSize	DWORD	Server performance option. See Optimize Server Hardware. and Configure the MaximumCacheSize Setting.
MaximumLogSize	DWORD	When the value set for MinimumSnapshotInterval has been reached and the log file size is greater than this value, a new snapshot will be created and the existing log file will be truncated. Server performance option. See Optimize Server Hardware. and Configure the MaximumLogSize Setting.
MaxRetries	DWORD	Server performance option for use with SQL Server. See Integrate Meridian With SQL Server.

Value Name	Data Type	Value Data
MinimumSnapshotInterval	DWORD	Timeout in minutes after which log truncation will be attempted if the value set for MaximumLogSize has been reached. Default = **240**. Server performance option. See Optimize Server Hardware.
RelativeCacheSize	DWORD	Server performance option. See Optimize Server Hardware and Configure the RelativeCacheSize Setting.
RetryWait	DWORD	Server performance option for use with SQL Server. See Integrate Meridian With SQL Server.
Schemaname	String	Name of the Oracle schema used by this vault.
Servername	String	Name of the computer running SQL Server that hosts this vault. Empty for default server located on local server.
ShutDownForBackup	DWORD	Obsolete
TraceName	String	Full local path to the trace file. If this value is not present, no trace file will be written. See Review the Server Configuration Information.
TraceOn	DWORD	If this value is >**0** and TraceName is set, activates tracing of all calls to the database engine. This reduces server performance by approximately 50%. See Review the Server Configuration Information.
UseCompatibleBackup	DWORD	If this value is **0**, the **Prepare for Backup Wizard** will create snapshot files from an Oracle vault that are compatible with the **Restart After Restore From Backup Wizard**. If this value is **1** (default), the wizard will only create backup files of the vault registration information and the data must be backed up and restored manually using Oracle tools. See Oracle Vault Backups and Prepare For Backups.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<*vaultname*>\DataServer

Registry values

Value Name	Data Type	Value Data
(default)	String	{B34AA9A8-B4A7-11D0-A75B-002018345407}

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<*vaultname*>\RegisterBehaviors

Registry values

Value Name	Data Type	Value Data
<*behaviorprogID*>	String	[*dependantbehaviorprogID*]:IsRegistered or IsNotYetRegistered

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<*vaultname*>\Services

Registry values

Value Name	Data Type	Value Data
<*serviceprogID*>	String	<*serviceprogID*>

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<*vaultname*>\StreamService

Registry values

Value Name	Data Type	Value Data
FTIRootPath	String	Parent folder of the FTI folder containing filtered content text files for this vault. When "*" (default), this value depends on the value of FullTextInLocalDataPath. See Content Indexing.
RootPath	String	The root folder used by Meridian to store the document stream data sub-folders for the vault.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\OML

Registry values

Value Name	Data Type	Value Data
BrowseForGlobalGroups	DWORD	If this value is **0**, authenticate role assignments only for local groups (default). If this value is **1**, authenticate for local and global groups. See Configure the BrowseForGlobalGroups Setting.
BrowseForNestedGlobalGroups	DWORD	Set to **1** to use nested global groups. This will work only if you use Active Directory in Native mode. BrowseForGlobalGroups should be also set to **1** for this feature to work. See Use Meridian With Nested Groups.
CacheCollections	DWORD	If this value is **0**, caching of collections is cleared. If this value is **1**, caching is enabled (default).
CacheObjects	DWORD	If this value is **0**, caching of objects is cleared. If this value is **1**, caching is enabled (default).
CacheLocalAttributes	DWORD	If this value is **1**, caches local attributes. This value can be set to 1 to make large imports faster (up to two times) by using additional memory to cache local attributes. If this value is **0** (default), no optimization will be used during hybrid Attach/Detach, and local attributes will be collected on every call.
CheckGeneralConsistencyFilter	DWORD	Run checks on vault like content without class, floating document, and so on. For internal use only.
CopyDLL	DWORD	Server performance option. See Configure the CopyDLL Setting.
CountHThreadEntries	DWORD	If this value is **1**, count every call to HTV engine DLL. For internal use only.

Value Name	Data Type	Value Data
ImplicitCreateDatabase	DWORD	If this value is **1**, create database if database does not exist. For internal use only.
ImportFilterFile	String	Path to an import filter file to be used for excluding specified properties during vault import. See Exclude Existing Property Values When Importing a Vault.
LargeSelectionThreshold	DWORD	The minimum number of documents in a static collection (for example, 1000) at which to use a special algorithm that improves server performance when deleting large static collections (the collection only, not the documents). If absent or **0**, uses the default algorithm for deleting small and large static collections, which can take more time. When a static collection is deleted by the special algorithm (LargeSelectionThreshold > **0**) the references between the documents and the now absent collection become orphaned and need to be cleaned up separately. This can be done with the **Clean up deleted static collections after successful check** option in the **Vault Consistency Wizard**. It can also be done with the command line tool `AMCleanDSC.exe` that is installed by default in the `C:\Program Files\BC-Meridian\Program` folder on the server. Run the tool with these parameters: `AMCleanDSC.exe [M:<FullyQualifiedMachineName>] <VaultName> [<DocBatchSize>] [<DelayBetweenBatches>]` The parameters are described in the following table.
MallocSpy	DWORD	If this value is **1**, enables EDM Server memory allocation spying. For internal use only.
ObjectIDStart	DWORD	First digits or new Object ID values. For internal use only.
ObjectsCacheDepth	DWORD	Maximum number of objects in cache. If this value is **0**, object cache is unlimited. Default is **200**. See Configure the ObjectsCacheDepth Setting.
ShowDialog	DWORD	If this value is **1**, EDM Server service shows OML dialog of object counter in the debug version. If this value is **0**, dialog is not shown (default). For internal use only.

Value Name	Data Type	Value Data
SkipCheckDatabase	DWORD	If this value is **1**, skip check/repair database step. If this value is **0** (default), do not skip.
UseACL	DWORD	If this value is **1**, use ACL. Otherwise (default), use security descriptors.
UseBulkLink	DWORD	If this value is **0** (default), do not use bulk link.
UseCheckGeneralConsistency	DWORD	If this value is **1** (default), skips all invalid documents and document items (versions, streams) when importing an old vault to a new vault. If this value is **0**, the check is not skipped.
UseHypertrieveThread	DWORD	For internal use only.
UserGroupCacheTimeout	DWORD	The interval in minutes at which the Meridian application server retrieves user group membership information. If the **Windows global and local groups** option is selected for the Security role assignments setting in the vault properties in the Meridian Enterprise Administrator, the information is retrieved from the Active Directory domain controller and the default is **60** minutes. If the **Accruent groups** option is selected, the information is retrieved from the user database (whether on the Meridian EDM Server or on Meridian Enterprise Server) and the default is **5** minutes. If the **Windows local groups** option is selected, this value is not used. Changing the **Security role assignments** setting from one option to another automatically adjusts this value to the corresponding default.
UseROT	DWORD	If this value is **1** (default), use Running Object Table. If this value is **0**, do not use.

AMCleanDSC.exe command line parameters

Parameter	Description
FullyQualifiedMachineName	Optional fully qualified name of the server hosting the vault to clean up. The default is the computer on which the tool is run. For example, `M:MyServer.MyDomain.com`.

Parameter	Description
VaultName	Required display name of the vault to clean up. For example, `MyVault`.
DocBatchSize	Optional number of documents in each batch to clean up. The default is **1000**.
DelayBetweenBatches	Optional time in milliseconds to pause between each batch of documents to allow for other processes to run. The default is **0**. Increase this number if there are very large deleted collections.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\OML\AMFSSharePath

Registry values

Value Name	Data Type	Value Data
(default)	String	Share name used by AMFS to allow authorized access to vault documents.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\OML\AMServerManagerAccount

Registry values

Value Name	Data Type	Value Data
(default)	String	Name of a local or primary domain Windows account to use as a rescue account. If a domain account is to be used, do not specify the domain name. See Create a Rescue Account For Security Administration.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server

Registry values

Value Name	Data Type	Value Data
DaysSinceLastOpen	DWORD	The number of days since the EDM Server service was last active. Used to display a warning to confirm the correct server time and prevent vault access. See Server Time Requirements.

Value Name	Data Type	Value Data
EnableFQDNS	DWORD	If this value is **1**, the NETBIOS names of Meridian application servers are not used and their fully-qualified domain names are used instead. This setting is provided for customers who require access to Meridian servers across domains and NETBIOS is not allowed. If this setting contains any other value, NETBIOS names are used. The default is **0**. To enable FQDNS, set the EnableFQDNS value to **1**. When set to: • **0**: If the full computer name is less than or equal to 15 characters, old rendering and profile jobs can work with DNS names. If the full computer name is greater than 15 characters, you must re register the vault with the full name and recreate all rendering profiles and jobs. • **1**: The complete paths of documents that are stored in Meridian local workspaces are longer than they would be if the setting is **0**. Some applications may not accept the longer names and fail to find documents. Before you set EnableFQDNS to **1** in a production environment, we recommend that you test it thoroughly with the longest vault paths and all expected applications. For the shortest paths, we recommend that domain, server, folder, and document names be as short as possible and that the vault folder structure to documents be as short as possible. Documents might fail to download from remote site caches. To resolve this, re-register the vault in Meridian Enterprise Server using the fully qualified domain name. Also, update the **Server URL** option of the site cache

Value Name	Data Type	Value Data
		configuration to the fully qualified domain name. Publishing jobs executed by Meridian Enterprise Server can cause undesirable results or not work at all if the source system name in the job definition is not also specified in FQDN format. **Important!** By default, each user's local workspace folder structure contains the Meridian server's NetBIOS computer name, for example, `C:\BC-WorkSpace\<UserName>\M-<ComputerName>,D-<DatastoreName>`. When **EnableFQDNS** is enabled, new local workspace folders will be created with the server's fully-qualified domain name, for example, `C:\BC-WorkSpace\<UserName>\M-<ComputerName.DomainName>,D-<DatastoreName>` and the existing local workspace files will not be copied to the new folders. Instead, new copies will be made in the new folders from the server as necessary. Therefore, **EnableFQDNS** should only be enabled after business hours and after all user local workspaces have been synchronized to the server. The old local workspaces should also be deleted to prevent users from accidentally making changes to the files in the wrong folder. For more information, see the *Configure a Publishing Job* article in the *Meridian Enterprise Server Administrator's Guide*.

Value Name	Data Type	Value Data
EnforceRenamePrivilege	DWORD	If this value is **1**, checks that a user has the Rename privilege before allowing them to rename documents. If this value is **0** or missing, the Rename privilege is not enforced (default).
EnterpriseServerAddress	String	URL of the Meridian Enterprise Server.
HyperionServerAddress	String	URL of the Meridian Enterprise Server web server to use for user account management or audit log storage.
LastEffectivity	Binary	Date and time of the last access of the server. This value is used for checking if one transaction takes place after a previous transaction, hence making sure the versioning system is working correctly.
LogLastEffectivityChange	Binary	If this value is **1**, a message is added to the **Application** event log that records when the value of the **LastEffectivity** value is changed. If this value is **0**, no additional messages are logged. This value is intended for troubleshooting mismatches between the Meridian server time and that of client PCs.
LicenseDB	String	Path to the Meridian license database file.
LicenseServerMachine	String	Fully-qualified domain name of the computer hosting the Accruent License Server. Changes take effect only when the license server, Meridian Enterprise, and Meridian Enterprise Server computers are rebooted.
HideVaultIfUserHasNoAccess	DWORD	This value is set by the **Hide vaults to which a user has no access** option of the EDM Server. Set this to **1** to hide inaccessible vaults. Set to **0** (default) to show all vaults.
RepairWorkflowProps	DWORD	If this value is **1**, the upgrade handler repairs wrong values in workflow properties. If this value is **0** or omitted, no repair is performed.

Value Name	Data Type	Value Data
SharedFolder	String	Path to the publicly shared folder that contains the PowerUser interface extensions and user assistance content. See Move the BC-Meridian Extensions Folder.
ShowUsers	DWORD	Interval in milliseconds to refresh the **Users** tab in the Meridian Enterprise Administrator. The default is 5000 (5 sec), the minimum value is 1000 (1 sec), 0 disables refresh.
TablesDB	DWORD	If this value is **1** (default for 64-bit version), lookup tables are stored in Microsoft SQL Server Compact Edition instead of in an Microsoft Access file. If this value is **0** for a 64-bit version, a 64-bit OLEDB driver must be installed separately.
TablesDBSqlCeOptions	String	Optional parameters to add to the connection string used by Meridian Enterprise to connect to the SQL Server Compact Edition database where external lookup lists are stored. By default, the connection string is not editable and includes only the **DataSource** parameter. For example, to increase the default maximum database from 256 MB to 2 GB: `SSCE:Max Database Size=2048`
TablesDBSqlCeProvider	String	The version of Microsoft SQL Server Compact Edition to use for the external tables database. The default is **Microsoft.SQLSERVER.CE.OLEDB.3.5**. To use Microsoft SQL Server Compact Edition 4.0, set to **Microsoft.SQLSERVER.CE.OLEDB.4.0**.

Value Name	Data Type	Value Data
TablesDBMsJetOptions	String	Optional parameters to add to the connection string used by Meridian Enterprise to connect to the Microsoft Access database where external lookup lists are stored. By default, the connection string is not editable and includes only the **DataSource** parameter. For example, to increase the default maximum database from 256 MB to 2 GB: `SSCE:Max Database Size=2048`
TaskServerMachine	String	Name of the computer hosting the Meridian Task Server. Set as described in Set Up the Task Server.
UseAMFS	DWORD	This is a legacy setting related to a Windows feature that is no longer supported. Do not change the default value of this setting, or you will encounter issues with clients being unable to access file contents.
UseEnterpriseServerForAuditLog	DWORD	If this value is **1**, use the Meridian Enterprise Server specified for the **HyperionServerAddress** value for audit log storage. If this value is **0** (default), use the database connection specified by the **AuditConnectionString** value as described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Installed DataStores\<vaultname>.

Value Name	Data Type	Value Data
UseEnterpriseServerForUserManagement	DWORD	If this value is **1**, use the Meridian Enterprise Server specified for the **HyperionServerAddress** value for user account storage. If this value is **0** (default), use a local Microsoft SQL Server Compact Edition database. SQL Server Compact has reached End of Life Status. We recommend using Enterprise Server for your user account storage.
UseImportedFrom	DWORD	Controls setting of the **AMFSObjectPropertySet.ImportedFrom** property during document import operations. Supported values are: **0**: Empty string **1**: Full path of the source file (default) **2**: Source file name only This setting is applied if the server registry key with the same name and described in HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Client\Settings is missing.
UsePURasOFF	DWORD	If this value is **1** (default), a PowerUser license will be claimed by the Office client. If none are available, the user will be denied access. If this value is **0**, a PowerUser license will not be claimed, and the user will be denied access. See Accruent License Server Service.
UserGroupPrefix	String	Can be used to filter the user group names returned from **IAMDocumentRepository2.GetUserGroups**. If no value is specified, all groups are returned.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server\Licensing

Registry values

Value Name	Data Type	Value Data
AuditLicenseRequests	DWORD	License server activity logging. The logged data can be viewed in the **Accruent-LicenseServer** event log. The possible values are: **0**: Disable logging (default) **1**: Log only rejected license requests **2**: Log only successfully claimed licenses **3**: Log all claimed and rejected licenses The higher the value, the more messages will be added to the event log. Non-default values should only be set for troubleshooting.
LicMgrGroup<*n*>	String	User group name for which to reserve licenses for the corresponding product. Domain user groups can be used as well as local. See Reserve Licenses.
LicMgrProduct<*n*>	String	License prefix of a product for which to reserve licenses (for example, **M—PUR** for PowerUser). See Reserve Licenses.
LicMgrRefresh<*n*>	DWORD	Interval in minutes that the License Server should wait to reread information from this registry section. See Reserve Licenses.
LicRestrictGroup<*n*>	String	User group name to which to restrict licenses for the corresponding product. Domain user groups can be used as well as local. See Restrict Licenses.
LicRestrictProduct<*n*>	String	License prefix of a product to which to restrict licenses (for example, **M—PUR** for PowerUser). See Restrict Licenses.

Value Name	Data Type	Value Data
Log	DWORD	If this value is **1** (default), license server logging is enabled. If this value is **0**, logging is disabled.
Log_FileName	String	License server log file name. The default is `%temp%\BCLicense.log` where `%temp%` is the environment variable of the user specified by **BackupServers_User**.
Log_FileSize	DWORD	Maximum license server log file size (8 MB by default). There might be many error messages when a connection is interrupted between license servers. When this limit is reached, only the most recent messages are stored. Each time the license server service starts, the log file is recreated.
PostEventOnLicenseReclaim	DWORD	To log additional events when named licenses are reclaimed by the same user, set to **1**. The default is **0**, no additional events.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server\UserDatabase

Registry values

Value Name	Data Type	Value Data
ConnectionString	String	Path to the Meridian user and group database file. For example, `C:\BC-Meridian Vaults\ICUserDB.mdb`.
UserDBSqlCeProvider	String	The version of Microsoft SQL Server Compact Edition to use for the user database. The default is **Microsoft.SQLSERVER.CE.OLEDB.3.5**. To use Microsoft SQL Server Compact Edition 4.0, set to **Microsoft.SQLSERVER.CE.OLEDB.4.0**. SQL Server Compact Edition is in End of Life Status. This setting still exists for backwards compatibility, but we recommend migrating to Enterprise Server.
UserNameFormat	DWORD	Format for the display of user names. If this registry value is missing or empty, the to-do list name only is shown. The user information shown is always that of the primary Windows account associated with the Meridian user account. The possible values and their corresponding formats include: **0**: To-do list name (Display Name) **1**: Display Name **2**: Display Name (email@address) **3**: Display Name (Domain\User) Changing this value requires that the EDM Server service be restarted to take effect.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink

Registry values

Value Name	Data Type	Value Data
AhaPortal	DWORD	If this value is **1** (default), the item **Meridian Wishlist** is visible in the user's menu in PowerWeb. If this value is **0**, the item is hidden.
AnonymousUsesNetViewer	DWORD	If this value is **0** (default), PowerWeb will not allow anonymous users to use the viewer and thereby claim licenses. If this value is **1**, the viewer may be used.
ApplyMetadata	DWORD	If this value is absent or **1**, the default behavior occurs. In this case, when users create new documents and set properties that are used in the Field-Path definition, the new values are applied as soon as possible. This can cause new folders to be created with an underscore (_) as the name . If this value is **0**, the new values are applied later in the transaction after the folder names have already been set.
CADLinkExtensions	String	Semicolon-delimited list of file extensions for which to enable the CAD application links in PowerWeb. The extensions are as follows: dst; dgn; dwg; doc; docx; docm; xls; xlsx; xlsm; ppt; pptx; pptm; vsdx; vsdm.

Value Name	Data Type	Value Data
ColumnFilteringLimit	DWORD	If the number of documents in a search result is below the threshold set by this setting, column filtering is available for the search results. If the number of documents is above this threshold, column filtering is disabled. This setting improves the speed at which search results are displayed in PowerWeb. **0**: default value, no limitations placed on search result size
CompanyLogo	String	The filename of an image to show as the logo in PowerWeb. By default, the Accruent logo is shown. The file must reside in the `C:\inetpub\AMM\Img` folder on the PowerWeb server.
CustomFullURL	String	URL of Meridian PowerWeb for use from outside the LAN (for example, `http://<YourDomain>:8082/meridian/start`). This setting should only be used as a temporary solution while troubleshooting host name resolution problems with the default URL. Also see **UseCurrentHost** in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager View Control2\Settings.
DbgXMLPath	String	Path to a folder to save XML files generated by PowerWeb. For debugging only.
DisableThumbnailUpdate	DWORD	Method used to create thumbnail images: **0** (default): Create the thumbnail image from the preview image stored in the file if it exists. **1**: Do not create thumbnail images at all. **2**: Use the web server to create thumbnail images from the source file only if no preview image exists.

Value Name	Data Type	Value Data
DisableVisibilityExpressionsOnEdit	DWORD	Controls if PowerWeb should check your VBScript for visibility expressions when the user is editing a property or wizard page. You should configure this setting if your configuration is complex and the visibility expressions in your VBScript are resulting in lag time. **0** (default): PowerWeb evaluates the visibility expressions as configured in the Configurator. **1**: When a user is editing a wizard page, PowerWeb does not evaluate visibility expressions related to the display of property pages. **2**: When a user is editing a wizard page, PowerWeb does not evaluate visibility expressions related to the display of commands. **4**: When a user is editing a property page, PowerWeb does not evaluate visibility expressions related to the display of property pages. **8**: When a user is editing a property page, PowerWeb does not evaluate visibility expressions related to the display of commands. To apply multiple settings at the same time, combine their respective values. As an example, to disable both property page visibility and command visibility expression when editing property pages, combine **4**+**8**. The result is **12**, which is the value you should use.
Domain	String	When set to a valid domain or sub-domain name, is used as the origin (`document.domain`) of web pages loaded into external property pages in the client applications. This value is intended to help achieve compliance with the same-origin policy enforced by web browsers.
DownloadInBrowser	DWORD	If this value is **0** (default), PowerWeb will download documents via external executable `AMDownload.exe`. If this value is **1**, PowerWeb will download documents inside the browser process.

Value Name	Data Type	Value Data
PDFTronFontLocation	String	Web location where you've unpacked the PDFTron fonts. This redirects the PDFTron to use a local font package and prevents it from attempting to download fonts from the internet. Learn how to configure the PDFTron local fonts.
HelpURL	String	URL where the Meridian webhelp (HTML) documentation files are located. This value overrides the **WebHelpBaseURL** setting described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion for PowerWeb only. For information about installing the webhelp documentation files, see Install the Webhelp Documentation.
Icons	String	Full path to a folder containing PowerWeb icons. To be used only in environments where there is no virtual directory for image files (`Img` by default).
Images	String	Name of the folder containing PowerWeb user interface image files (`Img` by default).

Value Name	Data Type	Value Data
MaxItemsInList	DWORD	The maximum number of items that appear when expanding a folder or navigation level. If you click a folder that contains a number of items larger than this pre-configured limit, instead of listing the items, a pane appears with the following options: **Search by name** and **Quick Search**. For navigation views, this feature doesn't consider the selected level. This as a limitation that will be addressed in a future release. If you select a document and the number of incoming or outgoing references is larger than the number for the pre-configured limit, only that number of references appear. In this case, a message appears saying that there are too many references. The reason for these limitations is that showing a large number of items might affect performance. The default value is **3000**. ItemsPerCall is another option to configure the number of items that appear when expanding a folder.
MaxUploadSize	DWORD	The maximum file size allowed to be uploaded in PowerWeb in **megabytes**. If a user attempts to upload a document (individually or as part of a batch) exceeding this size, they will receive a warning. The warning instructs the user to upload the document using the Local Workspace Client. The default value is **500**.
NestingFolderDepth	DWORD	The maximum number of folder levels to process in one batch in PowerWeb before terminating to prevent infinite operations caused by unexpected errors.

Value Name	Data Type	Value Data
NumberOfThreads	DWORD	Number of sessions that can run simultaneously. Default = 10. If PowerWeb performance is slow on a system with many users, it might be because all threads are in use, and user requests must wait until a thread becomes available. If more than 80 users are accessing PowerWeb on a single IIS server and there are slow response times during peak usage, we recommend increasing the **NumberOfThreads** value to one-fifth of the number of users accessing PowerWeb at busy times. For example, if there are 100 users accessing PowerWeb during busy times, we recommend setting the **NumberOfThreads** value to 20 (one-fifth of 100 users).
ProfilesPath	String	Name of the folder containing PowerWeb user preference settings (`Profiles` by default). Users must have read/write permissions to this folder.
QuickFindMultiWordAll	DWORD	If this value is **0** (default), Quick Find searches in PowerWeb will return matches with **any** of the entered keywords. If this value is **1**, Quick Find searches will return matches with **all** of the keywords, the same as PowerUser Quick Find searches.
QuickFindScope	DWORD	Scope of properties searched by the **Quick Search** box in the toolbar in PowerWeb: **0**: Search all text properties (default) **1**: Search all text properties and full-text index **2**: Search the **Name** property only
RefrainFromErrors	DWORD	If this value is set to **1**, some errors will not display during form validation. The default value is **0**.

Value Name	Data Type	Value Data
RemoveLinkAnnotations	DWORD	If this value is **1**, removes any link annotations that were generated in an intermediate (XOD) file that is used by the PDFTron viewer. If this value is **0** (default), the link annotations are left intact and may be followed by users. This value is provided to improve viewing performance of files that contain thousands of hyperlinks that are not expected to be used. This value only has effect when the intermediate files are generated. It has no effect when viewing documents for which XOD files have already been generated that contain link annotations.
ReportDocumentsLimit	DWORD	Sets the maximum number of documents allowed in a report. Setting this limit improves system performance by preventing users from accidentally generating excessively large reports. The default value is **10000**. Set to **0** to remove the limit.
SameIISEDMAccount	DWORD	Set this value to **1** if the site cache server and/or the Meridian application server are installed on a separate computer from the Meridian web server and the IIS application pool under which they run is the same account as the **EDM Server** service. You must also set this value to **1** when using SAML authentication. If the services run under different accounts and are installed on the same computer, set this value to **0**. For more information about authentication issues in distributed service environments, see Security Delegation. The default for this value is set by the installation package depending on the components selected.

Value Name	Data Type	Value Data
SessionTimeOut	DWORD	Number of minutes of inactivity after which a user session is considered inactive and terminated. Default: **15**. The user session is an object that the IIS creates when a user becomes active in PowerWeb. Terminating it when the user becomes inactive conserves resources on the IIS server. If the user still has PowerWeb open and resumes activity, a new session object will automatically be created. The user does not need to re-authenticate when this occurs.
SessionWaitTimeOut	DWORD	Number of milliseconds of inactivity after which a user session is considered inactive, terminated, and a new session created. Default = no timeout. The session will not be terminated. If no timeout is specified, the PowerWeb client might stall for the current user or for all users in certain circumstances. To avoid this, we recommend setting the timeout to 60,000 milliseconds (one minute).
SiteCacheForView	DWORD	If this value is **1** (default), documents are downloaded from the site cache (if configured) to the user's local workspace for viewing. If this value is **0**, documents are downloaded directly from the Meridian server and bypass the site cache.
Sources	String	Name of the folder containing PowerWeb CSS and JavaScript files (`Src` by default).

Value Name	Data Type	Value Data
SynchronizeDirect	String	Semicolon-delimited list of file extensions for which to enable synchronization in PowerWeb. The extensions are as follows: dst; dgn; dwg; doc; docx; docm; xls; xlsx; xlsm; ppt; pptx; pptm; vsdx; vsdm. We recommend you use this setting if you use these file formats so that the results of synchronization will be available immediately. See our Document Synchronization Methods Overview to learn about the three methods you can use to synchronize document contents, title blocks, and references with PowerWeb.
SyncRefs	DWORD	If this value is **1** (default), external references are synchronized according to the options set for the document type. If this value is **0**, external references are not synchronized.
TempPath	String	Name of the folder containing PowerWeb user temporary files (`AMTemp` by default). Users must have read/write permissions to this folder.
ThumbnailCX	DWORD	Size of thumbnail image width in pixels (hexadecimal).
ThumbnailCY	DWORD	Size of thumbnail image height in pixels (hexadecimal).
ThumbnailTimeout	DWORD	Amount of time in milliseconds to wait for thumbnail generation.

Value Name	Data Type	Value Data
UpdateContentPublisher	DWORD	If this value is **1**, use Meridian Enterprise Server publishing jobs to synchronize document properties and references as described in *Configure the Synchronize Content Options* in the *Meridian Enterprise Server Administrator's Guide*. • If the file extension is in the SynchronizeDirect registry value, the update is processed immediately. • If the file extension is NOT in the SynchronizeDirect registry value, the update is sent to the Publisher. • If the extension is NOT in the CADLinkExtenstion registry value, independent of SynchronizeDirect, the update is NOT processed. If this value is **0**, use legacy synchronization. • If the file extension is in the SynchronizeDirect registry value, the update is processed immediately. • If the file extension is NOT in the SynchronizeDirect registry value, the update is NOT processed. • If the extension is NOT in the CADLinkExtenstion registry value, independent of SynchronizeDirect, the update is NOT processed.
URLMapping	String	Name of the PowerWeb virtual directory (URL) for the PowerWeb application.
UsePDFTron	DWORD	If this value is **1**, renditions will be shown in PDFTron for all PowerWeb users. Before a rendition can be viewed in PDFTron for the first time, the rendition must be updated. If set to **0**, the viewer assigned to the PDF file type in the user's preference settings will be used.
UseThumbnailTask	DWORD	When the value is **0** (default),thumbnails are generated by the Meridian web server.

Value Name	Data Type	Value Data
UseNetworkLogon	DWORD	Set to 1 to use the **Network** logon type. This allows you to remove Meridian users from the **Allow Log on Locally** group policy. If the key is missing or set to a value other than 1, Meridian uses the default **Interactive** logon type.
UseViewerWebApp	DWORD	Set to **0** to use the PDFTron 8 viewer in Meridian PowerWeb, which supports functionalities not yet available in Meridian 2025, such as hotspots or compatibility with Microsoft Edge Internet Explorer mode.
WebClient	String	Name of the PowerWeb ISAPI application DLL used by AMXIIS and AMXFilter. Do NOT change.
WebDav	String	Name of the DLL used by IIS to support the WebDav protocol. Do NOT change.
WebServerAddress	String	URL used by AMXIIS and AMXFilter in the form http://<*Computer*>:<*Port*>
XMLValidation	DWORD	If this value is **1**, documents are scanned for invalid XML symbols. If set to **0** (default), documents are not scanned.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\Auth

Registry values

Value Name	Data Type	Value Data
UseOpenIdConnectAuthentication	DWORD	If set to **1**, enables SAML authentication.
PowerWebAppUrl	String	URL used to connect to PowerWeb. This must be the same URL as the one provided to the SAML identity provider, for example, `http://<MyDomain>/meridian`.
TenantId	String	Meridian Portal tenancy name.
IssuerUri	String	URL of the Meridian Cloud authentication server: `https://auth-ci2.meridiancloud.io/auth`.
ClientId	String	Value entered during registration with the SAML identity provider: `mvc.owin.implicit`.
ClientSecret	String	Value entered during registration with the SAML identity provider.
AccessTokenHeaderName	String	Random value comprised of letters, digits, and underscores but no dashes, for example, `AccessToken91ac5084bcc34faa8f27de9080ac2325`.
SubjectHeaderName	String	Random value comprised of letters, digits, and underscores but no dashes, for example, `Subject_91ac5084_bcc3_4faa_8f27_de9080ac2325`.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\LockOnCheckOut

Registry values

Value Name	Data Type	Value Data
LockOnCheckOut	DWORD	• If set to **0**, PowerWeb *will not* download and lock the document upon a workflow state change. This is the default setting. When set to **0**, locking will only happen after a workflow state change if: ◦ the current person is the to-do person for the workflow state and ◦ the workflow state allows editing of the document content. • If set to **1**, PowerWeb *will* download and lock the document upon a workflow state change. If this setting is absent, the system will use the setting from the user's profile.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\Published Locations\<*ID*>

Registry values

Value Name	Data Type	Value Data
CheckCredentials	DWORD	If this value is **1**, explicit user authentication is required to open a vault. If **0** (default), the current Windows account is used and separate authentication is not necessary. This setting corresponds to the **Authenticate logon credentials with the operating system** option described in the *Configure Authentication* article in the *Meridian Enterprise Configuration Guide*.
CollectExisting	DWORD	If this value is **1**, the **Value** list in the **Find** dialog box shows a list of the existing values in the vault for the selected property regardless of how the **Select a value from** option is set for that property in the vault configuration as described in the *Restrict user input* article in the *Meridian Enterprise Configuration Guide*. If **0** (default), no values are listed in the **Find** dialog box. If desired, set this value to **1** if all properties that are likely to be searched have manageable quantities of unique, existing values and the performance of showing the value lists is acceptable. The behavior of the value list on property pages is unchanged and reflects the configuration setting. This affects only PowerWeb, not PowerUser.
CommonWorkspace	String	The lock ID uses the format COMPUTERNAME\USERNAME. This setting specifies the value for COMPUTERNAME if the system cannot determine it automatically, such as in a remote access session.
Name	String	Name specified in Configurator for the published vault context.
Scope	String	Name of a scope to show for the location.

Value Name	Data Type	Value Data
StartPage	String	GUID of a global search query to set as default the default landing page.
Vault	String	Vault context published by PowerWeb for use by Local Workspace.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server for a format string

Registry values

Value Name	Data Type	Value Data
LogTimeStampFormat	String	Allows you to specify that the date in a comment log for a workflow action or other action is shown as the full month name. This registry key is required only on the EDM Server. You must specify a format using wcsftime function format specification. For example: • Default: %d-%b-%y %X (27-Aug-20 7:04:51 PM) • Original: %x %X (08/27/2020 7:04:51 PM)

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\Style Sheets

Registry values

Value Name	Data Type	Value Data
Path	String	Name of the folder containing PowerWeb style sheet files (`Templates` by default). Users must have read permissions to this folder.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian \CurrentVersion\WebLink\UserPreferences\Default

> **Note:**
> Unless otherwise noted, all values in this registry key are the defaults for new users. Values set by a user are stored in the user's profile file described in Configure Default PowerWeb User Settings and override these settings. They correspond directly to the options on the **Preferences** page in PowerWeb shown in the following table.

Registry values

Value Name	Data Type	Value Data	Option
AddRoleAssignmentsInDialog	DWORD	If set to **1**, will show an advanced dialog box for assigning roles to a folder. This dialog is more convenient in environments that have thousands of user accounts in the Meridian Enterprise Server user database and it allows the user to filter the list of groups and users before selecting names to assign to a role. If set to **0**, the advanced dialog box is disabled and the standard dialog box is shown.	Not shown
ColorScheme	String	The name of the custom color scheme in which to show PowerWeb. This setting is only effective if the **UseColorScheme** setting is **1**. For information about creating a custom color scheme, refer to *Create a Custom Color Scheme* in the *Meridian Enterprise Configuration Guide*.	Choose a color scheme to use

Value Name	Data Type	Value Data	Option
Datalist	DWORD	If the value is **1** (default), an alternative drop-down control for lookup lists that provides type-ahead value matching is shown. **0** is disabled.	Not shown
DownloadDocumentWithRefs	DWORD	If this value is **1** (default), when PowerWeb commands download documents to Local Workspace, also download referenced documents. If this value is **0**, do not download referenced documents.	ActiveX compatibility mode
EnableBaselines	DWORD	If this value is **1**, enables viewing the vault at a baseline or specific date or time. If this value is **0** (default), viewing the vault's history is prohibited.	Not shown
EnableCopyPaste	DWORD	If this value is **1**, enable the clipboard Cut, Copy, and Paste command when PowerWeb is used. If this value is **0** (default), the commands are disabled.	Not shown
ForceRelogin	DWORD	If this value is **1** (default), clears the users' log on credentials from the browser cache when they log off of PowerWeb. This prevents the credentials from being reused accidentally or maliciously by other persons to comply with your organization's security policies. This setting is only relevant if the website is configured to use Basic authentication. If this value is **0**, the browser cache is not cleared.	Not shown

Value Name	Data Type	Value Data	Option
ItemsPerCall	DWORD	Number of documents per page. Default = **200**. Valid values can be **1**-**3000**. If you click a folder that contains a number of items larger than this limit, a message will appear asking if you want to continue. MaxItemsInList is another option to configure the number of items that appear when expanding a folder. For information about MaxItemsInList, refer to *HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink* in the *Meridian Enterprise Administrator's Guide*.	**Items per page** option in search results
LockOnCheckout	DWORD	If this value is **1** (default), documents are locked in the user's local workspace after workflow actions that allow the documents to be edited. If this value is **0**, the documents are not locked. This setting can be configured for individual users by adding it to the users' PowerWeb profile file as described in Configure Default PowerWeb User Settings.	Not shown

Value Name	Data Type	Value Data	Option
ProjectsFolderTree	DWORD	Changes the behavior of the **Select Project** dialog box that is shown when a user creates a new project copy of a document. If the value is **1** (default), the user is allowed to navigate a folder tree to select the destination folder. The root folder of the tree can be set using a virtual scope as described in the *VaultEvent_ChangeScope* event section in the *Vault Events* article, and the default destination folder with the *DocCopyMoveEvent_SelectTarget* event in the *Document Copy/Move Events* article of the *Meridian Enterprise VBScript API Reference Guide*. The **Next** button is disabled if the user selects an invalid destination.	Not shown
SelectUserDialogThreshold	DWORD	The number of users at which to show an advanced **Select User** (to-do) dialog box for workflow transitions. The advanced dialog box shows larger name lists, supports list paging, and allows filtering the names. If set to **0**, the advanced dialog is disabled and the standard dialog box is shown. The default is **100**.	Not shown
SiteCache	DWORD	If this value is **1** (default), all PowerWeb sessions will use the site cache that is specified for the **Site Cache URL** option in the user's preferences. If this value is **0**, no site cache will be used.	Site cache mode
TimeZone	String	Default time zone for PowerWeb users. Valid values are the names of the registry keys in `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones`.	Current time zone

Value Name	Data Type	Value Data	Option
UpdateThumbnailOnCheckin	DWORD	If this value is **1**, update thumbnail images when documents are released from under change by PowerWeb. If this value is **0** (default), do not update thumbnails.	Update thumbnails when releasing Quick Change
UpdateThumbnailOnCreate	DWORD	If this value is **1**, create thumbnail images when documents are imported by PowerWeb. If this value is **0** (default), do not create thumbnails.	Create thumbnails on import of document
UseColorScheme	DWORD	If this value is **1**, uses the color scheme specified in **ColorScheme**. For information about creating a custom color scheme, see the *Create a Custom Color Scheme* article in the *Meridian Enterprise Configuration Guide*.	Use custom color scheme
UseDocumentMimeType	DWORD	If this value is **1**, when documents are downloaded to Local Workspace by PowerWeb, open the document immediately using the registered Windows MIME application. If this value is **0** (default), do not open the documents.	**Open it in application** option in the **BlueCielo Upload/Download Control** dialog box
UseHTMLImport	DWORD	When set to **1** (default), enables drag-and-drop document import and an HTML-based **Select Folder** dialog box by the **Import Documents** command to import documents in other than the **Folders** navigation view. When set to **0**, disables drag-and-drop document import and documents are always imported into the root folder of the vault. To set this option for individual PowerWeb users, set the **UseHTMLImport** setting in the users' profiles as described in the *Edit PowerWeb User Profiles* article in the *Meridian Enterprise Configuration Guide*.	Not shown

Value Name	Data Type	Value Data	Option
ViewRenditions	DWORD	If this value is **1**, document renditions are shown by default when comparing documents and when viewing the full screen property window for revisions. If this value is **0** (default), the native document is shown by default when comparing documents and when viewing the full screen property window for revisions.	View renditions
ViewPanel	DWORD	If this value is **1** (default), the view bar is available in PowerWeb. If set to **0**, the view bar is hidden. This setting can be configured for individual users by adding it to the users' PowerWeb profile file as described in Configure Default PowerWeb User Settings.	Not shown

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian \CurrentVersion\WebLink\UserPreferences\Default\Find Templates

For information about configuring the PowerWeb **Find** form page, see the *Configure Searches* article in the *Meridian Enterprise Configuration Guide*.

Registry values

Value Name	Data Type	Value Data
1, 2, 3…	String	ID numbers that specify the properties to show on the PowerWeb **Find** form page.
PropertyCount	DWORD	Quantity of properties to be displayed on the PowerWeb **Find** form page.
1.Operator, 2.Operator, 3.Operator...	DWORD	The default search operator for each property displayed on the PowerWeb **Find** form page. The value is specified as the numeric equivalent of one of the **IC_OP_OPERATOR** constants.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\WelcomeScreen

Registry values

Value Name	Data Type	Value Data
CompanyLogo	String	Logo shown on the PowerWeb **Welcome** page. There is no default image. Place the image in `C:\Inetpub\AMM\Img`.
Greeting	String	Greeting text (256 characters maximum) shown on the PowerWeb **Welcome** page. If not specified, default text is shown.
SupportText	String	Support contact text (256 characters maximum) shown on the PowerWeb **Welcome** page. If not specified, default text is shown.
SupportMail	String	Support contact email address (256 characters maximum) shown on the PowerWeb **Welcome** page. No default is shown.
WelcomeText	String	Welcome text (256 characters maximum) shown on the PowerWeb **Welcome** page. If not specified, default text is shown.

HKEY_LOCAL_MACHINE\Software\Wow6432Node

This branch of the Windows registry supports 32-bit applications running on 64-bit versions of Windows as described in the following Microsoft Support article:

Registry changes in x64-based versions of Windows Server 2003 and in Windows XP Professional x64 Edition

Meridian Enterprise uses this branch for the same purpose. Therefore, any of the registry branches and values in the Software\Cyco branch may also appear in this branch.

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\InetStp\Components

Registry values

Value Name	Data Type	Value Data
ISAPIExtensions	DWORD	Set to **1** if the computer is a web server running a 64-bit version of Windows and 32-bit PowerWeb components are installed.
ISAPIFilter	DWORD	Set to **1** if the computer is a web server running a 64-bit version of Windows and 32-bit PowerWeb components are installed.

Client Registry Keys

The following tables list registry keys that can be found on a Meridian client computer.

HKEY_CURRENT_USER

The following tables list the registry keys of the HKEY_CURRENT_USER hive. These keys affect only the current user of the computer.

HKEY_CURRENT_USER\Software\Cyco\AutoManager View Control2

Registry values

Value Name	Data Type	Value Data
ServerMachine	String	Name of the Meridian server where the viewer control will query for the name of the computer where the Meridian license server is running. The control will then attempt to claim licenses from the license server. **Note:** If this value is not set, the viewer control will look for the server name in the **ServerMachine** value in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager View Control2. If a name is not found, users will be prompted to select the Meridian server computer name when the viewer control cannot find a license server. The user's selection is saved in this value. Custom deployment packages should set the value of ServerMachine in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager View Control2 so that the Meridian server name is available for all users of the client computer.

HKEY_CURRENT_USER\Software\Cyco\AutoManager View Control2\Settings

Registry values

Value Name	Data Type	Value Data
AVLandscape	DWORD	Controls the rotation of watermarks (only when printed in landscape orientation) so that they can match the orientation of the printer driver used. When set to **1**, watermarks are rotated clockwise. When set to **0xFFFFFFFF**, they are rotated counter-clockwise. If this value is missing, the value with the same name in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager View Control2\Settings is used.
ColorAdditions	DWORD	Color number (hex) of added entities when comparing vector documents in the viewer.
ColorDeletions	DWORD	Color number (hex) of deleted entities when comparing vector documents in the viewer.
ColorUnchanged	DWORD	Color number (hex) of unchanged entities when comparing vector documents in the viewer.
EmbedAcrobatIntoIE	DWORD	If this value is **1**, invokes the default system action for URL hyperlinks when viewing PDF documents with the Acrobat viewer. If this value is **0** (default), the hyperlinks may not work as expected.
UseNativeCompareEngine	DWORD	If this value is **0** (default), documents are initially compared using the Accruent viewer.
WriteLog	DWORD	If this value is **1**, enables output to the file specified for **LogFile**. If this value is **0** (default), output is disabled. Because the log file can become very large, we recommend that you only enable this option for troubleshooting.

HKEY_CURRENT_USER\Software\Cyco\AutoManager View Control2\Settings\AVLandscape

Registry values

Value Name	Data Type	Value Data
<*PrinterName*>	DWORD	Controls the rotation of watermarks (only when printed in landscape orientation) so that they can match the orientation of the specified printer driver. When set to **1**, watermarks are rotated clockwise. When set to **0**, they are not rotated. If this value is missing, the value with the same name in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager View Control2\Settings\AVLandscape will be used. If both settings are missing, the **AVLandscape** value in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager View Control2\Settings will be used.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion

Registry values

Value Name	Data Type	Value Data
Language	String	Locale code of the language to show in the Meridian Enterprise client applications. This also affects how dates are shown. Overriden by the default **Language** value in `HKEY_LOCAL_MACHINE\Software\Cyco\Meridian Enterprise\CurrentVersion`. For more information about switching languages, see Install Second Language Support.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Administrator

Registry values

Value Name	Data Type	Value Data
LastComputer<*n*>	String	Numbered list of most recently accessed server computer names
LastDatastore<*n*>	String	Numbered list of most recently accessed datastore names
LastVault<*n*>	String	Numbered list of most recently accessed vault internal names
LastVaultDisplayName<*n*>	String	Numbered list of most recently accessed vault display names

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMDocUpdateUtl\Settings

Registry values

Value Name	Data Type	Value Data
CheckBlankPropertiesAssigned	DWORD	If set to **1** (default): All Meridian client links check empty mapped property values to determine if the value was set that way (Empty) or if they have never been set (Null). If a property was set to Empty, the link empties the corresponding document property. If set to **2** or greater: The links force all mapped document properties to empty regardless of whether the file properties are Empty or Null. If set to **0**: The check is not performed. The companion to this setting is HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMLink\Settings, which controls value checking in the application links within third-party applications. Also see the description of the **CheckBlankPropertiesAssigned** setting in the *Configure Empty Property Synchronization* article in the *Meridian Enterprise Configuration Guide* .

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMDownload

Registry values

Value Name	Data Type	Value Data
AskBeforeDownload	DWORD	If this value is **1**, prompt before downloading documents when they are placed under change from PowerWeb. If this value is **0**, do not prompt. Configured on the **Preferences** page of a PowerWeb session.
DownloadLocation	String	Path to a folder for downloading documents from PowerWeb. Vault folder structure subfolders will be created at this location. Configured on the **Preferences** page of a PowerWeb session.
OpenFolder	DWORD	If this value is **1**, open a downloaded document's parent folder in Windows Explorer after download has completed. If this value is **0**, do not open the folder. Configured on the **Preferences** page of a PowerWeb session.
OpenInApplication	DWORD	If this value is **1**, after a download has completed, open the downloaded document in the application registered in Windows for the downloaded file's extension. If this value is **0**, do not open the document. Configured on the **Preferences** page of a PowerWeb session.
UseLocalWS	DWORD	If this value is **1**, use the Local Workspace folder as the default download folder. If this value is **0**, do not use as the default folder. Configured on the **Preferences** page of a PowerWeb session.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMEdmUI

Registry values

Value Name	Data Type	Value Data
SavedCriteria	DWORD	The last used search criteria. See also KeepSearchSettings. The full set of search criteria is stored for every vault.
ReportsAddToExisting	DWORD	If this value is **1**, add new report data to existing files. If this value is **0**, do not add to existing files. Configured in the **Report** dialog of PowerUser at report build time.
ReportsFolder	String	Path of the default report destination folder. Configured in the **Report** dialog of PowerUser at report build time.
ReportsOpenWhenDone	DWORD	If this value is **1**, when a report has completed, open it in the application registered in Windows for the report file's extension. Configured in the **Report** dialog of PowerUser at report build time.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMEdmUI\Settings

Registry values

Value Name	Data Type	Value Data
DoNotCreateDDDSubfolders	DWORD	If this value is **1**, forces Duplicator to not create separate subfolders in the default destination folder for every **Copy with references** or **Derive with references** action. If this value is **0** (default), creates subfolders.
ProgressX	DWORD	Default screen coordinate **X** value of the **Progress** dialog.
ProgressY	DWORD	Default screen coordinate **Y** value of the **Progress** dialog.
Splitter_<*n*>	DWORD	Comma-separated list of numbers that define the last location and display of Meridian client application splitter bars.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMFind\Settings

Registry values

Value Name	Data Type	Value Data
DefaultStringOp	DWORD	One of the following numbers: 1 Equals 2 Less than 3 More than 4 Less or equal to 5 More or equal to 6 Not equal to 9 Is empty 10 Is not empty 11 Contains 12 Does not contain 13 Starts with 14 Does not start with 15 As DOS wildcard If the value is missing or invalid, the default condition Contains (11) is used.
InternalPropertiesAssign	DWORD	If this value is **0** (default), system properties are not included in the property lists that are shown on the **Property Assignments** pages of workflow states and transitions. If this value is **1**, the system properties are included. This value can be modified in the user interface by enabling the **Show system properties** option on the configuration pages.
KeepSearchSettings	DWORD	If this value is **1** (default), the **Find** dialog stores the last used search settings and reloads them when it is run the next time. If this value is **0**, settings are not saved.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHook\Contexts

Registry values

Value Name	Data Type	Value Data
DataStoreName	String	Default datastore name without any slashes or backslashes
DateTimeUTC	Binary	Date and time
MachineName	String	Default Meridian application server computer name without any slashes or backslashes
SectionAddress	String	Default datastore section UNC name
VaultName	String	Default vault name without any slashes or backslashes

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHook\Contexts\<*executable*>

Registry values

Value Name	Data Type	Value Data
DataStoreName	String	Default datastore name last opened by <*executable*>
DateTimeUTC	Binary	Date and time
MachineName	String	Default Meridian application server computer name last opened by <*executable*>
Object	String	Default document object ID last opened by <*executable*>
SectionAddress	String	Default datastore section URL last opened by <*executable*>
VaultName	String	Default vault name last opened by <*executable*>

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHook\Contexts\<*executable*>\Dialog Detect

Registry values

Value Name	Data Type	Value Data
<dialogname>	DWORD	See the *Reset Application Integration Dialog Boxes* article in the *Meridian Enterprise User's Guide*.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHook\Contexts\<*executable*>\Last View

Registry values

Value Name	Data Type	Value Data
(default)	String	Internal ID of the last Navigation view used with Application Integration
Last Navigation View	String	Name of the last Navigation view used with Application Integration

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHook\Contexts\<*executable*>\Quick Find

Registry values

Value Name	Data Type	Value Data
ComboBoxValue<*n*>	String	Search value last typed by the user in the search field represented by ComboBoxValue<*n*>of the **Quick Find** dialog within Application Integration.
LastOperator	DWORD	Number corresponding to the search operator last selected by the user in the **Quick Find** dialog within Application Integration.
QuickFindProperty	String	Internal and display name of the property last selected by the user in the **Quick Find** dialog within Application Integration.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHookTray\ForceList\<*executable*>

Registry values

Value Name	Data Type	Value Data
Path	String	Path of an executable to force to use Meridian Application Integration **Note:** • The corresponding key with the same name in HKEY_LOCAL_MACHINE is checked first and, if not set, this value is checked. This value is set by the Application Integration **Show Accruent Dialog For** dialog box. The HKEY_LOCAL_MACHINE value is not set by the **Show Accruent Dialog For** dialog box but can be set by a System Administrator and is retained for backward compatibility with previous versions. • If there are multiple versions of the same program installed on the PC, they will all be included regardless of their paths.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHookTray\RejectList\<*executable*>

Registry values

Value Name	Data Type	Value Data
Path	String	Path of an executable to exclude from Meridian Application Integration **Note:** • The corresponding key with the same name in HKEY_LOCAL_MACHINE is checked first and, if not set, this value is checked. This value is set by the Application Integration **Edit Exclusion List** dialog box. The HKEY_LOCAL_MACHINE value is not set by the **Edit Exclusion List** dialog box but can be set by a System Administrator and is retained for backward compatibility with previous versions. • If there are multiple versions of the same program installed on the PC, they will all be excluded regardless of their paths.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHookTray\Settings

Registry values

Value Name	Data Type	Value Data
Off	DWORD	If this value is **1**, disables Application Integration. If this value is **0**, enables Application Integration (default). Configured on the Application Integration shortcut menu, as described in the *Application Integration Options* article in the *Meridian Enterprise User's Guide*.
RunOnStartup	DWORD	If this value is **1**, runs Application Integration on Windows startup (default). If this value is **0**, does not run Application Integration. Configured on the Application Integration shortcut menu, as described in the *Application Integration Options* article in the *Meridian Enterprise User's Guide*.
ShowBalloonOnStart	DWORD	If this value is **1** (default), show balloon tooltip on startup. If this value is **0**, do not show the tooltip.
UseDefaultBrowser	DWORD	If this value is **1**, use Application Integration as the default file browser. If this value is **0**, use the standard file dialog (default). Configured on the Application Integration shortcut menu, as described in the *Application Integration Options* article in the *Meridian Enterprise User's Guide*.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMLink\Settings

Registry values

Value Name	Data Type	Value Data
CheckBlankPropertiesAssigned	DWORD	If set to **1** (default), all application links check empty mapped property values to determine if the value was set that way (Empty) or if they have never been set (Null). If a property was set to Empty, the link empties the corresponding document property. If set to **2** or greater, the links force all mapped document properties to empty regardless of whether the file properties are Empty or Null. If set to **0**, the check is not performed. **Note:** The companion to this setting is HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMDocUpdateUtl\Settings, which controls value checking in the application links within the Meridian applications. Also see the description of the **CheckBlankPropertiesAssigned** setting in the *Configure Empty Property Synchronization* article in the *Meridian Enterprise Configuration Guide* .
EnableRemoteDocumentCache	DWORD	If set to **1**, additional caching of documents is done to improve the performance of the application links with large assemblies when PowerWeb is used in Remote mode with a site cache. If set to **0**, additional caching of documents in remote mode is not performed. This setting applies only to the current user and if missing, the value with the same name is applied if it exists in the HKEY_LOCAL_MACHINE hive, which applies to all users of the same PC.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMOfficeAddIn

Registry values

Value Name	Data Type	Value Data
TempFolder	String	The path to an existing folder to use for temporary files created by the Office application link. This setting is intended for use when the path to the Windows temporary folder is too long and results in odd behavior of the link. By default, the link uses the path that is stored in the Windows environment variable %TEMP%.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMOfficeAddIn\Excel

Registry values

Value Name	Data Type	Value Data
EnableToolbar	DWORD	If this value is **1**, display the Meridian toolbar in Microsoft Excel. If this value is **0**, do not display the toolbar.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian \CurrentVersion\AMOfficeAddIn\PowerPoint

Registry values

Value Name	Data Type	Value Data
EnableToolbar	DWORD	If this value is **1**, display the Meridian toolbar in Microsoft PowerPoint. If this value is **0**, do not display the toolbar.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMOfficeAddIn\Word

Registry values

Value Name	Data Type	Value Data
EnableToolbar	DWORD	If this value is **1**, display the Meridian toolbar in Microsoft Word. If this value is **0**, do not display the toolbar. **Note:** Besides setting this value to **0** to hide the toolbar, you must manually remove the toolbar from the ribbon in the Word, which stores it in the template `Normal.dot`. You must also remove the toolbar if the Office application link is uninstalled.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMPersistEnv\Settings

Registry values

Value Name	Data Type	Value Data
DataVersion	DWORD	Version number of vault configuration data to export from Configurator for import into other vaults.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AmSldWorksEx\Settings

Registry values

Value Name	Data Type	Value Data
CacheLockOnOpen	DWORD	If this value is **>0**, forces the link to set cache lock on every document in an assembly that is currently under change by the user. If this value is **0**, does not set cache lock.
EnableBrowseDocSync	DWORD	If this value is **1**, synchronize Meridian Browser page tree item with the open document. If this value is **0**, disable synchronization.
EnableBrowseVaultSync	DWORD	If this value is **1**, synchronize Meridian Browser page vault context with the open document. If this value is **0**, disable synchronization.
EnableBrowsePage	DWORD	If this value is **1**, enable Meridian Browser page. If this value is **0**, disable page.
EnableBrowsePageTips	DWORD	If this value is **1**, enable Meridian Browser page tips. If this value is **0**, disable page tips.
EnablePRBaseToFileOnOpen	DWORD	If this value is **1**, enable property synchronization from vault when opening document. If this value is **0**, disable synchronization.
EnablePRFileToBaseOnSave	DWORD	If this value is **1**, enable property synchronization to vault when saving document. If this value is **0**, disable synchronization.
EnableReplacementsScan	DWORD	If this value is **1**, enable scanning for replaced parts when opening document. If this value is **0**, disable scanning.
ReadOnlyReferences	DWORD	If this value is **1**, forces the **Don't prompt to save read-only referenced documents (discard changes)** setting in the SolidWorks **System Options** dialog to enabled. If this value is **0**, the SolidWorks setting is unaffected.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMStationEx\Settings

Registry values

Value Name	Data Type	Value Data
DoNotCreateMStationTagsets	DWORD	If this value is **0** (default), enable import of new tag definitions during property synchronization from file. If this value is **1**, disable synchronization. See the *Tag Synchronizer Tool* article in the *Meridian Enterprise Configuration Guide*.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMSync\Settings

Registry values

Value Name	Data Type	Value Data
CacheSize	DWORD	Maximum amount of disk space in MB reserved for local workspace. Default is **750**. If omitted, 10% of free disk space is used but not less than the default. Configured in **Local Workspace Options** dialog, as described in the *Configure Local Workspace* article in the *Meridian Enterprise User's Guide*.
ForceClean	DWORD	If this value is **1**, all Read-Only local workspace files are cleaned irrespective of the **CacheSize** setting and the last file access time.
LastSync	Binary	Data specifying the date and time the local workspace was last synchronized.
RecentOnly	DWORD	If this value is **1**, synchronize only recently accessed writable documents. Configured in **Local Workspace Options** dialog, as described in the *Configure Local Workspace* article in the *Meridian Enterprise User's Guide*.
SyncEnabled	DWORD	If this value is **0**, disables periodic synchronization of local workspace. If this value is **1**, enables synchronization. Configured in **Local Workspace Options** dialog, as described in the *Configure Local Workspace* article in the *Meridian Enterprise User's Guide*.
SyncInOffline	DWORD	If this value is **1**, synchronize in offline mode. If this value is **0** (default), do not synchronize in offline mode.
SyncTime	DWORD	Interval in minutes between local workspace synchronizations. Configured in **Local Workspace Options** dialog, as described in the *Configure Local Workspace* article in the *Meridian Enterprise User's Guide*.

Value Name	Data Type	Value Data
TraceMask	DWORD	Number representing the current selected local workspace log trace mask levels: 1 Success 2 Information 4 Warnings 8 Errors Configured in local workspace log dialog.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMVault\Most Recent Opened Vaults

Registry values

Value Name	Data Type	Value Data
Vault <*n*>	String	Numbered list of most recently opened vaults in the form <*vault*>\\<*machine*>\<*datastore*>\<*section*>

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AMWFMTUI\Init

Registry values

Value Name	Data Type	Value Data
ImportState	DWORD	
Last configuration <*n*>	String	Numbered list of most recently opened **Database Import Wizard** configuration files

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\<*application*>\Layout\BarLayout-ToolBarManager

Registry values

Value Name	Data Type	Value Data
CoolLook	DWORD	If this value is **1** (default), enable “cool look” of the toolbar. If this value is **0**, clear the look.
LargeButtons	DWORD	If this value is **1**, enable large buttons in the toolbar. If **0** (default), use small buttons.
ToolTips	DWORD	If this value is **1** (default), enable tooltips. If this value is **0**, disable tooltips.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\<*application*>\Most Recent Opened Vaults

Registry values

Value Name	Data Type	Value Data
Vault <*n*>	String	Numbered list of most recently opened vaults

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\<*application*>\Most Recent Opened Workareas

Registry values

Value Name	Data Type	Value Data
Workarea <*n*>	String	Numbered list of most recently opened work areas (obsolete)

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\<*application*>\Settings

Registry values

Value Name	Data Type	Value Data
ActionOnThumbDblClk	DWORD	Action to take when the user double-clicks the thumbnail. Only PowerUser. **0**: Do nothing **1**: Open document in associated application **2**: Show viewer full-screen **3**: Turn viewer on/off (default) **4**: Regenerate thumbnail
ActionOnViewerDblClk	DWORD	Action to take when the user double-clicks the viewer window. Only PowerUser. **0**: Do nothing **1**: Open document in associated application **2**: Show viewer full-screen (default)
dbgDisableAutoRefresh	DWORD	If this value is **1** (default), disables some additional automatic refreshing of property pages. It is the opposite value of the **Automatically refresh property pages** option. Not applicable to Office client.
EnableGlobalSearchWithScopes	DWORD	If this value is **1**, the **All vaults** options are available in **Quick Find** and in the **Find** dialog when a scope is active. If this value is **0** (default), the options are hidden. If this setting is enabled, users may find documents that are not visible to them in certain scopes.
FindLastObjectOnOpen	DWORD	If this value is **1**, upon opening a vault, navigate to the last selected document. If this value is **0**, do not navigate. **1** for PowerUser, **0** for Office client.

Value Name	Data Type	Value Data
FindLastObjectOnView	DWORD	If this value is **1**, upon changing views, navigate to the last selected document. If this value is **0**, do not navigate. **0** for PowerUser, **1** for Office client.
FullRowMenuBar	DWORD	If this value is **0**, the toolbars share space with the menu bar. If this value is **1** (default), toolbars occupy the whole bar. Not applicable to Office client.
HeaderFont	DWORD	Font for header names in the Navigation view in the form <*name*>;<*size*>;<*attr*> like: Microsoft Sans Serif;-12;3264 Negative size means points. Attributes include: **1**: Bold **2**: Italic **8**: Underline **16**: Strikeout Character set multiplied by 16. Not applicable to Office client.
HideKnownExtensions	DWORD	If this value is **0** (default), do not hide file extensions for registered file types. If this value is **1**, hide file extensions.
InstantView	DWORD	If this value is **1** (default), the viewer pane immediately displays the selected document. If this value is **0**, the user must click the **Refresh** button. Not applicable to Office client.
ItemsPerCall	DWORD	Maximum number (default = 200) of documents for which to retrieve information in one call. Valid values can be 1–3000.
ItemsPerTransaction	DWORD	Maximum number (default = 30) of documents to batch process in one transaction. Valid values can be 1–100000.

Value Name	Data Type	Value Data
KeepClipboardData	DWORD	If this value is **1**, prevents flushing clipboard data upon switching to another vault. If this value is **0** (default), flushes the data.
KeyFindProperty	DWORD	Internal and display names of the property last used for **Quick Find**. For example, _DISPLAYNAME|Name.
LabelFont	DWORD	Font for document and folder names in the Navigation view in the form <*name*>;<*size*>;<*attr*> like: Microsoft Sans Serif;-12;3264 Negative size means points. Attributes include: **1**: Bold **2**: Italic **8**: Underline **16**: Strikeout Character set multiplied by 16 Not applicable to Office client.
LastObjectID	DWORD	String representing GUID of the last selected document, for example, {84743CE0-E232-11D9-0000-9BE8AF3C9914}.
LastOpenedVault	String	Name of the last opened vault in the form **/Amfs="M-<*ComputerName*>,D-<*VaultName*>"**. This vault will be reopened on next start of the application if the Shift key is not pressed.
LinesBetweenItems	DWORD	If this value is **0** (default), disable lines between documents in the Navigation view. If this value is **1**, enable lines.
LoadDataOnDemand	DWORD	If a positive number and the number of rows in a tableview exceeds the number, data is retrieved when needed. If this value is **0**, data is retrieved immediately. If this value is a negative number, then load on demand is cleared and number specifies the threshold. Not applicable to Office client. Default = **0xfffffc18 (-1000)**.

Value Name	Data Type	Value Data
MainViewSplitHorizontal	DWORD	If this value is **0** (default), the main view is split in such a way that navigation is on the left, and properties on the right. If this value is **1**, the main view is split in such a way that navigation is on the top, and properties on the bottom.
MainViewSplitterPosition	DWORD	Percentage (multiplied by 10) of space that the navigation view takes of the window. Default is **500** (50%).
MaxDoc2Show	DWORD	Maximum number (default = 1000) of documents per folder. If the number of documents exceeds this number, a warning message will be shown. Not used if set to zero or negative.
<*machine*>_<*vault*>_Opened	DWORD	Counter of how many times this vault has been opened in order to show or not to show proper nag screen.
PropDocSplitterPosition	DWORD	Percentage (multiplied by 10) of space that the properties pane takes of the window. Default is **500** (50%).
QuickSearchList	Binary	History of quick searches.
QuickSearchOperator	DWORD	Index number of the last used search condition.
RedlinesEnabled	DWORD	If this value is **1** (default), enables redlines in the viewer pane. If this value is **0**, disables redlines. Doesn't disable redlining in a full-screen viewer. Not applicable to Office client.
ResumeDelay	DWORD	Delay in milliseconds that will be used to resume the viewer. Default = 0x3e8 (1000) (1 second). Not applicable to Office client.
ShowDoc	DWORD	If this value is **0**, disables the viewer pane. If this value is **1** (default), display the viewer pane.
ShowProp	DWORD	If this value is **0**, disables the properties pane. If this value is **1** (default), display the properties pane. Not applicable to Office client.

Value Name	Data Type	Value Data
ShowMenuBar	DWORD	If this value is **0**, disables the menu bar. If this value is **1** (default), displays the menu bar. Not applicable to Office client.
ShowMgrToolBar	DWORD	If this value is **0** (default), disables the Manager tool bar. If this value is **1**, displays the **Manager** tool bar. Not applicable to Office client.
ShowStatusBar	DWORD	If this value is **0**, disables the status bar. If this value is **1** (default), displays the status bar. Not applicable to Office client.
ShowSwitchBar	DWORD	If this value is **0** (default), disables the switch bar. If this value is **1**, displays the switch bar. Not applicable to Office client.
ShowToolBar	DWORD	If this value is **0**, disables the tool bar. If this value is **1** (default), displays the tool bar. Not applicable to Office client.
ShowUserInitials	DWORD	If this value is **0** (default), displays the user's full name in the status bar. If this value is **1**, display the user's initials in the status bar if they are set in the user info.
UpdateSelectedItem	DWORD	If this value is **0** (default), disables refresh of the viewer pane every time a document is selected. If this value is **1**, the viewer pane is refreshed. Not applicable to Office client.
UseSuspendResume	DWORD	If this value is **1** (default), force the viewer to close the document when the application becomes inactive, and reopen it again when the application is activated. If this value is **0**, do not close the viewer. Not applicable to Office client.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\<*application*>\Settings\Assistant

Registry values

Value Name	Data Type	Value Data
AutoHide	DWORD	If this value is **1** (default), automatically hide the Help assistant after the specified amount of time. If this value is **0**, do not hide the assistant.
AutoHideDelay	DWORD	Time in seconds after which the Help assistant will be hidden. Default = **15** seconds. Not applicable to Office client.
BackgroundColor	DWORD	Color (default = 0x00ffffc0) of Help assistant notes. Not applicable to Office client.
Counter<*ID*>	DWORD	Number of times the Help assistant screen identified by <*ID*> has appeared. Not applicable to Office client.
CounterValue	DWORD	Maximum number of times each of the Help assistant screens should appear. Default = **3**. Not applicable to Office client.
Enabled	DWORD	If this value is **1** (default), enable the Help assistant. If this value is **0**, clear the assistant. Not applicable to Office client.

Value Name	Data Type	Value Data
Font	DWORD	Font for Help assistant notes in the form <*name*>;<*size*>;<*attr*> like: Microsoft Sans Serif;-12;3264 Negative size means points. Attributes include: 1 Bold 2 Italic 8 Underline 16 Strikeout Character set multiplied by 16 Not applicable to Office client.
UseCounters	DWORD	If this value is **1** (default), limit the number of times each of the Help assistant screens appear. Not applicable to Office client.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\<*application*>\Settings\Columns\<*GUID*>

Registry values

Value Name	Data Type	Value Data
<*InternalPropertyName*>	DWORD	Width of the column containing this property

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\<*application*>\Settings\<*MachineName_VaultName*>\Commands

Registry values

Value Name	Data Type	Value Data
Cmd<*group*>_<*ID*>	DWORD	Sum of bit flags for the command item. <*group*> can be: 0 Document 1 Folder 2 Vault 3 Work area (obsolete)

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AssetManagement

Registry values

Value Name	Data Type	Value Data
ItemsToFind	DWORD	The maximum number of items to show in query results by the Meridian Asset Management Module. The value must be >= 10. If this value is missing the value with the same name in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AssetManagement is used. In PowerWeb, if this value is **0**, all items are shown. If the value is absent, the default is **250** items.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AutocadLink

Registry values

Value Name	Data Type	Value Data
AcadBaseConfig[1]	DWORD	Controls the basic functionality provided by the AutoCAD link: **0**: Basic AutoCAD link features only **1**: Basic AutoCAD link features plus sheet set support (default) **2**: Basic AutoCAD link features plus plain drawing asset management support (not for use with AutoCAD P&ID or AutoCAD Plant 3D) **3**: Enable all AutoCAD link features **32**: Enable the **Synchronize All Data Shortcuts to Vault** command in the AutoCAD Civil 3D application link.
AcadPnIDConfig[1]	DWORD	Controls the P&ID functionality provided by the AutoCAD link. This settings requires AutoCAD P&ID or AutoCAD Plant 3D. **0**: P&ID project features only (default) **1**: P&ID project features plus asset management support
ButtonsForAll	DWORD	If set to **1**, shows **OK to All** and **Cancel to All** buttons in the confirmation dialog box that appears when a user invokes the **Sync Tag Hotspot** command on a selection of documents and one or more of the documents has circular references. By default, the dialog box will appear once for every document in the selection that has circular references so that the user can decide what to do with each document. This setting allows the user to apply their response to all of the problem documents in the selection at one time. The default is **0**, which does not show the batch response buttons.

Value Name	Data Type	Value Data
Civil3DHideWCDialog[1,2]	DWORD	If set to **1**, the user is not prompted to select specific data shortcuts from which to create working copies when the **Edit data shortcuts** command is run. Working copies of all data shortcuts are made automatically. The default is **0**.
Civil3DSyncType[1,2]	DWORD	Controls the synchronization of the folder specified for **Civil3DSyncWorkingFolder**: **1**: Synchronize to the local working folder (on drawing open) **2**: Synchronize to the vault (on drawing close) **4**: Ask the user before synchronization **8**: Synchronize only once per AutoCAD session If this value is missing from either registry key mentioned in the note at the beginning of this topic, then the setting with the same name on the **AutoCAD** tab of the **Application Link Settings** in the **Environment** branch of the vault configuration is applied.
Civil3DSyncWorkingFolder[1,2]	DWORD	If this value is **1**, synchronizes the entire folder that is specified as the working folder in AutoCAD Civil 3D. If this value is **0** (default), only the data shortcuts folder is synchronized. • Automatic synchronization is disabled when AutoCAD Civil 3D is run by Publisher. • If this value is missing from either registry key mentioned in the note at the beginning, then the setting with the same name on the **AutoCAD** tab of the **Application Link Settings** in the **Environment** branch of the vault configuration is applied.

Value Name	Data Type	Value Data
ManualUpload	DWORD	This setting allows you to opt out of automatic uploads of AutoCAD documents. **0**: Setting is disabled. **1**: Automatic upload is disabled. A new **Upload Document** button is added to the Meridian ribbon. This button is visible in remote mode only, and is enabled after the first save of the document. **2**: Ignored. **3**: Automatic upload is enabled on document close only. A new **Upload Document** button is added to the Meridian ribbon. This button is visible in remote mode only, and is enabled after the first save of the document.
RealDwgForceValidity[1]	DWORD	If this value is **1** (default), the **Sync Properties to File** command works with AutoCAD Release 14 and older drawings but importing drawings can fail if the title blocks are synchronized also. If this value is **0**, the command does not work with older drawings but importing drawings will not fail if the title blocks are synchronized.
ReleaseNewCivil3DDataShortcuts[1,2]	DWORD	If this value is **1**, Civil 3D data shortcuts are automatically released from their workflows when they are imported to the vault by working folder synchronization. If this value is **0** (default), the shortcuts are not automatically released.
RepairDocState	DWORD	If this value is **1**, it fixes an issue with drawings being read-only and cannot be saved when opened from PowerWeb in Online mode with a site cache configured. The default value is **0**.

1. The following locations will be searched for this value in the order listed and the value of the first location where it is found will be applied:
    a. HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AutocadLink (affects all users of the PC)
    b. This registry key (affects only the current user of the PC (affects all users of the PC).

2. In addition to the locations listed above, the **[Civil_3D]** section on the **AutoCAD** tab of the **Application Link Settings** in the **Environment** branch of the vault configuration (affects all users of the vault).

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian \CurrentVersion\BCSharedFolderSync\Settings\Log

Registry values

Value Name	Data Type	Value Data
File	String	The fully qualified path and filename of the log file.
MaxSize	DWORD	The maximum size in KB to maintain the log. The default is 1 MB. Data is overwritten on a first in, first out basis upon each launch of `BCSharedFolderSync.exe`.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\CCL\Settings

Registry values

Value Name	Data Type	Value Data
VisualStyles	DWORD	This value is **0** if the operating system does not support visual themes, otherwise 11 (0x0000000b). Set to **0** to clear the use of Enhanced visual mode.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Client

Registry values

Value Name	Data Type	Value Data
Features	String	Set this value to **0000000000000080** to enable the Meridian client applications to download documents from a local site cache in a WAN environment.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\Currentversion\Client\Bcsitecacheauth

The values in this key are read and, if not present, the values with the same name in HKEY_LOCAL_MACHINE are checked.

Registry values

Value Name	Data Type	Value Data
M360Tenant	String	Name of the Meridian Portal tenancy where the OpenId authentication credentials are specified.
IssuerUri	String	URI of the OpenId authority.
UseOpenIdConnectAuthentication	DWORD	If this value is **1**, connect this PC to the site cache server using the OpenId authentication credentials specified in the configuration of the tenant in **M360Tenant**. If this value is **0** (default), connect to the site cache server via the logged on Windows account.
UseWorkspace	DWORD	If this value is **0** (default), temporary copies of documents are downloaded from the site cache to the user's normal local workspace just as if they were working in a vault in their own domain. Typically, the path of the local workspace contains the user's Windows account name. If this value is **1**, places the temporary copies in a separate local workspace path that contains the name of the account used by the OpenId authentication credentials.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Client\Settings

Registry values

Value Name	Data Type	Value Data
AssetManagementUseAdditionalFiltering	DWORD	If this value is **1**, retired and inactive project copies are hidden in the **Manage Tag Links** dialog box of the Meridian Asset Management Module.
AutoExpandOnDrag	DWORD	If this value is **1**, causes folders to automatically expand when a document is dragged over them. If this value is **0** (default), the folders do not automatically expand.
BCSiteCacheURL	String	URL of the site cache server for use by PowerWeb. This setting overrides the same setting in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client for the current user. **Important!** Users should not work on the same documents from more than one PC with Application Integration in Remote mode and site caches enabled or document content inconsistencies can occur.
BriefCaseCache	DWORD	Location of temporary folder for external format briefcases. If this value is not set (default), uses default temporary directory (%TEMP% environment variable).
BriefCaseOpenFormat	String	Default briefcase metadata format created on 32-bit computers. The default is XML (always on 64-bit computers). Set this value to **.mdb** to store the metadata in Access format.

Value Name	Data Type	Value Data
ClientServerWebView	DWORD	If this value is **0**, the client applications use the locally installed viewers.
ContextHelpEnabled	DWORD	If this value is **1**, enables the context-sensitive Help in client applications. If this value is **0** (default), context-sensitive Help is cleared.
CopyFiles	DWORD	If this value is **1** (default), enables Duplicator's **Copy drawings and presentation documents** option. See *Duplicate References* in the *Meridian Enterprise User's Guide*.
CreateThumbnailOn	DWORD	Sum of bit flags indicating when to update thumbnails. 1 On import 2 On submit working copy 4 On change workflow state
dbgEnableScriptDebugger	DWORD	If this value is **0**, do not display the Script Debugger item on the **Tools** menu of PowerUser. If this value is **1**, show the Script Debugger item if a script debugger is installed. Configured in the **PowerUser Options** dialog. See *Advanced Options* in the *Meridian Enterprise User's Guide*.
DebugMode	DWORD	Sum of bit flags that specify debug levels. For internal use only.
DisableMenuWF	DWORD	If this value is **1**, disables the **Workflow** menu in PowerUser. If this value is **0** (default), enables the menu.

Value Name	Data Type	Value Data
DisableNotFoundMessage	DWORD	If this value is **1**, an information message is not shown when a user attempts to navigate to a document that is outside of the scope of the current navigation view. The view is automatically set to the **Explorer** view. If this value is **0** (default), the message is shown and the user must dismiss the dialog box before the view is changed.
DisableOfflineSwitch	DWORD	If this value is **1**, disable Offline mode switch in Application Integration. If this value is **0** (default), do not disable Offline mode. See Disable Offline Mode. This value overrides the value with the same name in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client.
DisableVaultShortcuts	DWORD	If this value is **0** (default), the **Create Shortcut to This Vault** command is enabled. If this value is **1**, the command is cleared for the current user. This setting must be **0** for the command to be enabled if a scope is active and the command is enabled for that scope.
DisplayManualReferences	DWORD	If this value is **1** (default), enables inclusion of manual references in **Assembly structure** and **Where used** dialogs. See *Reference Explorer* in the *Meridian Enterprise User's Guide*.
DisplayValidationAlerts	DWORD	If this value is **1**, show a warning when opening a document in a read-only workflow state. If this value is **0**, do not show a warning.
DoNotSyncLWS4ShellMenu	DWORD	If this value is **1**, the Local Workspace copy of the selected document will not be synchronized before retrieving related shell menu items. If this value is **0** (default), the document is synchronized.

Value Name	Data Type	Value Data
FlagsFor64bitExtensions	DWORD	Controls the loading of custom extensions by 64-bit client applications. If this value is **0**, do not restrict extension loading. If this value is **1**, do not load extensions. If this value is **2** (default), load extensions.
GrayTextColor	DWORD	If non-zero, Windows text color is used instead of standard (gray) color for cleared controls. On closing of PowerUser, this value is set back for dimmed controls. Default is **0**. **Important!** If this is set to anything but **0x808080**, can affect other applications after PowerUser is closed.
HighlightRecentDocs	DWORD	If this value is **1**, highlight documents that are less than RecentDocsDateSpan days old. If this value is **0** (default), do not highlight.
IncludeIntermediate	DWORD	If this value is **1** (default), enables the assembly duplicator's **Include connecting assemblies** option in the **Assembly Copy Options** dialog box. See *Duplicate References* in the *Meridian Enterprise User's Guide*.
LastReleasedColor	DWORD	Color to display last released document names in the **Show Revisions** dialog box.
OfflineMode	DWORD	If this value is **1**, use PowerWeb in offline mode. If this value is **0**, do not use offline mode. This can also be set on the Application Integration shortcut menu. For use with remote access software, set this value to **1** on the remote access client PC and to **0** on the remote access host PC. This value overrides the value with the same name in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client.

Value Name	Data Type	Value Data
QuickSearchAutoAppend	DWORD	If this value is **1** (default), enables the AutoComplete feature in **Quick Find** combo boxes. If this value is **0**, the feature is cleared.
RebuildDirectoryStructure	DWORD	If this value is **1**, sets the assembly duplicator's **Folder structure** option in the **Assembly Copy Options** dialog box to **Rebuild folder structure relative to each subassembly**. If this value is **0** (default), sets it to **Rebuild folder structure relative to the main assembly**. See *Duplicate References* in the *Meridian Enterprise User's Guide*.
RecentDocsDateSpan	DWORD	Age of documents in days to highlight. If this value is **0** (default), do not highlight.
RedlinesWidth	DWORD	Width in pixels to display Meridian redlines in the Meridian viewer. Configured in the **PowerUser Options** dialog. See *Appearance Options* in the *Meridian Enterprise User's Guide*.
ReleaseAllAssembly	DWORD	If this value is **0**, release only the documents that are parts of a CAD assembly. If this value is **1**, release the assembly documents and all other documents that are related by Meridian references.
RowsToRetrieveForFind	DWORD	Maximum number of documents to show in **Find** results at one time.
ShowAllTablesImportDB	DWORD	If this value is **0** (default) the **Database Import Wizard** in Meridian Enterprise Configurator will only show the tables of the type TABLE (named ranges) that are present in a Microsoft Excel worksheet for selection to import. If this value is **1**, the tables of all types are shown.

Value Name	Data Type	Value Data
ShowRenditions	DWORD	Displays the rendition of the selected document in the viewer pane by default instead of the source file. This setting can also be configured in the **PowerUser Options** and **PowerWeb Preferences** dialogs. For PowerUser, see *Appearance Options* in the *Meridian Enterprise User's Guide*. For PowerWeb, see *Personal Preferences* in the *Meridian Enterprise User's Guide*.
ThumbnailAutoUpdate	DWORD	If this value is **1** (default), enables automatic generation of thumbnails. If this value is **0**, disables automatic generation.
ThumbnailUpdateMode	DWORD	If this value is **1**, generates thumbnails with viewer. If this value is **0** (default), use saved preview images when available. Configured in the **PowerUser Options** dialog. See *Advanced Options* in the *Meridian Enterprise User's Guide*.
UpdateReferences	DWORD	If this value is **1** (default), enables the assembly duplicator's **Update SolidWorks references** option in the **Assembly Copy Options** dialog box. See *Duplicate References* in the *Meridian Enterprise User's Guide*.
UseImportedFrom	DWORD	This setting overrides the server registry key with the same name described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Server .
UseWebHelp	DWORD	If this value is **0** (default), local help content is shown when the user presses **F1** within a Meridian client application. Learn how to install an updated version of the local help. If this value is **1**, the Meridian online help content is shown.

Value Name	Data Type	Value Data
WebServicesMode	DWORD	If this value is **0** (default), Application Integration operates in Online mode. If this value is **1**, it operates in Remote mode. This value overrides the value with the same name in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client.
WorkSpaceDB	DWORD	The following locations will be searched for this value in the order listed and the value of the first location where it is found will be applied: 1. This registry key (affects only the current user of the PC). 2. HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client (affects all users of the PC) Local Workspace database format and version. Possible values are: **0**: Microsoft Jet database engine (default, installed separately) **1**: SQL Server Compact Edition 3.5 (installed separately) **4**: SQL Server Compact Edition 4 (installed separately) **8**: SQLite (installed only by the Meridian Cloud Client installation package) SQL Server Compact is in End of Life status. We provide SQL Server Compact as an option for backwards compatibility only.

Value Name	Data Type	Value Data
WorkSpaceLockID	String	The following locations are searched for this value in the order listed and the value of the first location where it is found is applied: 1. This registry key (affects only the current user of the PC). 2. HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client (affects all users of the PC) A unique value that identifies a user's Local Workspace on each computer that they use. This value is only used by PowerUser. For PowerWeb users, see the **WorkspaceLockID** value in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\Published Locations\<ID> If a pool of remote access host computers (running PowerUser) will be used, set this to a value to be used by all of the remote access host computers, such as **Citrix** or **RemoteDesktop**. The value can be anything so long as it is the same for all of the remote access host computers. For remote access host computers running PowerWeb, see the **CommonWorkspace** value in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\Published Locations\<ID>.

Value Name	Data Type	Value Data
WorkSpaceNoUserName	DWORD	The following locations are searched for this value in the order listed and the value of the first location where it is found is applied: 1. This registry key (affects only the current user of the PC). 2. HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client (affects all users of the PC) If this value is **1**, the user account name is not appended to the Local Workspace folder name. If this value is **0** (default), the account name will be appended. This is useful only if **WorkSpaceLocation** is also defined. If set in the HKEY_LOCAL_MACHINE hive on the Meridian web server for the account under which Application Integration runs, Application Integration will periodically clean up the local workspace location of all stale temporary files created for PowerWeb users.
WorkingColor	DWORD	Color to display document names in the view pane for documents under change.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Configurator

Registry values

Value Name	Data Type	Value Data
Various	Various	Settings related to the default location and display of Configurator user interface elements

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Configurator\Settings

Registry values

Value Name	Data Type	Value Data
ReuseExistingObjects	DWORD	If this value is **1** (default) existing workflow definitions are not updated when a vault configuration (`.met`) file is imported. This is to prevent errors that can occur from inconsistencies with active workflows. If this value is **0**, the imported definitions are saved. This value should only be changed if recommended by Accruent Technical Support.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\InventorLink

Registry values

Value Name	Data Type	Value Data
CacheLockOnOpen	DWORD	If this value is >**0**, forces the link to set cache lock on every document in an assembly that is currently under change by the user. If this value is **0**, does not set cache lock.
CreatesQuickChange	DWORD	If this value is >**0**, forces the link to use Quick Change instead of Under Change. If this value is **0**, does not use Quick Change.
HideGetWriteAccess	DWORD	If this value is **1**, hides messages by clicking **No**. If this value is **2**, hides message by clicking **Yes**. If this value is **0**, does not hide messages.
HideIsReadOnlyMessage	DWORD	If this value is >**0**, disables messages about the document being read-only. If this value is **0**, enables messages.
NewLibraryComponentDocType	String	Document type internal name to use for any new library document created by Inventor.
ReleaseNewLibraryComponent	DWORD	If this value is >**0**, forces the link to release a library component after it has been imported into the vault. If this value is **0**, does not release. Use with NewLibraryComponentDocType.
ShowAMBrowserOnOpen	DWORD	If this value is **0** (default), the Inventor browser will be activated upon file open commands. If this value is >**0**, the Meridian Assembly Browser will be activated.
ShowOptionsOnOpen	DWORD	If this value is **1** , the Inventor **File Open Options** dialog will be shown when opening assemblies. If this value is **0** (default), the dialog is not shown.

Value Name	Data Type	Value Data
ShowOptionsOnSave	DWORD	If this value is **1** , an **Options** button is added to the Inventor **Save Copy As** dialog and **File Save Options** dialog. Users may click this button to show the Inventor **File Save Options** dialog when saving assemblies. If this value is **0** (default), the button is not shown.
UpdateDWFForAll	DWORD	If this value is >**0**, the Inventor Link will generate DWF images for any modified files when saving. If this value is **0** (default), a DWF file for only the main document is generated.
UpdateDWFOnSave	DWORD	If this value is >**0**, the Inventor Link will generate a DWF image when saving a file. The DWF file is imported into the vault (if possible) as a hybrid part of the saved document. If this value is **0** (default), no DWF is generated.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\LotusManagerUI

Registry values

Value Name	Data Type	Value Data
HideVaultFolder	DWORD	If this value is **1**, hides the **Imported messages folder** option in the **Lotus Notes Export** dialog. The user may not select the destination folder and the vault configuration must store the messages correctly. If this value is **0** (default), the option is visible.
EmbeddedAttachments	DWORD	If this value is **1**, embedded graphics such as signature logos in IBM Lotus Notes messages will be imported into the vault. If this value is **0** (default), the images are not imported.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\MicroStationLink

The following locations will be searched for this value in the order listed and the value of the first location where it is found will be applied :

1. HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\MicroStationLink (affects all users of the PC)
2. This registry key (affects only the current user of the PC (affects all users of the PC).

Registry values

Value Name	Data Type	Value Data
ButtonsForAll	DWORD	If set to **1**, shows **OK to All** and **Cancel to All** buttons in the confirmation dialog box that appears when a user invokes the **Sync Tag Hotspot** command on a selection of documents and one or more of the documents has circular references. By default, the dialog box will appear once for every document in the selection that has circular references so that the user can decide what to do with each document. This setting allows the user to apply their response to all of the problem documents in the selection at one time. The default is **0**, which does not show the batch response buttons.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\OfficeClient

Registry values

Value Name	Data Type	Value Data
Various	Various	Settings related to the default location and display of Office client user interface elements

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Offline\Settings

Registry values

Value Name	Data Type	Value Data
AutoRemoteProp	DWORD	This value is **1** when Offline client is in the mode of showing remote properties. The next time it is Started, the mode will be restored.
CanChangeUser	DWORD	If this value is **1**, enable the user to log on with another name in the Offline client. If this value is **0**, do not allow other names.
ConnectOnStart	DWORD	This value is **1** when connected to a remote vault. The next time it is Started, it will try to reconnect to the vault.
CreateFolders	DWORD	If this value is **1** (default), allows creation of parent folder in the vault if the parent folder does not exist yet. If this value is **0**, does not allow folder creation.
CustomSecurity	DWORD	If this value is **1**, override Internet security settings. If this value is **0**, respect the settings.
ProcessRemote	DWORD	If this value is **1** (default), process remote folders and documents in offline mode. If this value is **0**, do not process.
ResursiveOnFolders	DWORD	If this value is **1** (default), process folders recursively in offline mode. If this value is **0**, do not recurse folders.
ShowNewAsWC	DWORD	If this value is **1**, also show documents that are new in the Local Workspace. If this value is **0** (default), do not show new documents.

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\ScriptEditor

Registry values

Value Name	Data Type	Value Data
Various	Various	Settings related to the default location and display of Script Editor user interface elements

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\ScriptEditor_Full

Registry values

Value Name	Data Type	Value Data
Various	Various	Settings related to the default location and display of Script Editor user interface elements

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\UIBeh

Registry values

Value Name	Data Type	Value Data
Various	Various	

HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\WPTEditor

Registry values

Value Name	Data Type	Value Data
Various	Various	

HKEY_LOCAL_MACHINE

The following tables list the registry keys of the HKEY_LOCAL_MACHINE hive. These keys affect all users of the computer.

HKEY_LOCAL_MACHINE\Software\Cyco

Registry values

Value Name	Data Type	Value Data
Active Product	String	Internal name of the active Meridian product.
AmAcDbHost<*n*>	String	Path of the active AutoCAD database library file.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian

Registry values

Value Name	Data Type	Value Data
Path	String	Path where the application is installed.
ProgramPath	String	Path to the application executables.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\<*PatchLevel*>

Registry values

Value Name	Data Type	Value Data
PatchLevel	String	Version name of the installed Meridian application.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion

Registry values

Value Name	Data Type	Value Data
AmwUpg	String	Path to the Meridian Workflow upgrade tool and support files.
CustomDocumentImagesLarge	String	Full path to the custom image list `CustomDocumentImagesLarge.bmp`.
CustomDocumentImagesSmall	String	Full path to the custom image list `CustomDocumentImagesSmall.bmp`.
CustomFolderImagesLarge	String	Full path to the custom image list `CustomFolderImagesLarge.bmp`.
CustomFolderImagesSmall	String	Full path to the custom image list `CustomFolderImagesSmall.bmp`.
Build	String	Build number of the installed Meridian application.
Features	DWORD	If this value is 1, enable prerelease features. If this value is 0 (default), do not enable features. This value is only used internally by Accruent.
KeepLocaleNumeric	DWORD	If this value is 0 (default), Meridian will not change numeric options of locale settings when a language other than English is installed.
Language	String	Locale code of the default user interface language chosen during installation. Can be overriden by the **Language** value in `HKEY_CURRENT_USER\Software\Cyco\Meridian Enterprise\CurrentVersion`. For more information about switching languages, see Install Second Language Support.

Value Name	Data Type	Value Data
LCID	DWORD	Locale ID number to be used to show data like dates. For example, the value 1024 (decimal) uses the default user locale, 2048 uses the default system locale, 1033 uses American English, 1034 uses Spanish Spain, and so on. If not set, then the locale is determined by the **Language** value. If the UI language is English, the default user locale will be used. For a list of the valid hexadecimal values, see LCID Structure.
PathName	String	Path to the Meridian client application.
RemoteOnly	DWORD	Controls the options that appear in the shortcut menu for the Accruent Application Integration icon in the system tray. There are two options for this setting: **0**: Default functionality. All options are available. If users using the Cloud Connector need to change the Site Cache URL, you will need to use this value. **1**: Remote mode settings only. The following settings are disabled: • Selecting Online mode. • Selecting the default context. • Selecting the Site Cache URL. • Selecting the option to sync in offline and remote mode. Learn more about these settings by reading the *Configure Local Workspace* article in the *Meridian Enterprise User's Guide*.
WebHelpBaseURL	String	This registry key value is no longer used as of the 2022 release.
WebHelpVersion	String	The online help version to display to users in PowerWeb and PowerUser. This value can be used to override the version of online help you display for your users. We do not recommend changing this value.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMAdmin

Registry values

Value Name	Data Type	Value Data
ForceShowUserManagementNode	DWORD	By default, the **Users and Groups** branch of the Meridian Enterprise Administrator utility is only visible when the user accounts and groups are stored in the Meridian user database. When the **Use Enterprise Server for user management** option is enabled as described in Configure the Connection To Meridian Enterprise Server, the branch is hidden because the user accounts and groups are then stored in the Meridian Enterprise Server database instead. Setting this value to 1 forces the branch to appear anyway. This is typically done so that an administrator can then use the **Unlock Documents** command described in Unlock Local Workspace Documents.
NodesMask	DWORD	Can be set to show some or all of the branches in the Meridian Enterprise Administrator utility. This is so that responsibility for maintaining the data in each branch can be delegated to different users without giving them access to other branches. Supports any combination of the following values: 1: License Server (hidden by default) 2: EDM Server 4: PowerWeb 8: AMFS Server 16: Accruent Users and Groups To show all of the branches, set this value to **31** decimal (**1F** hexadecimal). To show only the default branches, set this value to **30** decimal (**1E** hexadecimal).

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMDownload

Registry values

Value Name	Data Type	Value Data
Program	String	Path of the executable used for downloading documents by PowerWeb.
URL	String	Default URL for PowerWeb.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHook

Registry values

Value Name	Data Type	Value Data
MultiSelectionEnabled	DWORD	If this value is **1**, the file **Open** file dialog box of Application Integration allows the user to select multiple files to open in AutoCAD. If this value is **0**, only one file can be selected.
RevertToRoot	DWORD	Set to **1** to make the **Folder** view the default in Application Integration when you open or save a document. If the key is missing, Application Integration opens the last view you selected.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHookTray\ForceList\<*executable*>

Registry values

Value Name	Data Type	Value Data
Path	String	Path of an executable to force to use Meridian Application Integration. This value is checked first and, if not set, the corresponding key with the same name in HKEY_CURRENT_USER is checked. This value is not set by the Application Integration **Show Accruent Dialog For** dialog box but can be set by a System Administrator and is retained for backward compatibility with previous versions. The HKEY_CURRENT_USER value is set by the **Show Accruent Dialog For** dialog box. If there are multiple versions of the same program installed on the PC, they will all be included regardless of their paths.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMHookTray\RejectList\<*executable*>

Registry values

Value Name	Data Type	Value Data
Path	String	Path of an executable to exclude from Meridian Application Integration. This value is checked first and, if not set, the corresponding key with the same name in HKEY_CURRENT_USER is checked. This value is not set by the Application Integration **Edit Exclusion List** dialog box but can be set by a System Administrator and is retained for backward compatibility with previous versions. The HKEY_CURRENT_USER value is set by the **Edit Exclusion List** dialog box. If there are multiple versions of the same program installed on the PC, they will all be excluded regardless of their paths.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian \CurrentVersion\AMHookTray\SupportedTypes

Registry values

Value Name	Data Type	Value Data
ACAD 2000 I Dialog	String	Path of an executable to detect AutoCAD file dialog actions for Meridian Application Integration.
CommonDialog	String	Path of the executable to intercept common Windows application file dialog actions for Meridian Application Integration. Default = `CommDlgDetect.dll`.
InventorDetect	String	Path of an executable to intercept Inventor file dialog actions for Meridian Application Integration. Default = `InventorDetect.dll`.
Microsoft Office Dialog	String	Path of an executable to intercept Microsoft Office file dialog actions for Meridian Application Integration. Default = `MSOfficeDetect.dll`.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMOfficeAddIn\Excel

Registry values

Value Name	Data Type	Value Data
DisablePropertiesUpdate	DWORD	By default, the Office link updates document properties automatically depending on the settings configured for the vault. This value provides additional control over when property updates occur. The possible values are: **0**: Perform all automatic updates (default) **1**: Disable automatic updates when documents are opened **2**: Disable automatic updates when documents are saved **3**: Disable all automatic updates

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian \CurrentVersion\AMOfficeAddIn\PowerPoint

Registry values

Value Name	Data Type	Value Data
DisablePropertiesUpdate	DWORD	By default, the Office link updates document properties automatically depending on the settings configured for the vault. This value provides additional control over when property updates occur. The possible values are: **0**: Perform all automatic updates (default) **1**: Disable automatic updates when documents are opened **2**: Disable automatic updates when documents are saved **3**: Disable all automatic updates

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMOfficeAddIn\Word

Registry values

Value Name	Data Type	Value Data
DisablePropertiesUpdate	DWORD	By default, the Office link updates document properties automatically depending on the settings configured for the vault. This value provides additional control over when property updates occur. The possible values are: **0**: Perform all automatic updates (default) **1**: Disable automatic updates when documents are opened **2**: Disable automatic updates when documents are saved **3**: Disable all automatic updates

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AMOMLUI\SafeProperties

Registry values

Value Name	Data Type	Value Data
<PropertySet.PropertyName>	String	The property set and property name of a Meridian internal property to allow to be changed, such as by scripting. Multiple properties can specified by creating separate values. Most internal properties are read-only. This key is used by some Meridian modules to integrate with the internal property set. Use with extreme caution as data loss could occur from misuse.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AssetManagement

Registry values

Value Name	Data Type	Value Data
ItemsToFind	DWORD	The maximum number of items to show in query results by the Meridian Asset Management Module. The value must be >= 10. This value can overridden by **ItemsToFind** in HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AssetManagement. In PowerWeb, if this value is **0**, all items are shown. If the value is absent, the default is 250 items.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\AutocadLink

Registry values

Value Name	Data Type	Value Data
AcadBaseConfig[1]	DWORD	Controls the functionality provided by the AutoCAD link: **0**: Basic AutoCAD link features only **1**: Basic AutoCAD link features plus sheet set support (default) **2**: Basic AutoCAD link features plus plain drawing asset management support (not for use with AutoCAD P&ID or AutoCAD Plant 3D) **3**: Enable all AutoCAD link features **32**: Enable the **Synchronize All Data Shortcuts to Vault** command in the AutoCAD Civil 3D application link To learn more about the **Synchronize All Data Shortcuts to Vault** command, see *Data Shortcuts* in the *Meridian Enterprise User's Guide*.
AcadPnIDConfig[1]	DWORD	Controls the P&ID functionality provided by the AutoCAD link. This setting requires AutoCAD P&ID or AutoCAD Plant 3D. **0**: P&ID project features only (default) **1**: P&ID project features plus asset management support

Value Name	Data Type	Value Data
ButtonsForAll	DWORD	If set to **1**, shows **OK to All** and **Cancel to All** buttons in the confirmation dialog box that appears when a user invokes the **Sync Tag Hotspot** command on a selection of documents and one or more of the documents has circular references. By default, the dialog box will appear once for every document in the selection that has circular references so that the user can decide what to do with each document. This setting allows the user to apply their response to all of the problem documents in the selection at one time. The default is **0**, which does not show the batch response buttons.
Civil3DSyncType[1,2]	DWORD	Controls the synchronization of the folder specified for **Civil3DSyncWorkingFolder**: **1**: Synchronize to the local working folder (on drawing open) **2**: Synchronize to the vault (on drawing close) **4**: Ask the user before synchronization **8**: Synchronize only once per AutoCAD session
Civil3DSyncWorkingFolder[1,2]	DWORD	If this value is **1**, synchronizes the entire folder that is specified as the working folder in AutoCAD Civil 3D. If this value is **0** (default), only the data shortcuts folder is synchronized.

Value Name	Data Type	Value Data
DisableTitleBlockUpdate	DWORD	By default, the AutoCAD link updates mapped title block attributes automatically depending on the settings configured for the vault. This value provides additional control over when title block attribute updates occur. The possible values are: **0**: Perform all automatic updates (default) **1**: Disable automatic updates when documents are opened **2**: Disable automatic updates when documents are saved **3**: Disable all automatic updates To control updates to individual title blocks, see the **AutoUpdate** setting described in the *Configure Standard Title Block Synchronization* article in the *Meridian Enterprise Configuration Guide*.
DocAccessSaveThumbnail	DWORD	Controls the generation of thumbnail images during link updates. If this value is **0** (default), thumbnails are not saved. If this value is **1**, thumbnails are saved. **Important!** If this value is **1** and thumbnail generation fails for any reason, it could prevent property synchronization, which could be more important.
DocAccessUseTmpFileOnSave	DWORD	This setting is for supporting AutoCAD drawing title block updates over a Citrix remote access connection. If this setting is **1**, the drawing is opened for reading only and changing its content is performed by using a temporary file. The default is **0**.

Value Name	Data Type	Value Data
DocAccessUseTmpFolder	DWORD	This setting is for supporting AutoCAD drawing title block updates over a Citrix remote access connection. If this setting is **1** and **DocAccessUseTmpFileOnSave** is set to **1**, the temporary file is created in the system temporary folder. If it is set to **0** (default), the file is created in the same folder as the original file.
ManualUpload	DWORD	This setting allows you to opt out of automatic uploads of AutoCAD documents. **0**: Setting is disabled. **1**: Automatic upload is disabled. A new **Upload Document** button is added to the Meridian ribbon. This button is visible in remote mode only, and is enabled after the first save of the document. **2**: Ignored. **3**: Automatic upload is enabled on document close only. A new **Upload Document** button is added to the Meridian ribbon. This button is visible in remote mode only, and is enabled after the first save of the document. To learn about remote mode, see the *Offline Mode And Remote Mode* section or the *Application Links In Remote Mode* article in the *Meridian Enterprise User's Guide*.
RealDwgFonts	String	The path to RealDwg fonts installed by the Meridian Enterprise setup program.
RealDwgForceValidity[1]	DWORD	If this value is **1** (default), the **Sync Properties to File** command works with AutoCAD Release 14 and older drawings but importing drawings can fail if the title blocks are synchronized also. If this value is **0**, the command does not work with older drawings but importing drawings will not fail if the title blocks are synchronized.

Value Name	Data Type	Value Data
ReleaseNewCivil3DDataShortcuts[1,2]	DWORD	If this value is **1**, Civil 3D data shortcuts are automatically released from their workflows when they are imported to the vault by working folder synchronization. If this value is **0** (default), the shortcuts are not automatically released.
RepairDocState	DWORD	If this value is **1**, it fixes an issue with drawings being read-only and cannot be saved when opened from PowerWeb in Online mode with a site cache configured. The default value is **0**.
SyncTagsOnSave	DWORD	If this value is greater than **0**, updates Meridian Asset Management Module tag references when drawings are saved.
TurnOnMenuBar	DWORD	If this value is **1**, shows the AutoCAD link menu bar. If this value is **0**, the menu bar is hidden.
UseRowRibbon	DWORD	Controls the style of the display of the Accruent page in the AutoCAD Ribbon. The possible values are: **0**: Without items rows **1**: With item rows (default) For more information, see the *AutoCAD Link* article in the *Meridian Enterprise User's Guide*.

1. The following locations will be searched for this value in the order listed and the value of the first location where it is found will be applied :
    a. This registry key (affects all users of the PC)
    b. HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\AutocadLink (affects only the current user of the PC)
2. In addition to the locations listed above, the **[Civil_3D]** section on the **AutoCAD** tab of the **Application Link Settings** in the **Environment** branch of the vault configuration.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client

Registry values

Value Name	Data Type	Value Data
BCSiteCacheURL	String	URL of the site cache server for use by PowerWeb. This value is set by the installation package. If this value is missing, then the value with the same name in HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Client\Settings is applied. **Important!** Users should not work on the same documents from more than one PC with Application Integration in Remote mode and site caches enabled or document content inconsistencies can occur.
ConnectionRetries	DWORD	The maximum number of connection retries that the Site Cache Client makes. The default value is **3**.
ConnectionRetryInterval	DWORD	The time interval in seconds between connection retries made by the Site Cache Client. The default value is **10**.
DefaultVaultListLocation	String	See *Lookup Lists* in the *Meridian Enterprise Configuration Guide*.
DisabledFeatures	DWORD	This value is intended to improve the performance of PowerWeb deployments where no Meridian Enterprise Server computer is deployed and the **Computer running the Enterprise services** option of the **EDM Server** service is empty as described in Configure the connection to Meridian Enterprise Server. Set to **0x000c0000** (hexadecimal) to prevent PowerWeb from attempting to connect to a Meridian Enterprise Server computer.

Value Name	Data Type	Value Data
DisableOfflineSwitch	DWORD	If this value is **1**, disable Offline mode switching in Application Integration. If this value is **0** (default), do not disable Offline mode switching. See Disable Offline Mode. If this value is missing, then the value with the same name in HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Client\Settings is applied.
ExcludeCertificates	DWORD	If this value is **1**, prevents the names of certificates from appearing in the **User Name** list when electronically signing documents in PowerWeb with the **ActiveX compatibility mode** option enabled and a security policy is configured to use a certificate and PIN. If this value is **0** (default), the certificates are shown and can be selected.
ExtForDuplicator	String	List of file extensions separated by semicolons for the types of documents for which the Duplicator commands are enabled. By default, `".dwg;.iam;.ipt;.idw;.ipn;.asm;.sldasm;.drw;.slddrw;.prt;.sldprt;.dst"`.
EnableScriptLog	DWORD	If this value is **1**, VBScript events, command scripts, evaluated expressions, and external function calls are logged to a file for troubleshooting customization and performance. The log is also shown in a left pane in PowerUser. If this value is **0** (default), logging is disabled. To enable the **Download Log** menu command in PowerWeb, set the **CanDownloadLog** setting to **1** in the user's PowerWeb profile file as described in the *Edit PowerWeb User Profiles* article in the *Meridian Enterprise Configuration Guide*.
ForceDocTypeDialog	DWORD	If this value is **1**, forces display of the **Create a new document** dialog. If this value is **0** (default), does not force display of the dialog.
HideDuplicator	DWORD	If this value is **1**, the client disables the Duplicator menu commands. If this value is **0** (default), the commands are enabled.

Value Name	Data Type	Value Data
LogDetails	DWORD	Set this value to **1** to record Site Cache Client connection retries in the log.
LWSConflictTime	DWORD	The maximum allowable difference between the server clock time and the client workstation time in seconds. This registry key must be set on the workstation. The default value for it is **1**.
MinutesToSleep	DWORD	Time interval after which PowerUser closes the vault, thus releasing the database connection license (but not the client license) and server memory resources. If this setting is absent or **0**, the application will not close the connection on a timely basis.
NotReservedTmmLic	DWORD	If this value is **1**, reserved licenses are not required for the Meridian Transmittal Management Module. If this value is **0** (default), licenses must be reserved.
OfficeClient_MaxInstances	DWORD	The maximum number of Office Client instances that can be open simultaneously on the computer.
OfflineLicense	DWORD	If this value is **1**, attempt to claim offline license succeeded. If this value is **0**, attempt failed.
OfflineMode	DWORD	If this value is **1**, metadata cached in the Local Workspace database and documents are not automatically synchronized with the Meridian application server in real-time, users must invoke the synchronization commands described in the *Manually synchronize the local workspace* article in the *Meridian Enterprise User's Guide*. If this value is **0**, they are automatically synchronized with the Meridian application server depending on the setting of **WebServicesMode**. This setting can also be set on the Application Integration shortcut menu. For use with remote access software, set this value to **1** on the remote access client PC and to **0** on the remote access host PC. If this value is missing, then the value with the same name in HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Client\Settings is applied.
PowerUser_MaxInstances	DWORD	The maximum number of PowerUser instances that can be open simultaneously on the computer.

Value Name	Data Type	Value Data
RunRemoteApp	DWORD	This value is intended for use with remote access software as described in Prepare the Remote Access Client Computers. This value enables support for opening documents in the registered Windows application on the remote client PC when the user double-clicks on the document in PowerUser running on a remote host PC. If this value is **1** when the user double-clicks on the document: • The local workspace on the remote access host is synchronized (the document and all its references are downloaded and the document is locked in the vault). • The registered application on the remote access host is not launched as usual. • The document is downloaded to the local workspace on the remote access client PC the same as if the PowerUser were running locally. A special empty file is created in a sub-folder of the local workspace named *<WorkSpaceLocation>/<VaultContext>*__$$RUN on the remote access client PC. The name of the file is the full path to the document in the local workspace with the backslashes replaced with the vertical bar character (|), for example, M-MyPC,D-MyVault|New Folder|New Text Document.txt.run. • Application Integration running on the remote access client PC monitors the sub-folder. When Application Integration detects a .run file, it opens the local workspace document in the registered application on the local PC for the user to work with the document. After the application is launched, Application Integration deletes the .run file. If this value is **0** (default), the document is opened in the registered application on the remote host PC as usual.

Value Name	Data Type	Value Data
SkipSyncForOpen	String	List of file extensions separated by semicolons for the types of documents to be skipped by Local Workspace reference synchronization when the files are opened in the native application. By default, ".iam;.ipt;.idw;.sldasm;.asm; .sldprt;.prt;.slddrw;.drw;.dgn;.dwg". The default is not used if a value is absent. It is set by the setup program only if the key does not exist and depends on the links installed.
SkipSyncForView	String	List of file extensions separated by semicolons for the types of documents to be skipped by Local Workspace reference synchronization when the files are opened for viewing. By default, ".iam;.ipt;.idw;.sldasm;.asm; .sldprt;.prt;.slddrw;.drw;.dgn;.dwg". The default is not used if a value is absent. It is set by Setup only if the key does not exist, and depends on the links installed.
SkipToC	DWORD	Set this value to **1** for the synchronization to skip the Table of Contents.
SpecialBuild	String	Optional text shown at the top of splash screens and About dialogs.
UseAMFS	DWORD	This is a legacy setting related to a Windows feature that is no longer supported. Do not change the default value of this setting, or you will encounter issues with clients being unable to access file contents.
UseCICO	DWORD	Set this value to **1** for compatibility with remote access software. For more information, see Prepare the Remote Access Host Computer.

Value Name	Data Type	Value Data
WebServicesMode	DWORD	If this value is **0** (default), metadata cached in the Local Workspace database and documents are automatically synchronized with the Meridian application server in real-time using DCOM. If this value is **1**, the they are automatically synchronized using an HTTP connection to the Meridian web server. If this value is missing, then the value with the same name in HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Client\Settings is applied.
WorkSpaceAccountName	DWORD	If this value is **1**, the user folder in Local Workspace will contain the domain name from the user account like *<UserName>.<DomainName>*. If this value is **0** (default), the folder name will not contain the domain name.
WorkSpaceDB	DWORD	The following locations are searched for this value in the order listed and the value of the first location where it is found is applied: 1. HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Client\Settings (affects only the current user of the PC) 2. This registry key (affects all users of the PC.) Local Workspace database format and version. Possible values are: • **0**: Microsoft Jet database engine (default, installed separately) • **1**: SQL Server Compact Edition 3.5 (installed separately) • **4**: SQL Server Compact Edition 4 (installed separately) • **8**: SQLite (included) **Important!** SQL Server Compact is in End of Life status. We provide SQL Server Compact as an option for backwards compatibility only.

Value Name	Data Type	Value Data
WorkSpaceLocation	String	Path to the Local Workspace folder in the form *<LocalDrive>**<FolderName>*. The default value is set during Meridian client installation and can be left at the default value or it can be modified. This setting is for online clients only. The Windows **%USERNAME%** environment variable may be used. For compatibility with remote access software, set this value to ***<RemoteResourceName>**<ShareName>**<FolderName>***. In order for the remote access host computer to store documents on the remote access client computer for editing, the remote access client computer's drive resources must be accessible through the remote access connection. This capability goes by different names depending on the remote access software used. For example, the option is named Local Resources in Microsoft Remote Desktop Connection and is enabled by default. To specify a local resource for Microsoft Remote Desktop Connection, replace *<RemoteResourceName>* with **tsclient** and *<ShareName>* and *<FolderName>* with appropriate values for the remote access client computers. If you are using different remote access software, set **WorkSpaceLocation** to a value that is appropriate for your remote access software and ensure that the local drive resource is shared or mapped accordingly.

Value Name	Data Type	Value Data
WorkSpaceLockID	String	The following locations are searched for this value in the order listed and the value of the first location where it is found is applied: 1. HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Client\Settings (affects only the current user of the PC) 2. This registry key (affects all users of the PC.) A unique value that identifies a user's Local Workspace on each computer that they use. This value is only used by PowerUser. For PowerWeb users, see the **WorkspaceLockID** value in HKEY_LOCAL_ MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\Published Locations\<ID> If a pool of remote access host computers (running PowerUser) will be used, set this to a value to be used by all of the remote access host computers, such as **Citrix** or **RemoteDesktop**. The value can be anything so long as it is the same for all of the remote access host computers. For remote access host computers running PowerWeb, see the **CommonWorkspace** value in HKEY_LOCAL_ MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink\Published Locations\<ID>.

Value Name	Data Type	Value Data
WorkSpaceNoUserName	DWORD	The following locations are searched for this value in the order listed and the value of the first location where it is found is applied: 1. HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\Client\Settings (affects only the current user of the PC) 2. This registry key (affects all users of the PC.) If this value is **1**, the user account name is not appended to the Local Workspace folder name. If this value is **0** (default), the account name will be appended. This is useful only if **WorkSpaceLocation** is also defined. If set in this branch (HKEY_LOCAL_MACHINE) on the Meridian web server for the account under which Application Integration runs, Application Integration will periodically clean up the local workspace location of all stale temporary files created for PowerWeb users.
WorkSpaceSharedCheck	DWORD	If this value is **1**, during document downloads, shared workspace folders are detected and recreated if they do not exist, which can take a unacceptable amount of time if the folders no longer exist. If this value is **0** (default), this checking is not done and downloads occur faster but referenced drawings may not be resolved correctly. If there is no desktop.ini file and the Shared Workspace does not function, this can be resolved by setting the value to **1**. This ensures that the necessary .ini file is created in the workspace location on the download operation.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\Currentversion\Client\Bcsitecacheauth

The values with the same name in HKEY_CURRENT_USER are checked first and, if not set, the values in this key are read, if present.

Registry values

Value Name	Data Type	Value Data
M360Tenant	String	Name of the Meridian Portal tenancy where the OpenId authentication credentials are specified.
IssuerUri	String	URI of the OpenId authority.
UseOpenIdConnectAuthentication	DWORD	If this value is **1**, connect this PC to the site cache server using the OpenId authentication credentials specified in the configuration of the tenant in **M360Tenant**. If this value is **0** (default), connect to the site cache server via the logged on Windows account.
UseWorkspace	DWORD	If this value is **0** (default), temporary copies of documents are downloaded from the site cache to the user's normal local workspace just as if they were working in a vault in their own domain. Typically, the path of the local workspace contains the user's Windows account name. If this value is **1**, places the temporary copies in a separate local workspace path that contains the name of the account used by the OpenId authentication credentials.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\Client\Options for all scanners

Registry values

Value Name	Data Type	Value Data
Bilevel	DWORD	Monochrome raster image format number. Absent key corresponds to Undefined. 1 TIFF uncompressed 2 TIFF PackBits 3 TIFF Huffman encoded 6 TIFF Group 4 (default)
Color	DWORD	Color raster image format number. Default = 12 (JPEG). Absent key corresponds to Undefined.
Gray	DWORD	Grayscale raster image format number. Default = 12 (JPEG). Absent key corresponds to Undefined.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\ICWLink

Registry values

Value Name	Data Type	Value Data
SkipUpdateReferencesEvents	DWORD	Set to **1** to skip the following events: • DocCADLink_InitializeUpdateReferences • DocCADLink_BeforeUpdateReferences • DocCADLink_AfterUpdateReferences • DocCADLink_TerminateUpdateReferences This improves performance when you edit and save assemblies in Autodesk Inventor. If the key is missing or set to a value other than 1, the system runs all reference update events.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\InventorLink

Registry values

Value Name	Data Type	Value Data
OnImportAssmTimeout	DWORD	Time (in msec) for the **Assembly Import Wizard** to wait to complete when importing an assembly. Default = **1000**.
RedrawTitleblocksOnUpdate	DWORD	If this value is >**0**, enables regeneration of title blocks after properties update to file. If this value is **0**, disables regeneration.
SettingsSource	DWORD	If this value is **1** (default), the following settings are read from the Inventor application link settings configured in Configurator. If this value is **0**, these settings are read from the registry of the client computer: HideIsReadOnlyMsg HideGetWriteAccess CreatesQuickChange NewLibraryComponentDocType RedrawTitleblocksOnUpdate ReleaseNewLibraryComponent For more information about these settings, see the *Control Autodesk Inventor Link Dialogs* and *Configure Autodesk Inventor Link Options* articles in the *Meridian Enterprise Configuration Guide*.

Value Name	Data Type	Value Data
SupportInventorDWG	DWORD	This value controls whether AutoCAD DWG files and their references, Autodesk Inventor DWG files and their references, or both are supported by the application links and utilities (Assembly Import Tool, for example): **0**: Only AutoCAD drawings are supported. Autodesk Inventor drawings are not supported. Default. **1**: AutoCAD drawings are not supported. Autodesk Inventor drawings are supported **2**: Both Autodesk Inventor and AutoCAD drawings are supported but errors can occur if the applications use different versions of RealDWG on the same computer **3**: Prevents **Documents of this version are not supported** errors when attempting to synchronize properties to a drawing that was created from an Autodesk Inventor DWG template
TerminateInventor11	DWORD	If this value is **1**, activates a workaround that solves a problem related to Inventor 11 Automation Server. If this value is **0** (default), does not activate the workaround.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\MicroStationLink

The following locations will be searched for this value in the order listed and the value of the first location where it is found will be applied :

1. This registry key (affects all users of the PC)
2. HKEY_CURRENT_USER\Software\Cyco\AutoManager Meridian\CurrentVersion\MicroStationLink (affects only the current user of the PC)

Registry values

Value Name	Data Type	Value Data
ButtonsForAll	DWORD	If set to **1**, shows **OK to All** and **Cancel to All** buttons in the confirmation dialog box that appears when a user invokes the **Sync Tag Hotspot** command on a selection of documents and one or more of the documents has circular references. By default, the dialog box will appear once for every document in the selection that has circular references so that the user can decide what to do with each document. This setting allows the user to apply their response to all of the problem documents in the selection at one time. The default is **0**, which does not show the batch response buttons.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\RevitLink

Registry values

Value Name	Data Type	Value Data
FamilyInspector	DWORD	If set to **1**, the **Family Inspector** command is available in the **Accruent** ribbon in Revit. When set to **0**, the command is not available.
NoUploadOnSave	DWORD	If set to **1**, the **Upload Project** command is available in the **Accruent** ribbon in Revit. Allows users to postpone uploading their project until they click the **Upload Project** button. When set to **0**, the command is not available. The project will be uploaded each time they save the project. The **Upload Project** button will be disabled until the project is first saved. After the project is uploaded, the button will again become disabled until the next save.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager View Control2

Registry values

Value Name	Data Type	Value Data
AppDir	String	Path to templates used by the Meridian viewer's **Compare** command.
BluePrintWSDL	String	URL of the Accruent web service. For example: `http://<ServerName>/BCWebService/BCWebService.BluePrintService.svc?wsdl`
Ccl	String	Name of the current version of the BlueCielo common module.
DLLDir	String	Path to the Meridian viewer modules.
HelpFile	String	Path to the Meridian viewer Help file.
Language	String	Language used by the Meridian viewer control. For information about switching languages, see Install Second Language Support.
RED	String	Name of the current version of the Meridian viewer redline module.
ServerMachine	String	Name of the Meridian server where the viewer control will query for the name of the computer where the Meridian license server is running. The control will then attempt to claim licenses from the license server. The viewer control will look first for the server name in **ServerMachine** in HKEY_CURRENT_USER\Software\Cyco\AutoManager View Control2. If a name is not found, then it will look in this value. If a server name is still not found, users will be prompted to select the Meridian server computer name when the viewer control cannot find a license server. The user's selection is saved in **ServerMachine** in HKEY_CURRENT_USER\Software\Cyco\AutoManager View Control2. Custom deployment packages should set this value so that the Meridian server name is available for all users of the client computer.
VWM	String	Name of the current version of the Accruent viewer view manager module.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager View Control2\Settings

Registry values

Value Name	Data Type	Value Data
AVLandscape	DWORD	Controls the rotation of watermarks (only when printed in landscape orientation) so that they can match the printer orientation. When set to **1**, watermarks are rotated clockwise. When set to **0xFFFFFFFF**, they are rotated counter-clockwise. This is a general setting that applies to all printers. To specify a rotation for a specific printer, see HKEY_CURRENT_USER\Software\Cyco\AutoManager View Control2\Settings\AVLandscape, which is also applied if this value is missing.
DisableChangeViewerPriority	DWORD	If this value is **1**, the users of the PC cannot change the priority of the viewers in the Meridian Enterprise client applications as described in *Change Viewers* in the *Meridian Enterprise User's Guide*. If this value is missing (default) or **0**, the users can change the viewer priority normally.
UseCurrentHost	DWORD	If this value is **1**, PowerWeb downloads files for viewing from the Meridian web server using its protocol, host name, domain name, and port number. If this value is missing (default) or **0**, it downloads files from the URL specified for **CustomFullURL** as described in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager Meridian\CurrentVersion\WebLink.

HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager View Control2\Settings\AVLandscape

Registry values

Value Name	Data Type	Value Data
<*PrinterName*>	DWORD	Controls the rotation of watermarks (only when printed in landscape orientation) so that they can match the orientation of the specified printer driver. When set to **1**, watermarks are rotated clockwise. When set to **0**, they are not rotated. This value is applied if the value is missing with the same name in HKEY_CURRENT_USER\Software\Cyco\AutoManager View Control2\Settings\AVLandscape. If both settings are missing, the **AVLandscape** value in HKEY_LOCAL_MACHINE\Software\Cyco\AutoManager View Control2\Settings will be used.

HKEY_LOCAL_MACHINE\Software\Microsoft\Visio\AddIns\AMOfficeAddIn.AMOfficeAddIn

Registry values

Value Name	Data Type	Value Data
FriendlyName	String	Accruent Office Link
Description	String	Accruent Meridian Enterprise link to MS Office
LoadBehavior	DWORD	3
CommandLineSafe	DWORD	1

HKEY_LOCAL_MACHINE\Software\Wow6432Node

This branch of the Windows registry supports 32-bit applications running on 64-bit versions of Windows as described in the following Microsoft Support article:

Registry changes in x64-based versions of Windows Server 2003 and in Windows XP Professional x64 Edition

Meridian Enterprise uses this branch for the same purpose. Therefore, any of the registry branches and values in the Software\Cyco branch may also appear in this branch.

HKEY_CLASSES_ROOT

The following tables list the registry keys of the HKEY_CLASSES_ROOT hive. These keys affect all users of the computer.

HKEY_CLASSES_ROOT\BlueCielo

Registry values

Value Name	Data Type	Value Data
(default)	String	URL:BlueCielo Protocol
URL Protocol	String	The type of document shortcuts added to email messages sent by PowerUser and returned by the **Vault.ComposeURL** method expressed as one or more AS_URL_FLAGS constants. For more information about the **Vault.ComposeURL** method, see the *Vault Object* article in the *Meridian Enterprise VBScript API Reference Guide*.

Meridian Task Server

Meridian Enterprise can be customized to provide extended functionality with the Meridian Task Server. The Task Server is a service that can be installed as part of a Meridian installation. It can run on any computer on a LAN.

By customizing Meridian events with VBScript, Meridian client applications can use the Task Server for processes that do not require user interaction or that are best offloaded to the Task Server computer, freeing the client computer for use by the user. The Task Server can be instructed to run predefined tasks that can be controlled by arguments that are determined by the customization code.

After submitting a task to the Task Server, the client application will continue, leaving the execution of the task to the Task Server. The Task Server will autonomously run all submitted tasks. It does not require any communication with the client that submitted the task, and it will not provide any feedback to the client about the result of the task.

Executing a task with the Task Server has these main advantages:

- **Ease of deployment and maintenance**: No software or configuration is required on the client computer (for example, the client needs no email software).
- **Performance**: Tasks do not use any resources of the client computer that submitted the task.
- **Flexibility**: Tasks can be invoked from PowerWeb.

The Task Server is not suited for operations that require:

- Interaction with the user
- Returning a result
- Confirmation when executed (success or failure)

The Task Server service itself does not perform tasks. It can be thought of as a central task controller, able to receive incoming task requests from client applications and to delegate those tasks to specified extensions. Tasks are performed by special ActiveX components called task server extensions. Task server extensions extend the Task Server with specific task functionality. The functionality does not rely on the configuration of the client workstation.

Set Up the Task Server

The first step in setting up a task server is to select the computer where the Task Server service will be run and task server extensions will run tasks. The computer you select depends on the resources required by the tasks you plan to use, but the computer should also conform to the system requirements described in Task Server System Requirements. In most cases, the Task Server can run on the Meridian application server. But if you plan to run resource-intensive tasks during production hours, a dedicated computer is preferable.

Set Up Task Server

To set up a Task Server:

1. Install the Task Server software components.

   Run the Meridian setup program on the Task Server computer and select only the Task Server component. This will install the Task Server service, which will be ready to process tasks without any further configuration.

2. Set the Task Server computer name on the Meridian server.

   When submitting tasks for a Task Server, the Meridian clients need to know the name of the Task Server computer where the tasks should be sent. By default, they retrieve this information from the Meridian EDM Server service to which they are already connected.

   If the Task Server computer is not also the computer where the EDM Server service is running, you should set the Task Server name on the EDM Server computer so that the clients can retrieve the name.

Set Task Server Computer Name

To set the Task Server computer name:

1. In the Meridian Enterprise Administrator, select **EDM Server** in the left pane.

   The list of active vaults appears in the right pane.

2. On the **Action** menu, select **Properties**.

   The **EDM Server Properties** dialog box appears.

3. Click the **Task Server** tab.

   The Task Server options appear.

4. Click **Browse**.

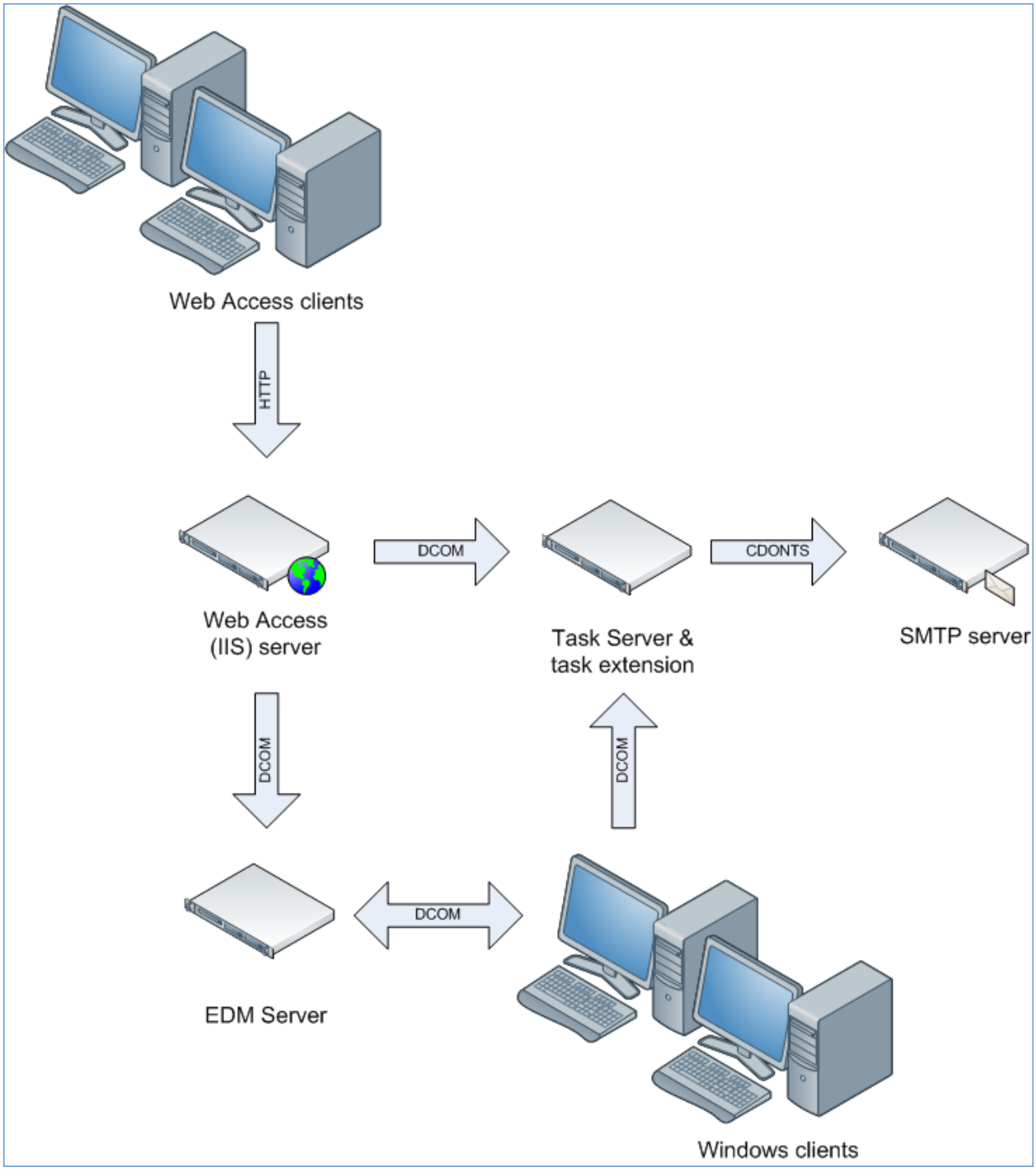
5. Select the computer.
6. Click **OK**.

Alternatively, clients can specify a Task Server computer name at the time that they submit tasks. This is useful when there are multiple Task Servers. In that case, the name of the Task Server must be passed in the task submission code as in the following example:

```
Vault.Task.Submit
("<LibraryName>.<ClassName>",,,,"<TaskServerComputerName>")
```

Task Server System Requirements

In principle, a client connection to the Meridian application server is not required in order to submit a task to the Task Server. However, this depends on the nature of the task. The following figure shows the relationship of the Task Server to other software components using the example email task extension. It illustrates that the Task Server does not rely on any other Meridian software.



The only requirements for using the Task Server are:

- Client applications, such as PowerWeb, must be able to create a DCOM connection to the Task Server.
- The task extension (DLL) must be registered on the Task Server computer.

- Any services or resources used by the task extension must be available (for example, Microsoft Collaboration Data Objects in the figure).

Task File Management

The Task Server stores submitted tasks as XML files in the following folder structure for processing:

`C:\ProgramData\BlueCielo\AMTasks`

Three subfolders are created as required:

- `Pickup`: Contains task files waiting to be processed.
- `Delayed`: Contains task files that have been specifically set to be executed at a later date or time.
- `Bad`: Contains task files that raised an error on execution. You will find an entry in the Windows application log describing the problem.

Task Server With PowerWeb

Because tasks can be invoked from VBScript customization, they can be used for both PowerUser clients and PowerWeb. VBScript customization is executed by the PowerWeb module that runs as an IIS extension.

The Task Server and PowerWeb (IIS) do not need to be installed on the same computer, but the PowerWeb process must have sufficient privileges to connect to the Task Server via DCOM. This will depend on the user account used for PowerWeb.

> **Note:**
> When PowerWeb is run with the IIS **Application Protection** option set to **Low (IIS Process)**, it will run under a local user account by default. In this case, it will have no access to a remote Task Server.

Submit a Task

Tasks for execution by the Task Server can be submitted from VBScript. To allow tasks to be invoked by the Meridian client applications, there is a **Task** object in the VBScript object model. The **Task** object is a property of the **Vault** object. It implements three methods required to compose and submit tasks: **Set**, **Submit**, and **Reset**.

First, the **Set** and **Reset** methods are used to set the correct parameter values for the task. These values are the specifics of the task to be performed and they are temporarily stored on the client. When the **Submit** method is called, these values will be passed to the Task Server where they are stored until the task is executed.

Reset method

Clears all **Task** object parameter values before the object is used to invoke another task.

Syntax

```
Reset
```

Remarks

There can only be one instance of the **Vault.Task** object. It is good coding practice in VBScript to use **Reset** before starting each task. This will ensure that all parameters are cleared the next time **Vault.Task** is used.

Example

```
Vault.Task.Reset
```

Set method

Stores a value for a specified parameter that will be passed to the Task Server (by **Submit**).

Syntax

```
Set (Parameter As String, Value)
```

Parameters

Name	Description
Parameter	String name of the parameter to be set. Required.
Value	Value of the parameter to be set. Required.

Remarks

Each task extension can define its own parameters. Refer to the documentation of the extension to find the appropriate names.

Submit method

Connects to the Task Server to submit a task.

Syntax

```
Submit (Type As String, [FSObject], [StartAt], [Priority], [Server])
```

Parameters

Name	Description
Type	The type of task that will be executed. This must be the ProgID of the task extension. The ProgID is a combination of the project name and the class name used by the Visual Basic project that produced the task extension. Required.
FSObject	A **Document** or **Folder** object. This parameter is only required if the task extension uses this information. Optional.
StartAt	A Date value. If any value is provided for this parameter, the Task Server will delay the execution of the task until this date/time. The Date value should be in Greenwich Mean Time (GMT). Optional.
Priority	Reserved for future use.
Server	The name of the Task Server computer to run the task. You can omit this parameter to use the default Task Server computer. Optional.

Remarks

All parameters provided by the **Set** method will be automatically passed to the Task Server when the task is submitted.

Apryse / PDFTron Local Fonts

By default, Apryse (formerly PDFTron) downloads fonts from the internet if they aren't available in your local Meridian installation. If your environment restricts internet access due to firewall rules or security policies, you can configure Meridian to use these fonts from a local folder instead.

Configure the use of local fonts in:

- Meridian PowerWeb
- Meridian Explorer

Configure Apryse / PDFTron Local Fonts in PowerWeb

Configure Meridian PowerWeb to use Apryse (formerly PDFTron) fonts from a local folder. By default, Apryse downloads fonts the internet if they aren't available in your local Meridian installation. This allows you to have access to all fonts Apryse provides, even if your environment restricts internet access.

1. In your web server, download the font package.
2. Extract the downloaded file to a subfolder, such as **Fonts**.

   We recommend the `C:\inetpub\AMM\Src\PDFTron` folder path.
3. Create a virtual directory in IIS for the folder that contains the font files.

   This directory must be accessible from the web. Use the **Anonymous Authentication** to allow access.
4. In IIS, add the following file extensions:
   - **.lzma** with MIME type **font/ttf**
   - **.brotli** with MIME type **font/ttf**
5. If your environment uses **CORS**, set the HTTP header **Access-Control-Allow-Origin** to *****.
6. In IIS Manager, go to **Default web site** > **Advanced settings**.
7. In **Enabled protocols**, select **HTTPS**.

   Do not use HTTP protocol. PDFTron forces HTTPS, even if HTTP is specified.
8. Open the Windows Registry Editor and go to:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Cyco\AutoManager Meridian\CurrentVersion\WebLink`
9. Add a **String** value named **PDFTronFontLocation**.
10. Set the registry value to the web location of the font files.

    For example, if your fonts are in `C:\inetpub\AMM\Src\PDFTron\Fonts`, the registry key value is **https://<YourPowerWebServer>/AMM/Src/PDFTron/Fonts**.

    You can also use a relative path if the virtual directory is under **Default web site** in IIS, such as **/PDFTronFonts**.

Configure Apryse / PDFTron Local Fonts in Explorer

Configure Meridian Explorer to use Apryse (formerly PDFTron) fonts from a local folder. By default, Apryse downloads fonts the internet if they aren't available in your local Meridian installation. This allows you to have access to all fonts Apryse provides, even if your environment restricts internet access.

1. In your web server, download the font package.
2. Extract the downloaded file to a subfolder, such as **Fonts**.

   We recommend the PDFTron subfolder, where the BCEnterprise IIS application is installed.
3. Create a virtual directory in IIS for the folder that contains the font files.

   This directory must be accessible from the web. Use the **Anonymous Authentication** to allow access.
4. In IIS, add the following file extensions:
   - **.lzma** with MIME type **font/ttf**
   - **.brotli** with MIME type **font/ttf**
5. If your environment uses **CORS**, set the HTTP header **Access-Control-Allow-Origin** to *****.
6. In Windows Explorer, go to `C:\ProgramData\BlueCieloECM\EnterpriseServices`.

   The disk location might vary according to installation.
7. Open the **PDFTronViewerSettings.dat** file.
8. Add the **PDFTronFontLocation** string setting.
9. Set the setting to the web location of the font files.

   For example, if your fonts are in `C:\inetpub\wwwroot\BCEnterprise\PDFTron\Fonts`, the setting value is **https://<MyExplorerWebServer>/BCEnterprise/PDFTron/Fonts**.

Configure Third-Party Identity Provider: Meridian-to-Okta

Configure a third-party identity provider (IdP) with OpenID Connect (OIDC) to activate secure authentication in Meridian. You integrate Okta to streamline sign-in across Meridian PowerWeb, Explorer, and Site Cache clients. This configuration helps centralize identity management, reduce repeated logins, and improve security.

Prerequisites

Your IT administrator must configure a new OIDC app integration in Okta to use this tool. If you need assistance with your implementation, reach out to your Accruent representative.

Meridian-to-Okta OIDC Configuration tool

Use this tool to set up integration between Meridian and Okta. This tool lets you activate or deactivate OIDC authentication for Meridian clients.

1. Open the **OktaConfigurator.exe** application at */Program Files/BC-Meridian/Program/OktaConfigurator*.
2. Enter the following information:
    - **Okta account URL**: The base URL of your Okta tenant.

      The integration automatically populates the **Authority**, **Token endpoint**, and **User info endpoint** fields.
3. Select **Confirm and continue**.
4. Select **Enable** or **Disable** to activate or deactivate third-party authentication in the following clients, then enter the following information:
    - **PowerWeb URL**:
        - **PowerWeb URL**: The URL of your PowerWeb environment.
        - **Client ID**: The unique identifier for the PowerWeb app in Okta.
        - **Client Secret**: The secret associated with the PowerWeb app in Okta.
    - **Explorer Client**:
        - **Explorer Client URL**: The URL of your Explorer environment.
        - **Client ID**: The unique identifier for the Explorer app in Okta.

- **Client Secret**: The secret associated with the Explorer app in Okta.

- **SiteCache URL**

5. When you select **OK**, Meridian updates the IIS configuration to use this authentication method in the clients you choose.

Windows Installer Package Custom Actions

The Windows Installer packages that are provided with Meridian Enterprise implement some custom actions in order to automate the installation processes. These custom actions are typically executables that the package starts to perform some action other than copying and registering files. The following tables list the custom actions that are performed by the Windows Installer packages developed by Accruent.

The custom actions that are performed by the 64-bit Meridian Enterprise server components package named `Accruent Server Components (x64).msi` are described in the following table.

Meridian Enterprise server components (x64) package custom actions

Name	Description	When	MSI Type	Properties
StopAMFS	Stops amfssvc service before replacing it with 64-bit version	Install \ Run	370 – runs `net.exe stop amfssvc`	NET
UnregAMFS	Unregisters 32-bit amfssvc service	Install \ Run	114 – runs `amfssvc.exe /remove`	AMFSSVCPATH
RegisterAMFS	Registers 64-bit amfssvc service	Install \ Run	1682 – runs `amfssvc.exe /install`	

The custom actions that are performed by the 32-bit and 64-bit Meridian Enterprise client component packages named `Accruent Meridian Enterprise (x64).msi` and `Accruent Meridian Enterprise.msi` are described in the following table.

Meridian Enterprise client component packages custom actions

Name	Description	When	MSI Type	Properties
AALR<*nn*>	Finds the name of a subkey in the AutoCAD registry branch	Install \ Run	163840 – uses custom `InstUtlM.dll`	PALR<*nn*>

Name	Description	When	MSI Type	Properties
AALR<*nn*>P	Finds the name of a subkey in the AutoCAD P&ID registry branch	Install \ Run	163840 – uses custom `InstUtlM.dll`	PALR<*nn*>P
StartHook	Starts `AMHookTrayU.exe` at the end of setup	Install \ Run	1746 – runs `AMHookTrayU.exe`	
StartHook64	Starts `AMHookTrayU.exe` at the end of setup	Install \ Run	1746 – runs `AMHookTray.exe`	
StartHookOnRollBack	Starts `AMHookTrayU.exe` at the end of setup	Rollback \ Run	1490 – runs `AMHookTrayU.exe`	
StartHookOnRollBack64	Starts x64 `AMHookTrayU.exe` at the end of setup	Rollback \ Run	1490 – runs `AMHookTrayU.exe`	
ReadOldInstallDir	Sets **INSTALLDIR** to the location of a previous x64 installation	Install \UI\ Run	291	INSTALLDIR OLDPATHNAME
ReadOldInstallDir32	Sets **INSTALLDIR32** to the location of a previous x32 installation	Install \UI\ Run	291	INSTALLDIR32 OLDPATHNAME
TerminateHook	Closes `AMHookTrayU.exe` at the beginning of setup to avoid FileInUse messages	Install \UI\ Run	131200 – uses custom `InstUtlM.dll`	

SQL Azure Database Creation Script

As of the 2022 release, SQL Azure is supported as a database provider for Meridian Enterprise Server. However, there are a few limitations to this support:

- We only support Azure virtual machines (VMs).
- The setup script should only be used with a fresh installation of Enterprise Server. Any existing configuration will be overwritten or will not be functional anymore.

This script creates configuration and Explorer databases in Azure SQL server and configures your Meridian installation to use Azure databases. You also have the option to create a new Azure resource group and SQL server.

If you decide not to use this option, your existing group or server will be used. The databases will be created with a performance level of **S0**, but you can scale up your databases to another size later.

After setup is complete, you can use the **CreateRepository** script switch to create a new Explorer repository.

Prerequisites

The following requirements must be met to successfully use this script.

- **PowerShell 5.1** or higher is required, but we recommend using **PowerShell 7**
- **Az** and **SqlServer** PowerShell modules

  If you run the script, it will detect if the modules are not available.

Required script files

The following script files can be found in `C:\Program Files\BC-Meridian\Enterprise Server\AzureSql` after installing Meridian:

- **AzSqlConfig.json**: Configuration file in JSON format

  This is a sample configuration file. You are not required to use this specific file.
- **AzureSqlSetup.ps1**: PowerShell script
- **CreateExplorerDb.sql**: Explorer Repository SQL script

Configuration file settings

The following parameters can be defined in the configuration file.

Configuration file settings

Parameter	Definition
subscriptionId	Subscription ID for the Azure SQL server ($subscriptionId = $config.AzSql.subscriptionId)
location	Location of the Azure SQL server ($location = $config.AzSql.location)
resourceGroupName	Resource group name of the Azure SQL server ($resourceGroupName = $config.AzSql.resourceGroupName)
sqlServerName	SQL Server name
startIp	Starting IP address of the Azure SQL server ($startIp = $config.AzSql.startIp)
endIp	Ending IP address of the Azure SQL server ($endIp = $config.AzSql.endIp)
SqlLogin	The SQL Server account username you want to use
configDatabaseName	Configuration database name
repoDatabaseName	Explorer repository database name
explorerRepositoryName	Explorer repository display name
serverDnsName	Server DNS name for public URL of Hyperion. If empty, the Server FQDN name will be used.

Script arguments

The following switches and arguments can be used in the **AzureSqlSetup** Powershell script.

Switches

- `SetupAzSql`: Used to set up Azure SQL
- `CreateRepository`: Used to create a new Explorer repository

Arguments

- `ConfigFile`: Required. This is the path to the configuration file.
- `CreateResGroup`: Optional, used to create a resource group. This is set to **yes** by default.
- `CreateSqlSever`: Optional, used to create a SQL server. This is set to **yes** by default.

Example argument 1

This example sets up Azure SQL using an existing resource group and creates a new SQL server if one does not exist.

```
.\AzureSqlSetup.ps1 -SetupAzSql -ConfigFile  AzSqlConfig.json false
```

Example argument 2

This example creates a new Explorer repository.

```
.\AzureSqlSetup.ps1 -CreateRepository -ConfigFile  AzSqlConfig.json
```

Procedures

To implement this configuration:

1. Navigate to `C:\Program Files\BC-Meridian\Enterprise Server\AzureSql`.
2. Extract the files to a folder on your Meridian Enterprise Server.

   The location you extract to is not important, but you will need to navigate to this location in PowerShell later. In our case, we extracted the files to a sub-folder in our C drive.
3. Open **AzSqlConfig.json** in any editor.
4. Refer to the *Configuration file settings* table above and define your configuration settings.
5. Save your changes.
6. Run PowerShell as an Administrator.
7. Navigate to the folder where you extracted the script files.
8. Run **AzureSqlSetup.ps1** using the `SetupAzSql` script argument defined in the *Script arguments* section above.

   You are prompted to sign in to Azure.
9. Sign in to your Azure account.

   Once you are successfully signed in, you are presented with a setup configuration summary.
10. Check the summary to ensure your settings are properly configured.
11. Type **Yes** and press **Enter** on your keyboard to continue.

    If you want to change your configuration settings, type **No** instead.

12. Type the password you want to use for your SQL account, and then press **Enter** on your keyboard.

    Make sure to use a password you will remember, or store it in a safe location, such as your organization's password manager application.

    The script executes. It may take some time to complete. Do not close the application.

    When the script is successful, it will return the message, "Azure SQL Setup finished."

13. Run **AzureSqlSetup.ps1** using the `CreateRepository` script argument defined in the *Script arguments* section above.

    You are prompted to sign in to Azure.

14. Sign in to your Azure account.

    Once you are successfully signed in, you are presented with a setup configuration summary.

15. Check the summary to ensure your settings are properly configured.

16. Type **Yes** and press **Enter** on your keyboard to continue.

    If you want to change your configuration settings, type **No** instead.

17. Enter the password for your SQL account.

    The script executes. It may take some time to complete. Do not close the application.

    When the script is successful, it will return the message, "Script done".

Troubleshooting

The following scenarios may occur when attempting to implement SQL Azure.

- When trying to install a PowerShell module, the following error might occur: “No match was found for the specified search criteria and module name…”

  To resolve this issue, specify TLS 1.2 for the .NET security protocol using the following command:

  ```
  [Net.ServicePointManager]::SecurityProtocol =
  [Net.SecurityProtocolType]::Tls12
  ```

- The SQL statement **Invoke-Sqlcmd** might fail with the following error: “A parameter cannot be found that matches parameter name ‘ConnectionString'“

  This happens when an old SQL module is installed (SQLPS). To resolve this issue, install the new **SqlServer** module with **-AllowClobber** option enabled:

  ```
  Install-Module -Name SqlServer -AllowClobber
  ```

SQL Server Database Creation Script

If your account on the Meridian Enterprise Server server does not have sufficient privileges to create a new database on the database server as described in Create a Meridian Explorer Repository, you can create the repository database with the following script.

> **Important!**
> Do not use this script to create a Meridian Enterprise vault database. This script is for creating Meridian Explorer repositories only. The database structures for vaults and for Meridian Explorer repositories are different. Instead, create the database as described in *Creating the vault database manually* in the *Meridian Enterprise Administrator's Guide*.

This script does not create a FILESTREAM file group. If you intend to use that feature for the repository, the file group must be configured manually.

To create a Meridian Enterprise Server configuration database manually, simply create a new database with the default parameters.

Create a Meridian Explorer Repository Database on the Database Server

To create a Meridian Explorer repository database on the database server:

1. In SQL Server Management Studio, run the following T-SQL script to create an empty database with the required file groups.
2. Change every occurrence of the text ***<DatabaseName>*** in the following script to the desired database name.
3. Edit the path specified for each of the **filename** parameters to refer to the correct locations.

```
USE [master]
GO
CREATE DATABASE [<DatabaseName>] ON PRIMARY
( NAME = N'<DatabaseName>', filename = N'C:\TEMP\<DatabaseName>.mdf'
,
MAXSIZE = UNLIMITED, FILEGROWTH = 1024KB ), FILEGROUP [CONTENT]
( NAME = N'<DatabaseName>_content', filename =
N'C:\TEMP\<DatabaseName>_CONTENT.ndf' ,
MAXSIZE = UNLIMITED, FILEGROWTH = 1024KB ), FILEGROUP [INDEXES]
( NAME = N'<DatabaseName>_indexes', filename =
N'C:\TEMP\<DatabaseName>_INDEXES.ndf' ,
MAXSIZE = UNLIMITED, FILEGROWTH = 1024KB )
LOG ON
( NAME = N'<DatabaseName>_log', filename = N'C:\TEMP\<DatabaseName>_
```

```
Log.ldf' ,
SIZE = 1024KB , MAXSIZE = 2048GB , FILEGROWTH = 10%)
GO
EXEC dbo.sp_dbcmptlevel @dbname=N'<DatabaseName>', @new_cmptlevel=100
GO
EXEC [<DatabaseName>].[dbo].[sp_fulltext_database] @action = 'enable'
GO
ALTER DATABASE [<DatabaseName>] SET ANSI_NULL_DEFAULT OFF
GO
ALTER DATABASE [<DatabaseName>] SET ANSI_NULLS OFF
GO
ALTER DATABASE [<DatabaseName>] SET ANSI_PADDING ON
GO
ALTER DATABASE [<DatabaseName>] SET ANSI_WARNINGS OFF
GO
ALTER DATABASE [<DatabaseName>] SET ARITHABORT OFF
GO
ALTER DATABASE [<DatabaseName>] SET AUTO_CLOSE OFF
GO
ALTER DATABASE [<DatabaseName>] SET AUTO_CREATE_STATISTICS ON
GO
ALTER DATABASE [<DatabaseName>] SET AUTO_SHRINK OFF
GO
ALTER DATABASE [<DatabaseName>] SET AUTO_UPDATE_STATISTICS ON
GO
ALTER DATABASE [<DatabaseName>] SET CURSOR_CLOSE_ON_COMMIT OFF
GO
ALTER DATABASE [<DatabaseName>] SET CURSOR_DEFAULT  GLOBAL
GO
ALTER DATABASE [<DatabaseName>] SET CONCAT_NULL_YIELDS_NULL OFF
GO
ALTER DATABASE [<DatabaseName>] SET NUMERIC_ROUNDABORT OFF
GO
ALTER DATABASE [<DatabaseName>] SET QUOTED_IDENTIFIER OFF
GO
ALTER DATABASE [<DatabaseName>] SET RECURSIVE_TRIGGERS OFF
GO
ALTER DATABASE [<DatabaseName>] SET ENABLE_BROKER
GO
ALTER DATABASE [<DatabaseName>] SET AUTO_UPDATE_STATISTICS_ASYNC OFF
GO
ALTER DATABASE [<DatabaseName>] SET DATE_CORRELATION_OPTIMIZATION OFF
GO
ALTER DATABASE [<DatabaseName>] SET TRUSTWORTHY OFF
GO
ALTER DATABASE [<DatabaseName>] SET ALLOW_SNAPSHOT_ISOLATION OFF
GO
ALTER DATABASE [<DatabaseName>] SET PARAMETERIZATION SIMPLE
GO
ALTER DATABASE [<DatabaseName>] SET READ_WRITE
```

```
GO
ALTER DATABASE [<DatabaseName>] SET RECOVERY FULL
GO
ALTER DATABASE [<DatabaseName>] SET MULTI_USER
GO
ALTER DATABASE [<DatabaseName>] SET PAGE_VERIFY CHECKSUM
GO
ALTER DATABASE [<DatabaseName>] SET DB_CHAINING OFF
GO
ALTER DATABASE [<DatabaseName>] SET RECOVERY FULL
```

Oracle Database Creation Script

If your account on the Meridian Enterprise Server server does not have sufficient privileges to create a new database on the database server as described in Create a Meridian Explorer Repository, you can create a Meridian Explorer repository database or a Meridian Enterprise Server configuration database with the following script.

> **Important!**
> Do not attempt to use this script to create a Meridian Enterprise vault database. The database structure of vaults is different.

Create a Meridian Explorer Repository Database

To create a Meridian Explorer repository database or a Meridian Enterprise Server configuration database on the database server:

1. In SQLPlus, run the following PL-SQL script.
2. Change <*UserName*> and <*Password*> to the desired user name and password respectively.

```
DEFINE UserName = "<UserName>"
DEFINE Password = "<Password>"
------------------------------------------------------------------------
-----------
CREATE USER &UserName IDENTIFIED BY &Password
ACCOUNT UNLOCK
– DEFAULT TABLESPACE "USERS"
– TEMPORARY TABLESPACE "TEMP"
– PROFILE "DEFAULT";
GRANT RESOURCE, CREATE SESSION TO &UserName; – required for Oracle 11
(nnk)
GRANT RESOURCE, CONNECT TO &UserName;
GRANT EXECUTE ON CTX_DDL TO &UserName;
GRANT CREATE VIEW TO &UserName;
GRANT ALTER ANY TABLE TO &UserName;
GRANT CREATE PROCEDURE TO &UserName;
GRANT CREATE TRIGGER TO &UserName;
GRANT CREATE UNLIMITED TABLESPACE TO &UserName;
– ALTER USER &UserName QUOTA 100M ON USERS;
--GRANT EXECUTE ON "CTXSYS"."CTX_DDL" TO "&UserName";
```

Windows Event Log IDs

Various Meridian Enterprise components log events in the Windows application and service event logs. These can be of any of the three supported event types: **Information**, **Warning**, or **Error**. The ID of the event can be used to determine the cause of the event and whether action needs to be taken to prevent the event from occurring.

The following table lists the event log IDs for the **Warning** and **Error** events from Meridian Enterprise sources. The **Information**-level events can be safely ignored.

Windows event log IDs

Category	ID	Level	Description or example error message shown
AutoManager EDM Server	6	Warning	This vault must be upgraded to the new version by your System Administrator.
AutoManager EDM Server	256	**Error**	Rare event generated only if updating the data version number fails during a vault upgrade.
AutoManager EDM Server	257	**Error**	Could not read User Database settings. Error code is 0x80070003.
AutoManager EDM Server	258	**Error**	Could not start User Database using this connection string 'C:\BC-Meridian Vaults\ICUserDB.SDF'. Error code is 0x80004005
Hypertrieve and **HyperCache**	257	**Error**	Load failed (124) C:\BC-Meridian Vaults\<VaultName>\<VaultName>.HDB
Hypertrieve and **HyperCache**	258	Warning	Low cache size on (0) C:\BC-Meridian Vaults*<VaultName>**<VaultName>*.hdb. Cache size 100MB is less than 25% of database size (1142MB). Performance may be degraded.

Category	ID	Level	Description or example error message shown
AutoManager OML	4	**Error**	Behavior BlueCieloECM.UIBehNet.Register failed to register; Cannot find class dependency 'UIBeh.Register' for 'BlueCieloECM.UIBehNet.Register'.
AutoManager OML	5	Warning	No more licenses available
AutoManager OML	256	**Error**	Generated when an invalid user account name is used or a disk full condition is suspected by the stream server.
AutoManager OML	258	Warning	Generated when an upgrade of security fails for very old vaults.
IC Meridian Object Manager	256	**Error**	Last error reported by the database engine, for example: • Exception in calling database engine. • Unexpected error in database engine. • The clock on the server has gained more than 7 days since the last time the EDM Server was active. Please contact your administrator to verify the time on the server. • Incorrect log version
AutoManager License Server	108	**Error**	**Compromised claimed licenses storage integrity.** This error means the claimed license file is corrupt.
AutoManager License Server	109	**Error**	**Invalid license file data.** This error means the license database file contains invalid data.
AutoManager License Server	110	**Error**	**Invalid claimed licenses storage data.** This error means the claimed license file contains invalid data.
AutoManager License Server	111	**Error**	**Missing claimed license storage.** This error means the claimed license file is missing.

Category	ID	Level	Description or example error message shown
AutoManager License Server	113	**Error**	**The License Server has expired.** This error means the license server version has expired or the license registration period has expired.
AutoManager License Server	115	Warning	**All licenses *<LicenseName>* in use.** This warning means there were no more of the specified licenses available to grant a request.
AutoManager License Server	116	**Error**	**Failed to create license database file.** This error means the license database file could not be created.
AutoManager License Server	117	**Error**	**Missing registry value.** This error means the a registry value that is required by the license server could not be found.
AutoManager License Server	118	**Error**	**License database file contains license[s] from later releases. Please upgrade license server.** This error means that licenses have been registered in the license server that were issued for a later version of Meridian software.
AutoManager License Server	120	**Error**	**Failed to read license database file.** This error means the license database file was found but could not be read.
AutoManager License Server	121	**Error**	**License request from later releases are not supported. Please upgrade license server.** This error means that a license was requested by a Meridian client application that is a later version than the license server.
AutoManager License Server	122	**Error**	**OS timer initialization failed.** This error means that an attempt by the license server to initialize an operating system timer failed.
AutoManager License Server	123	**Error**	**Failed to claim persisted licenses.** This error means that named licenses could not be claimed during startup.
AutoManager License Server	125	**Error**	**The BCLicense.exe file is corrupted.** This error means the license server executable file is corrupted.
HTSQLIO and **HTORAIO**	1	Warning	Connection to SQL server failed after 3 retries. Connection failure.

Category	ID	Level	Description or example error message shown
HTSQLIO and **HTORAIO**	2	Warning	Connection to SQL server required 2 retries.
AMTaskServer	0	Warning	A *<ErrorCode>* error occurred on an attempt to connect as user *<UserAccount>*. Reason: *<ErrorDescription>.* Execution of task *<TaskName>* failed. Reason: *<ErrorDescription>.*
AMTaskServer	0	**Error**	An error *<ErrorCode>* occurred in *<ErrorSource>* while processing the task *<TaskName>*. Reason: *<ErrorDescription>*.. A *<ErrorCode>* error occurred while processing the task *<TaskName>*. Reason: *<ErrorDescription>*.. A *<ErrorCode>* error occurred in *<ErrorSource>* while submitting a task of *<TaskName>* type provided by user *<UserAccount>*, as *<TaskFileName>*. A *<ErrorCode>* error occurred in *<ErrorSource>* while submitting a task of *<TaskName>* type provided by user *<UserAccount>*. Reason: *<ErrorDescription>*..

Service Account Usage

There are many locations where a dedicated service account can be used in Meridian Enterprise and its related Accruent products. We recommend that you specify the same account for all of the following that apply in your environment. The account can be set for many of these services by entering the account name when prompted during installation as described in Install the Server Components.

- Managing services, such as:
  - AutoManager EDM Server service in the **Services** control panel
  - AutoManager Task Server in the **Services** control panel
  - Accruent Meridian Services in the **Services** control panel
  - Accruent License Server in the **Services** control panel
- Dedicated Meridian user account to grant access to vault documents to Meridian PowerWeb and other systems
- Service Principal Name (SPN) described in Enable DCOM, if necessary
- Account used by Meridian for vaults hosted in Microsoft SQL Server as described in Configure the Windows Account Used By Meridian
- For activities related to Network Administration, such as:
  - Rescue account as described in Create a Rescue Account For Security Administration
  - Identity of the Accruent Meridian Services DCOM service as described in Configure the DCOM Identity Of Remote Services
  - Integration with an SMTP mail server as described in Specify a Mail Server
  - Meridian PowerWeb application pool as described in PowerWeb Server Privileges
  - Shared workspace synchronization as described in *Configure Shared Workspaces* in the *Meridian Enterprise Configuration Guide*
  - User group synchronization with Active Directory as described in Synchronize User Groups With Active Directory
  - Access to other Active Directory domains as described in Grant Membership Query Access
- For activities related to setting up vaults, such as:
  - Subscriptions and audit trail viewer application pool as described in Install the Subscriptions Viewer
  - Notifications table connection string as described in View and Edit Vault Properties

- Audit table connection string as described in View and Edit Vault Properties
- Scheduling vault backup and recovery tasks as described in Backups And Recovery
- Scheduling vault archiving as described in Run the Vault Archive Wizard
- Scheduling full-text content indexing as described in Configure Content Indexing

- Configuring data encryption as described in Software Data Encryption
- Vault data storage on SAN or NAS devices as described in Disk Subsystems
- Meridian Enterprise Server application pool as described in *Configure the Application Pool Account* in the *Meridian Enterprise Server Administrator's Guide*
- Meridian Explorer repository creation as described in Create a Meridian Explorer Repository
- For activities related to managing Publisher and publishing jobs, such as:
  - Account used to send publishing job notification messages as described in *Specify a Mail Server - Enterprise Server* in the *Meridian Enterprise Server Administrator's Guide*
  - Account used by Meridian to register rendition publishing tasks as described in *Register Documents For Publication* in the *Meridian Enterprise Server Administrator's Guide*
  - Publishing job metadata storage as described in *Configure a Publishing Job* in the *Meridian Enterprise Server Administrator's Guide*
  - Scheduling Publisher jobs as described in *Schedule Publishing Jobs* in the *Meridian Enterprise Server Administrator's Guide*
  - Account used by Publisher to publish documents to or from Meridian Project Portal as described in *Accruent Project Portal System Link* in the *Meridian Enterprise Server Administrator's Guide*
  - Account used by Publisher to publish documents to or from SharePoint as described in SharePoint System Link the *Meridian Enterprise Server Administrator's Guide*
  - Account used to run the Accruent File Publishing Service as described in *Configure the Accruent File Publishing Service* in the *Meridian Enterprise Server Administrator's Guide*
  - Account used to run the Meridian Project Portal Publishing Service as described in *Configure the Accruent Project Portal Publishing Service* in the *Meridian Enterprise Server Administrator's Guide*

Renditions Updater Tool

When you move from using AutoViewer to using PDFTron, if you want to see previous renditions of your documents you must create those renditions. As of 2021 R2, you can use the **Renditions Updater** tool, which allows you to generate these renditions in bulk.

When you use this tool, the rendition settings from the current version of the document are applied to all previous renditions of the document. In the 2022 release, the latest released revision of a document will be added to the queue if the document is in a workflow.

Renditions created using this tool are not visible in the native PowerUser viewer, they are visible only in the PowerWeb and Explorer clients. However, if you use a 3rd-party viewer, you can view renditions in PowerUser.

Important!

We recommend that you generate an updated rendition of the current version prior to running the renditions updater. The reason we recommend this is because our best practice recommendation is to have a different rendition job for historical versions of your documents.

When the current document revision is in a workflow and its rendition is not up to date, you cannot generate prior renditions using the Renditions Updater. For this reason, we recommend you only generate renditions for documents that are not currently in a workflow, or update the rendition of the current revision using the **Update Rendition** command or the **Document.UpdateRendition** method in script.

To learn about the **Update Rendition** command, see the *Update Renditions* article in the *Meridian Enterprise User's Guide*. To learn about the **Document.UpdateRendition** method, see the *Document Object Methods* article in the *Meridian Enterprise VBScript API Reference Guide*.

Use the Tool

To change an existing mapping, click the **Edit Map** button. If you want to clear the settings for a mapping, click the **Unmap jobs** button.

To use the updater tool:

1. Navigate to **C:** > **Program Files** > **BC-Meridian** > **Program**.
2. Double-click **RenditionsUpdater.exe**.

   The **Renditions Updater** tool opens.
3. Click the **Select** button to the right of the **Target Vault** field.
4. Select the vault you want to work with.

In the next step, you can choose between two options: you can select a collection or use a wildcard. Selecting a collection allows you to generate renditions for a specific subset of your documents, while using a wildcard will generate renditions for all documents in the vault that match your criteria.

5. Choose between two options:
   - To generate renditions for documents in a dynamic shared collection:
     a. Click the **Select** button to the right of the **Collections** field.
     b. Select the collection you want to generate renditions for.
   - Enter the type of documents you want to map in the **Wildcards** field.

     Enter each document type using the following syntax: ***[file extension]**. If you want to enter more than one document type, separate the document types with semicolons. For example, if you wanted to map Microsoft Word documents and CAD drawings, you would enter ***.docx;*.dwg** .
6. Click the **Map Jobs** button to the right of the **Wildcards** field.

   A **Job Mapping** window opens. The collections or wildcards you selected in step 5 appear as line items in the window.
7. Select the item you want to map from the top pane.
8. Select the rendition job you want to use for this item from the drop-down menu.

   Our best practice recommendation is to create a rendition job which is configured to not raise script events in Meridian, and then include that job name in your mapping. If you do not do this, you run the risk of triggering events which might not be applicable to historical versions of the document.

   To learn how to configure this setting, see the *Configuring the Publishing Options* article in the *Meridian Enterprise Server Administrator's Guide*.
9. Click the **Select** button.
10. Repeat steps 7-9 for each collection or wildcard.
11. Click **OK**.

    To change an existing mapping, click the **Edit Map** button. If you want to clear the settings for a mapping, click the **Unmap jobs** button.
12. Enter the number of items per job you want to process in the **Items per job** field.
13. Choose between two options:
    - Select the **Wait for job completion** check box.

      This check box will create a job in the Publisher for the first batch of renditions, but it will not create the next batch until the first batch has been processed.

- Clear the **Wait for job completion** check box.

  Clearing the check box will tell the tool to create all Publisher jobs immediately. This may decrease the performance of the server. Other users of the system may be affected.

14. If you want to modify where the log file is stored for the renditions updater, change the path in the **Log file path** field.
15. Choose between two options:
    - If you want to *append* new logging data for the renditions updater to the previous log, select the **Merge logs** field.
    - If you want to *overwrite* the previous logging data for the renditions updater, clear the **Merge logs** field.
16. Click the **Start** button.

Use Command-Line Options

These settings cannot be modified in the command line, but they are still applicable:

- The **items per job** is set to **20**
- The **wait for job completion** setting is set to **true**

To use the renditions updater tool with command-line options:

1. Navigate to **C:** > **Program Files** > **BC-Meridian** > **Program**.
2. Open a Windows Command Prompt.
3. Type **RenditionsUpdater.exe** into the command prompt window, and then add one or more of the following arguments.

   If there is a space in a parameter, put the parameter in quotation marks.

   - **v-<Vault Name>**: Vault name of the vault where you want to create missed renditions. You can omit this parameter if:
     - the vault name matches the datastore name AND
     - you include the datastore name in your argument.
   - **d-<Datastore Name>**: Datastore name of the vault where you want to create missed renditions. You can omit this parameter if:
     - the datastore name matches the vault name AND
     - you include the vault name in your argument.
   - **m-<Machine Name>**: Name of the machine with EDM Server that serves the vault.

- **j-<Job Name>** (Optional): Name of the rendition job you want to use to create missed renditions. Use this parameter if you want to use a rendition job that is different than the default Publisher rendition job.

  Our best practice recommendation is to create a rendition job which is configured to not raise script events in Meridian, and then include that job name in your mapping. If you do not do this, you run the risk of triggering events which might not be applicable to historical versions of the document.

  To learn how to configure this setting, see the *Configuring the Publishing Options* article in the *Meridian Enterprise Server Administrator's Guide*.
- **f-<File Name>**: Name of a file that contains a list of Meridian **Document IDs** that belong to documents that you want to check for missed renditions. You must include this parameter OR the Meridian Document ID parameter.
- **<Meridian Document ID>**: The **Document ID** of the document that you want to check for missed renditions. You can repeat the Document ID argument for as many documents as you need to process in the tool. You must include this parameter OR the file name parameter.
- **l-<Full File Path>** (Optional): The full file path for the log generated for the command. If the file path is invalid, a message is added to the log and the log is placed in the default location. For example:

  ```
  4/25/2022 12:07:52 PM [InfoWarning]: Invalid LOG path
  'C:\Program Files\BC-Meridian\Program\RenditionsUpdater.log'
  has been replaced with default
  'C:\Users\samantha.blackwood\AppData\Local\Meridian\Rendition
  sUpdater.log
  ```

- **l-** – If **l** is specified without a file path, logging is disabled. If **l** is not specified, the default logging path is used.

4. Once you have entered your command, press **Enter** on your keyboard.

   The command executes.

Here are some examples of valid command line arguments:

```
RenditionsUpdater.exe v-TestVault M-computer123 {CCDFABDC-F8ED-
11EA-0000-936CFB4D9868} {EF85EA0D-F8ED-11EA-0000-936CFB4D9868}

RenditionsUpdater.exe D-TestVault m-computer123 "j-Rendition Job
123" F-C:\Temp\DocumentList.txt

RenditionsUpdater.exe d-TestVault m-computer123 f-
C:\Temp\DocumentList.txt {CCDFABDC-F8ED-11EA-0000-936CFB4D9868}

RenditionsUpdater.exe v-"TestVault 2" M-QA-EDM {FF2CD8E1-0CBA-11EC-
0000-712D9406BDAA} l-"C:\Logs\Rend.log"
```

Glossary

A

Active Directory

A Microsoft directory service that provides central authentication and authorization services for Windows-based computers.

AMFS

The InnoCielo File System service that makes vaults available through the Windows file system.

approved

A workflow status that indicates that a document that has been approved for reproduction, distribution, manufacture, or construction.

archive

When used as a noun, a repository of obsolete documents kept for possible future reference. When used as a verb, the process of exporting obsolete documents from a repository.

assign to work area

The process of creating a copy of a document in a work area to isolate its changes from the original revision in the Main area.

attribute

When used to describe a file system, it is a property of a file such as Hidden, System, or Read Only. When used to describe an AutoCAD drawing, a named object in a drawing that is included in a block definition and used to store alphanumeric data.

audit log

A system-generated record of the date and time of user actions that create, modify, or delete critical business data.

audit trail

A system-generated record of the date and time of user actions that create, modify, or delete critical business data.

authorization key

The ten character hexadecimal code generated by BlueCielo ECM Solutions that authorizes a software license indefinintely. Authorization keys are generated based on

the license serial number, license key, and return key specific to each installation.

B

baseline

When used to describe Meridian Enterprise, a named moment in time in the history of a vault, such as a milestone.

Basic Authentication

A method designed to allow a web browser, or other client program, to provide credentials – in the form of a user name and password – when making a request from a server.

briefcase

An Accruent portable document package. A briefcase is a single file in an archive format that may contain multiple discrete documents. Briefcases may be in open standard formats such as ZIP and RAR, the Accruent BRC format, or custom formats. A briefcase may also contain document metadata in a data file and, in the Accruent BRC format, document redlines.

C

client

A computer, object, or program that obtains data or services from a server.

COM

Component Object Model - an interface standard for software componentry by Microsoft used to enable interprocess communication and dynamic object creation by programs.

content

The electronic data associated with a document.

content indexing

The process of extracting and indexing text data from documents for full-text searching. See also "full text search".

context

When used to describe Meridian Enterprise, a frame of reference comprised of a specific compartment of a vault and a moment in time for viewing the content of a vault.

criterion

A search filter condition comprised of a property name, operator, and value.

current

In general, the object that a user has selected or an object that is currently within the scope of a programming expression. When used to describe the history of a document, the latest revision of a document, which might not yet be released.

D

data source

An external data file or database that provides data that is presented by or imported into a Accruent system.

database

A structured set of document metadata used by a Accruent system. The database may be managed by Hypertrieve, SQL Server, or Oracle depending on the system.

DB

An Oracle database.

DCOM

Distributed Component Object Model - a Microsoft proprietary technology for software components distributed across several networked computers to communicate with each other.

derive

To create a new document based on an existing document. Also the name of a Meridian Enterprise command.

destination state

The state of a Meridian Enterprise workflow that follows a workflow transition.

details page

A type of property page that displays the properties of a document.

digital signature

A digitized image of a person's handwritten signature. See also "electronic signature".

discard

When used to describe Meridian Enterprise, to cancel the process of revising a document and delete the file copy that is being edited.

document

Information recorded on a medium (paper, digital media, and so on) for communication to others.

document controller
A person within a facility owner/operator organization that is responsible for the management of project documents.

document type
A classification of documents that share one or more document management characteristics such as format, purpose, or security.

document type workflow
A predetermined sequence of steps through which a document must be processed to generate a new approved revision in Meridian Enterprise. The workflow is defined by the document type from which the document was created.

document view
A view of a Meridian Explorer repository that displays documents.

document workflow interlock
A rule consisting of specific document types and property filters that limit when a project's workflow may proceed. Interlocks are configured by a System Administrator with the Meridian Enterprise Configurator application. Interlocks are available only with the Meridian Advanced Project Workflow Module.

domain controller
A server that responds to security authentication requests (logging in, checking permissions, and so on) within a Windows Server domain.

dynamic collection
A Meridian Enterprise saved search in which the search criteria are reevaluated and the results are updated whenever the collection is displayed.

E

e-signature
An electronic indication that a person adopts the contents of an electronic message. See also "digital signature".

ECM
Engineering Content Management. Content management as it applies specifically to engineering.

EDM
Engineering Document Management. Document management as it applies specifically to engineering documents.

effectivity

An attribute of a Meridian Enterprise property that determines when changes to its value apply within the life cycle of a document.

electronic signature

An electronic indication that a person adopts the contents of an electronic message. See also "digital signature".

environment

An organization's overall computing platform.

Explorer view

The view of a Meridian vault that displays documents organized within the Field-Path Relation.

external page

A type of property page that displays a web page that is hosted on a different information system.

F

Field-Path Relation

A hierarchical structure defined by properties that determines the folder structure of a vault and the locations of documents according to the values of the properties.

Folders view

The view of a Meridian Enterprise vault that displays documents organized by the vault's Field-Path definition.

FS

An acronym for file system.

full-text search

A method of searching for text contained in document content as opposed to searching document metadata. See also "content indexing."

G

grid view

Name of a Meridian Explorer view mode that displays search results in tabular format.

GUID

An acronym for Globally Unique Identifier.

H

history

A configurable option of a Meridian vault that causes it to save changes to documents and metadata over time. Allows users to view prior revisions of documents and their property values at specific moments in the past.

History mode

A configurable option of a Meridian vault that causes it to save changes to documents and metadata over time. Allows users to view prior revisions of documents and their property values at specific moments in the past.

HTTP

An acronym for Hypertext Transfer Protocol.

hybrid drawing

A drawing composed of both vector graphics and raster image files.

I

import

The process of creating a new file in a vault from a file outside the vault or repository .

inactive user

A user account that has been deactivated. The account is not deleted but the user cannot use the application. The account can be reactivated later.

initiate

The act of starting a new revision of a document by performing the first step of a workflow.

issue code

The name of a Meridian Transmittal Management Module property that stores a standard keyword or phrase. The issue code describes the reason why a transmittal was issued.

L

layout

A configurable arrangement of items on a form or page.

LDAP

An acronym for Lightweight Directory Access Protocol.

Local Workspace

A portion of disk space on a user's computer reserved for caching documents when they are viewed or edited. Using Local Workspace improves performance when working with very large documents. Meridian Enterprise's local workspaces can be synchronized with the vault at a configurable interval.

lookup list

A list of predetermined values for a property that is presented to the user for selection. Lookup lists can be either managed in the application or linked to an external database or query.

M

Main area

The area of a Meridian vault where released documents reside.

manager

The Meridian user who initiated the current document workflow and the only person with permission to change the current To-Do Person.

master document

In Meridian Enterprise, a released document from which one or more project copies are made that become either independent documents or new revisions of the master document. Master documents are designated by Meridian Enterprise and the Meridian Advanced Project Workflow Module. In Accruent Project Portal, a document to which a master file is attached.

Meridian Enterprise Server application server

The Meridian Enterprise Server data access and business services running on a server computer. May also be used to refer to the server hosting the services.

Meridian Explorer client

The Meridian Explorer application installed on the Meridian Enterprise Server web server.

metadata

Information that classifies, supplements, or describes a document. Metadata is commonly used to find documents as opposed to searching for data within documents (see “full-text search”). Metadata may also be used for a variety of other purposes.

N

NAT

An acronym for Network Address Translation.

Navigation view

A view of a Meridian vault that displays documents organized in a hierarchical structure according to a predefined set of properties.

O

OS

An acronym for operating system.

OU

An acronym for organizational unit.

P

package

A set of files that are used together for a common purpose. The files are often bound together in a single archive file for convenience when transporting, such as .zip and .msi files. Examples of file packages are software distribution packages and submittal packages. See also “briefcase.”

pane

A separate area of a split or single window used to display related data.

performance counter

Stores the count of specific program activities on a computer to conduct low-level performance analysis or tuning.

PowerUser

The Meridian desktop client software. Not related to the Windows administrative group Power Users.

PowerWeb

The Meridian Enterprise web browser-based client application.

preselection

A property filter that can be applied to a Meridian Explorer view to limit the number of visible items.

privilege

The right of a user to view specific data or execute a specific command. Privileges are assigned by a System Administrator.

project copy

A copy of a master document made for the purpose of creating a new independent document or creating a new revision of the master document. Project copies can be created in Meridian Enterprise.

project definition

A template used to create special folders in a vault that can represent design project processes. Project definitions are configured by a System Administrator with the Meridian Enterprise Configurator application. Meridian Advanced Project Workflow Module project definitions consist of a custom folder type, a workflow, and optional project workflow interlocks or document workflow interlocks. A project definition may restrict folders from being created at the root of a vault and may restrict creation of subprojects (Meridian Advanced Project Workflow Module only).

project folder

A folder created from a project definition template.

project workflow

The workflow of a project folder as defined by the project definition template from which it was created. Configured by a System Administrator with the Meridian Enterprise Configurator application.

project workflow interlock

A rule comprised of specific sub-project folder types and property filters that is applied to a project or subprojects that limits when a project's workflow may proceed. Interlocks are configured by a System Administrator with the Meridian Enterprise Configurator application. Interlocks are available only with the Meridian Advanced Project Workflow Module.

property

Descriptive data used to identify, classify, and find documents. Properties are organized into related groups called property sets.

property navigation

A dynamic search method in which a user progressively reduces the number of documents found by selecting from additional property values.

property page
A secondary window, usually displayed with a tab, that displays the properties of an object such as a document.

property set
A group of related properties.

publish
To create a copy of a document in another information system, optionally in a different electronic format.

purge
To completely and permanently delete data from a system.

Q

query
A search command comprised of one or more search criteria often expressed in Structured Query Language (SQL) syntax.

Quick Change
A very simple document workflow consisting of only two steps, Start Quick Change and Release Quick Change that may or may not increment the document's revision number depending on the configuration of the document type.

R

reassign
To immediately assign a document to the current work area for additional changes after discarding or releasing the current revision.

recovery log
The log of vault documents that can be executed in order to export the documents from a vault to a specified location on the file system. The recovery log is created for use in the event of a critical disaster to provide continued access to documents.

redline
Corrections to a drawing made graphically on a copy of the drawing. Redlines can be created for electronic drawings with the InnoCielo viewer by a user with the appropriate security privileges.

reference
A link that represents a relationship between two documents. References can be created automatically by Meridian (for example, AutoCAD External Reference) or manually by a user.

reference type
A classification of references that share one or more document management characteristics such as purpose, source or destination document types, or security.

references page
A type of property page that displays the references of a document.

related documents page
A type of property page that displays the documents that are related to the selected object.

related tags page
A type of property page that displays the asset tags that are related to the selected document.

release
The final step (transition) of a Meridian Enterprise workflow. When describing project workflow, refers to a new revision of a master document that was created from the content of a project copy. When describing document type or workflow definition workflows, refers to a new revision of the document that was created by completing the document's workflow.

render
Rendition (noun) refers to a copy of a document in a format other than the original. Render (verb) refers to the process of creating a rendition.

rendition
Rendition (noun) refers to a copy of a document in a format other than the original. Render (verb) refers to the process of creating a rendition.

repository
The largest logical container of a document management system for storing documents and metadata. A repository commonly contains all of the documents for a single organization, division, department, workgroup, or other purpose, organized into folders and sub-folders. The fundamental container of a Meridian Explorer system.

result grid
A configurable grid view used to display documents or tags found by a search.

retire
To classify a document as obsolete and prevent it from being revised.

return code
A standard keyword or phrase that represents the reason why a submittal was issued.

review
The process of evaluating the accuracy and completeness of revisions to a document.

revision
A milestone in a document's history that represents approved information at particular point in time identified by a number or letter.

revisions page
A type of property page that displays a list of the revisions of a document.

revoke
The act of canceling revision of a working copy of a document and deleting the copy being edited.

role
A named set of privileges to which users or groups are assigned by an administrator.

RPC
Acronym for Remote Procedure Call.

S

saved search
A user-defined set of search criteria that is saved for future reuse.

scope
A Meridian Enterprise feature that limits vault functionality and the visible information to named sets. A scope can be selected by users to make the system easier to use or to gain access to different documents.

search layout
A configurable combination of repository navigation and search filter parameters used by Meridian Explorer.

server
A centralized computer or application that provides services to one or more client computers or applications in a network.

shared workspace
A special folder in a Meridian Enterprise vault that is used to store files to support multi-user applications. The vault folder is mapped to a shared network location outside the vault that is used instead of local workspaces on the users' computers. Meridian Enterprise synchronizes the contents of the shared network location with the vault folder. Configurable options control other behaviors specific to using a shared workspace.

shortcut bar
The name of the accordion control containing shortcuts to views, vaults, and baselines that can be displayed in the left pane of the Meridian Enterprise desktop application.

SID
An acronym for System Identifier. A name that identifies a specific instance of a running Oracle database.

SMTP
An acronym for Simple Mail Transport Protocol.

snapshot
A read-only copy of metadata made so that slower data backup processes can occur while the application continues writing to its data. Backing up a snapshot minimizes maintenance downtime.

source state
The state of a workflow that precedes a workflow transition.

SSL
An acronym for Secure Sockets Layer or Transport Security Layer.

SSL/TLS
An acronym for Secure Sockets Layer or Transport Security Layer.

static collection
Saved search results that are displayed without reevaluating the search criteria.

sub-project
A Meridian Enterprise project folder contained within another project folder that can represent a subordinate process. Subprojects are available only with the Meridian Advanced Project Workflow Module.

submit
When used to describe a document, means to check in the working copy of a document that is under revision. Equivalent to releasing a document from a workflow.

submittal

A package of documents received by an organization for review, reference, modification, or final delivery.

T

tag

A vault or repository record that represents a logical asset stored in a separate maintenance management system. The logical asset represents a physical asset that is present at a facility that is managed with the maintenance management system. A tag may reference one or more documents, or the reverse.

tag type

The document type that is configured for use as asset tags.

thumbnail

A small preview image that is shown to assist the user in identifying a file.

TLS

An acronym for Secure Sockets Layer or Transport Security Layer.

To-Do List

The name of a navigation view in Meridian Enterprise.

transaction isolation

A property in a database system that defines how and when the changes made by one operation become visible to other concurrent operations.

transition conditions

Property value filters and logical expressions that are evaluated to determine the validity of a workflow transition to be executed by a user.

transition equivalence

The equality of a Meridian Enterprise transition in one document workflow to a transition in another document workflow. Transition equivalence makes it possible to execute a transition for one document in a batch of documents and have it also execute transitions in the other documents within the batch even if the transitions don’t have the same name, source state, or destination state. Configured by a System Administrator with the Meridian Enterprise Configurator application. Transition equivalence is available only with the Meridian Advanced Project Workflow Module.

transmittal sheet
A cover letter for a submittal that lists the names and other property values of the documents that are included in the submittal. It might also include comments about the status of the documents or the project, instructions to the recipient, and a date by which a response to the submittal is due back to the sender.

U

unretire
To reverse the effects of retiring a document so that it can be revised.

URL
An acronym for Uniform Resource Locator used to specify Internet and intranet addresses.

V

vault
A Meridian repository for storing documents related by organization, division, department, workgroup, or purpose.

VBScript
The Visual Basic scripting language (Visual Basic Scripting Edition).

version
A document derived or copied from another document of the same revision.

VPN
An acronym for Virtual Private Network.

W

WAN
An acronym for wide area network.

watermark
Textual or graphic information overlaid on a printed document used to indicate authenticity or validity.

Web Access
The Meridian Enterprise web browser-based client application.

web client
A client application that is presented in a web browser.

Work Isolation mode
The vault setting that defines how and when the changes made by one user become visible to other concurrent users.

workflow
A predetermined sequence of steps used to produce standardized results.

working copy
A temporary copy of a document made for making changes as an alternative to document workflow.

workstation
A personal computer used by an individual in a network. A workstation is the client in a client/server system.

X

X-Ref
An AutoCAD drawing that is linked to, but not inserted into, the current drawing. Changes made to referenced drawings (X-Refs) are automatically displayed in the current drawing when the current drawing is opened.

Index

A

accelerating
- access to cached data 329
- content index creation 299

access
- locked out 474
- privileges 443

accounts
- Oracle
  - configuring 402
  - EDM Server 401
- SQL Server
  - configuring 388
  - creating 386
- user accounts See *user accounts*

Accruent File System
- filters 222
- installing 45

Accruent Meridian Enterprise Developer Edition 110

Accruent SQLIO component 378-379

Acknowledge Current Server Time command 54

Active Directory
- domain privileges
  - to the server 449
  - with a service account 444
- mapping user properties 471
- multiple domains 455-456
- nested groups 454
- security problems 443
- synchronization parameters 470
- synchronizing users 467

ActiveX 57

administering
- networks 432
- user accounts 460

Administrator tool 167
- creating new vaults 172
- remote administration 479

ADSI management console 456

Advanced Vault Properties dialog 225

AMFS service (AutoManager File System)
- filters 222
- installing 45

AMRepU tool
- about 495
- create system status report 496
- review server configuration information 500

analyze
- vault database 224

antivirus applications 356

API
- installation 128

application
- Application Server
  - requirements 46
- backup & lock files 222
- event log 505

response option 319
Application Integration
about 111
Offline mode
disable 431
application links See *Application Integration*
architecture 26
client/server 26
content indexing service 30
data 38
data library 36
deploy for high availability 66
deployment strategies 63
document content service 31
EDM Server service 28
encrypted data 39
interprocess communication 35
license server service 29
optional modules 34
PowerWeb 32
archive
documents 286
Vault Archive Wizard
results 292
run the wizard 287
arguments
ADDLOCAL 100
audit log
about 189
audited actions 203
configuring connection 193
configuring viewer 197
creating database 191
installing viewer 195
localizing database 201
use Enterprise Server for the audit log 420
audit log database
creating 191
security 191
audit trail See *audit log*
authentication
PowerWeb on different server 122
authorization keys
enter 147
obtaining 144
register 145
AutoCAD
font files 354
Azure
database creation 713

B

background tasks
monitoring status of 257
backups
filter backup files created by application 222
preparation for 268
Meridian server and vault 225
Oracle vaults 399
SQL Server vaults 382
repository 261

restoring 271
vault backups 187, 263
bandwidth 55
batch
operations 328, 357
BC-Meridian Extensions folder 114
best practices
security role assignments 338
browsers
internet / intranet requirements 57
buffer, SQL Server 381

C

CAB files 495
cache
HyperCache
and Oracle 398
and SQL Server 381
size 177
CanPublish privileges 415
catalogs 295, 298
certificates, EFS 325
checklist
for application server installation 76
for configuring a site cache server 358
for configuring content indexing 293
for troubleshooting server 490
cidaemon.exe file 299
cisvc.exe file 299
Citrix Delivery Center 480
claiming
licenses 138
client components setup 92
client computers
minimum privileges 434
optimize performance 350
AutoCAD font files 354
multiple network protocols 352
multiple network providers 351
viewer refreshes 353
Client for Microsoft Networks 351
client licenses 138
client/server configuration 62
command line
create a recovery log 278
command-line arguments
and switches 98
silent client installation 95
system status report 496
upgrading installations 106
Windows Installer 96
commands
Acknowledge Current Server Time 54
Create Working Copy 172
Diagnostics 491
Download document 480
NET TIME 54
Submit Working Copy 172
committing
data changes 396
log files 264
compression, software disk 324

concurrent licenses 138
Configurator
role in Meridian Enterprise architecture 26
configure
antivirus applications 356
connection to Meridian Enterprise Server 418
content indexing 295
database settings 172
Event Viewer 492
Explorer synchronization jobs 254
jobs 254
Local Workspace 424
Meridian Enterprise application server 412
NetBIOS name resolution 458
Oracle accounts 402
Performance Monitor 493
ports 437
remote session support 480
SQL Server accounts 388
connection string
audit table 181, 193
notifications table
connect subscriptions database 181
create subscriptions database 185
open Audit Log Viewer outside of Meridian Enterprise 195
open Subscriptions Viewer outside of PowerUser 126
optimize batch operations 357
registry key
connect to Microsoft Access 543
connect to SQL Server Compact 542
user and group database file 547
repository 250, 254
service account usage 725
user accounts database
registry setting 547
Windows event errors
AutoManager EDM Server error 258 721
consistency, in vault databases 224
constants
AS_URL_FLAGS 693
content indexing 293
accelerating 299
configuring 295, 302
maintaining 298
restoring indexed vaults 301
troubleshooting 303
context indexing
service 30
counters
SQL Server performance 392
CPUs & system responsiveness 314
Create Recovery Log Wizard 278
Create Working Copy command 172
creating
Data Library 249
recovery logs 278
SQL Server accounts 386
system status reports 496

vaults 166, 172
web locations 232
CSV files 171
custom
properties
optimize performance 337

D

.dat files
ContentRepositories.dat 236
MRE2368.dat 253
noise.dat 300
PublishingCapability.dat
RetryWriteRendition 414
WaitWriteRendition 414
WebConfigDto.dat 440
data
caching in server memory 329
committing changes 396
encryption 325
synchronizing 421
Data Library 36
creating 249
creating and maintaining 248
database
connection licenses 138
engines
Azure 713
configuring 172
Hypertrieve 28, 171, 264
Oracle 28
SQL Server 28
supported 172
inconsistencies 224
settings 172
database recovery 264
Level 1 265
Level 2 266
Level 3 267
Database Wizard 250
DataStore.ini file
moving a Hypertrieve vault 242
preparing for backups 268
upgrading vaults to a newer database engine 118
date values 54**,** 705
DCOM protocol
allowing Web Acess 437
enabling 451
interprocess communication 35
multiple adapters 322
permissions 452
security 450
DCOMCNFG tool 437
debugging
enable VBScript logging
registry key settings 672
VBScript in PowerUser
registry key settings 672
VBScript in PowerWeb
registry key settings 672
demilitarized zone (DMZ) 436
department deployment model 71

deployment
models 67
department 71
enterprise 73
workgroup 68
strategies 63
Developer Edition 110
Developer tools 110
Diagnostics command 491
dialog boxes See *dialogs*
dialogs
Advanced Vault Properties 225
EDM Server Properties 327, 384
Local Workspace Options 603
New Account 463
New Email Address 463
New Filter 222
New Group 466
New Repository 250
Performance Options 319
QuickFind 591
Remove History 237
Select Computer 479
Select Users 466
SQL Server Login Properties 386
SQL Server Properties 225
System Properties 319
disabling
Offline mode 431
disaster recovery 278
disks
compression 324
space requirements 52, 379
subsystems 317
DLL files
<DatabaseEngine>SQL.dll 384
BlueCieloECM.Extensible.UI.dll 126
BlueCieloECM.InnoCielo.Meridian.dll 110
CommDlgDetect.dll 660
ht3.dll 118
ht3ora.dll 118
ht3sql.dll 118
ht5.dll 118
ht5ora.dll 118
ht5sql.dll 118
HTORAIO.dll 395
HTSQLIO.dll 378
InstUtlM.dll 711
InventorDetect.dll 660
MSOfficeDetect.dll 660
ObjectORA.dll 118
ObjectSet.dll 118
ObjectSetORA.dll 395
ObjectSetSQL.dll 327, 378
ObjectSQL.dll 118
removing shared 135
version mismatch 92
DMZ 436
Document Content Service 31
document types
security 339
documentation 123

documents
archiving 286-287
batch operations 328, 357
moving content files 245
Publish Document privilege 412
recovering 282
searching 293, 300
security 339
synchronizing Local Workspace documents 429
unlocking Local Workspace 427, 429
domain privileges
grant to the Meridian Server 449
grant with a service account 444
domains, multiple 455
grant membership query access 456
Download document command 480
driver, ORAIO (Oracle) 396
Drivers.txt file 500
dump files 407

E

EDM Server
account requirements for Oracle 401-402
configuring 327
DCOM protocol 35
enabling 54
functions 28
hardware configuration 45
install 86
Oracle account requirements 401
processes 26
properties 695
service accounts 444
toolbar buttons 169
EDM Server Properties dialog 327, 384
email
shortcuts to documents 693
email server 477
enabling
correct function of ActiveX controls 57
DCOM 451
EDM Server 54
Encrypting File System (EFS) 325
encryption 325
enterprise deployment model 73
environment variable RECOVERDIR 282
errors
rendition process log
no storage available 414
Windows event log 721
estimating server disk space 52
event logs 503
Application
configure filter 492
review 505
System 504
Event Viewer 492, 503
examining publishing jobs 259
excluding
properties in vault import 179
executable files
ADSyncUsers.exe 467, 470-471

AMCleanDSC.exe 532
AMDownload.exe 548
AMEDMW.exe 437, 490
amfssvc.exe 711
AMFTFilter.exe 293, 298, 301-302
AMHookTray.exe 102, 484, 486, 712
AMHookTrayU.exe 712
AMRecLog.exe 278
AMRep.exe 496
AMRepU.exe 496
AMRestor.exe 271
AMStmRec.exe 231
AMUpdateU.exe 107, 120
AMVltCons.exe 227
BCLicense.exe 723
BCP.exe 201
BCSharedFolderSync.exe 624
BCSyncUnlock.exe 429
BlueCieloECM.SdfToMdbConvertor.exe 117
BlueCieloECM.SiteCache.LwsClient.exe 358
cidaemon.exe 299
cisvc.exe 299
DAWebServiceTest.exe 91
dcomcnfg.exe 451-453
icosnlsver.exe 76
mtx.exe 437
net.exe 711
regsvr32.exe 695
RenditionsUpdater.exe 727
SAMLConfigurator.exe 488

executing
publishing jobs 255
Explorer
Data Library 37
jobs 254
exporting
document revisions 278, 282
external website pages
configuration
PowerWeb 550

F

files
AMRepU output 500
archive 286-287
AutoCAD font 354
DLL files See *DLL files*
dump 407
executable files See *executable files*
.dat files See *.dat files*
ipf.rules 438
ipnat.rules 439
LCK files (Hypertrieve) 171
LDF files (SQL Server log) 393
number per folder 335
recovered 231
shared DLL 135
stream 172
systems 38
temporary 222

types
CAB (compressed archive) 495
Hypertrieve (CSV, HDB, LCK, LOG, and SNP) 171
LDF (SQL Server log) 393
MET (vault configuration) 172
XML 700
FILESTREAM option 261
filtering
text noise 300
filters
file 222
toolbar 168
Find form (PowerWeb)
configuration 571
firewalls 437
folders
Backup 268
default structure 112
extensions 114
levels of 333-334
size of 335
font files
AutoCAD 354
full-text search
content indexing 293, 300

G

Global Assembly Cache 110, 403
groups
Active Directory 442
nested groups 454
toolbar 168

H

hardware requirements 83
HDB files (Hypertrieve) 171
high availability 66
High Performance Option (HPO)
physical memory 315
history
remove vault history 237
hosts, application 484
HyperCache 307
and Oracle 395
ORAIO 396
Vault Cache Memory 398
and SQL Server 378
monitor vault performance 392
Vault Cache Memory 381
configuring 310
HyperText Transfer protocol (HTTP) 35
Hypertrieve
database recovery 264-265
files 171
migrating vaults
to Oracle 406
to SQL Server 390
moving vaults 242
snapshots 264
Hyper-V 66

I

icosnlsver tool 274
iFilters 293
import
vaults
exclude existing property values 179
inconsistencies in vaults 224
indexing 293
accelerating 299
configuring 295, 302
filtering noise 300
maintaining 298
restoring indexed vault 301
initialization files
DataStore.ini 242, 268
ImportFilter.ini 179
initializing vaults 172
install
add components to existing install 121
checklist (server) 76
command-line arguments 96
components
to an existing installation 121
configuration 62, 92
deployment 63
Developer tools 110
optional components 100
Oracle 394
PowerWeb 122
preparation for 83
server components 84
server roles 50
silent setup 90, 95
SQL Server 377
Subscriptions Viewer 126
supplemental documentation 123
system requirements 44
Meridian clients 57
network requirements 55
prepare 83
uninstalling 135
upgrades 115
webhelp 124
Windows Installer package 96, 98
InstallShield vs. MSI 96
integrating
Meridian Enterprise Server with Meridian 411
international languages 61, 102
Internet Information Services (IIS)
and PowerWeb 32, 86
installation 122
user authentication 232
interprocess communication 35
invoking tasks from scripts 701
ipf.rules file 438
ipnat.rules file 439

L

language support 61, 102
levels of
recovery 265-267

License Server 29
deploy multiple 158
install 86
reserve licenses for remote access 482
run on different computer 459
licenses 137
authorization keys 147
monitoring usage 155
obtaining 144
reassigning named 157
registering 145
reregistering 29
reserving 148
restricting 151
special licenses 138
specify license server type 87
types of
concurrent 138
named 140
subscription 141
viewing current usage of 154
lists See also *lookup lists*
LM_Cyco.txt file 500
LM_services.txt file 500
Local Copy property 421
Local Workspace 421
configuring 424
path length 422
synchronizing and unlocking documents 429
unlocking documents 427
lock files, application 222
locked files 414
log files
event 503
Application 492, 505
System 504
Hypertrieve 171
Oracle 396
recovery 278
setup 111
SQL Server 393
transaction
configure 346, 348
database recovery 264-265, 399
Vault Consistency Wizard (VCW) 229
write-ahead 379
lookup lists See also *lists*
convert database to Access 117
rendition property set 414

M

maintaining
content indexing 298
vaults 166
managing
licenses 29
time zone settings 54
mapping
user properties to AD 471
membership query access 456

memory
caching 329, 342, 344
Oracle 398
SQL Server 381
management
Oracle 398
SQL server 381
settings 500
usage 315
Memory object 320
Meridian Enterprise
[Meridian.ShortName] Object Model See *objects*
installing 62
client components 92
modules
implementation of 34
licensing 138
Meridian Enterprise Server
configure connection to 418
integrate with Meridian 411
Meridian Task Server 694
MET files 172
metadata 38
archiving 286, 289
Data Library 36
methods
Reset 702-703
Set 702, 704
Submit 702, 705
User.HasPrivilege 415
Microsoft .NET Framework 47, 128
Microsoft Access
backup file containing lookup list data 268
convert external tables to 117
migrating Hypertrieve vaults
to Oracle 406
to SQL Server 390
minimizing SQL Server log file size 393
monitoring
background tasks 257
license usage 155
performance 493
SQL Server vault performance 392
vault status 187
moving
BC-Meridian Extensions folder 114
document content files 245
SQL Server vaults 391
vaults
Hypertrieve 242
MSI installer package 96
multi-homed computers 322
multiple
network adapters 322
network protocols for application server 323
network protocols for client computers 352
network providers 351
server deployment strategy 65
vault configurations 166

N

name resolution, NetBIOS 458
named licenses 140
reassign 157
nested groups 454
NET TIME command 54
NetBIOS name resolution 458
Network Time Protocol (NTP) 54
networks
administering 432
client computer privileges 434
PowerWeb server privileges 436
security requirements 433
server privileges 435
multiple adapters 322
multiple protocols 323
multiple providers 351
requirements 55
New Account dialog 463
New Email Address dialog 463
New Filter dialog 222
New Group dialog 466
New Repository dialog 250
New Web Location Wizard 232
noise blacklist 300
notifications
SMTP server 477

O

Object Model See *objects*
objects
Memory 320
Process 314
Task Object 702
Vault.Task 703
Offline and Online mode
Offline mode
disable 431
prerequisites 484, 486
OpenID Connect 488
operating systems
changing versions 274
optimizing
antivirus applications 356
batch operations 357
client computer performance 350
AutoCAD font files 354
multiple network protocols 352
multiple network providers 351
viewer refreshes 353
Local Workspace configuration 424
server hardware 311
CPU 314
dedicated server 312
disk subsystems 317
physical memory 315
virtualization software 313
server operating system 318
application response 319
multiple network adapters 322
multiple network protocols 323
software data encryption 325

software disk compression 324
virtual memory 320
server software 326
configure searching for global groups 330
dedicate one process to each vault 331
how many objects per user kept in memory 329
maximum number of actions allowed 328
system performance 306
vault configurations 332
custom properties 337
document type security 339
files per folder 335
folder levels 334
folder structure 333
multiple vaults 336
security role assignments 338
optional component installation 100
optional module licenses 138
Oracle
accounts 401-402
backups 399
Database Configuration Assistant 172
database creation script 720
HyperCache 395, 398
installation 394
installation requirements 84
migrating Hypertrieve vaults to 406
ORAIO driver 395-396
restoring vaults 407
ORAIO driver 395-396

P

page table entries (PTEs) 320
passwords 388**,** 402
path length 422
performance
and caching 421
and CPUs 314
bandwidth requirements 55
configuring 225, 306
counters 392
monitoring 493
optimizing in client computers 350
AutoCAD font files 354
multiple network protocols 352
multiple network providers 351
viewer refreshes 353
troubleshooting 490
tuning 341
vault configuration optimization 332
Performance Monitor
configuring 493
effects of the CPU 314
SQL Server vaults 392
Performance Options dialog 319
Permission for AMServerManagerAccount dialog 475
permissions See *privileges*
personal preferences See *preferences*
plug-ins 34

ports
configuring 437
PowerUser
configuring document shortcuts in emails 693
installation 111
running remotely 480
Subscriptions Viewer
requirements 126
PowerWeb 32
adding a location 234
allowing through firewall 437
configuration
colors and fonts 564
external domain only connections 236
external website pages 550
Find form 571
Quick Search 553
searches 553, 571
default user settings 109
enabling 232
IIS 437
installing 83, 86, 122
required user settings
ProfilesPath 553
stylesheets 564
TempPath 556
server privileges 436
set default user preferences 565
toolbar buttons 169
using Task Server with 701
preferences
PowerWeb
deploy standard preferences 565
Prepare for Backup Wizard 263, 268
Oracle vaults 399
SQL server vaults 382
preparing
for backup 268
about backups and recovery 263
Meridian server and vault 225
Oracle vaults 399
SQLServer vaults 382
preventing creation of application backup and lock files 222
privileges See also *security, roles*
access 443
advanced document properties 284
CanPublish 415
domain 449
grant with a service account 444
log on as batch job 383
minimum 434-435
PowerWeb server 436
Publish Document 412
process log
error
no storage available 414
Process object 314
processes
accelerate content index creation 299
dedicate to a vault 331
server processes 26

product codes 148
properties
date-based 54
excluding when importing a vault 179
Local Copy 421
searching
content indexing 293
protocols
DCOM
allow PowerWeb access through a firewall 437
configure permissions 452
interprocess communication 35
multiple network adapters 322
HTTP 35
multiple network 352
SMB 35
TCP/IP
interprocess communication 35
multiple network protocols 352
Publish Document privilege 412
Publisher 36
Data Library 37
vault settings 412
publishing
metadata 36
publishing jobs
default rendition job 414
examining 259
executing 255
performance 259
PublishingCapability.dat
RetryWriteRendition 414
WaitWriteRendition 414

Q

Quick Find
configuration 591
Quick Search
configuration
PowerWeb 553
quiet switch 98

R

RAID systems 317
reassigning named licenses 157
RECOVERDIR environment variable 282
recovery 263
document content files 231
documents 282
Hypertrieve databases 264
levels of 265-267
log files 278
prior revisions 284
refreshes, viewer 353
register
licenses in Administrator 145
named licenses 140
Registration Wizard 145
registry keys
client 575
server 508

windows 507
remote access
prepare the client computers 486
prepare the host computer 484
prepare the server 483
reserve licenses 482
remote administration 479
session support 480
remote site cache 358
rename
vaults 238
rendition jobs
conflict 414
rendition property set
lookup lists 414
renditions
retries 414
Renditions Updater tool 727
repair
vaults 227
reporting
from a repository 262
system status 495
reports
configuring with Data Library 36
repositories
backups 261
creating 250
reporting from 262
reregistering licenses 29
rescue account 474-475
reserving licenses 148
Reset method 702-703
resource usage 312
Restart After Restore From Backup Wizard 263, 271
Restart After Restore Wizard 271
restoring
vault backups 263
vaults 271
indexed vaults 301
Oracle vaults 407
retry rendition 414
reviewing server configuration information 500
revisions
recover prior revisions 284
Vault Archive Wizard
results 292
run 287
roles
about role-based security 461
relationship with Windows security 433

S

SAML Authentication
registry key setting 554
scanning
antivirus scans 356
scheduled tasks
backups 268
scripts
script files 95, 701-702

search
configuration
PowerWeb 553, 571
content indexing 293, 300
full-text search 293, 300
search results
inconsistent search results 303
no search results 303
security
accounts
Oracle 401-402
SQL Server 386, 388
audited actions 203
back door account 474
delegation 440
document type 339
domain privileges 444, 449
installation
checklist 76
Meridian Clients 57
network requirements 55
prepare 83
permissions and privileges
Active Directory 443
client computers 434
DCOM 452
Meridian server 435
PowerWeb server 436
Publisher 412
repositories
create a repository 250
requirements 433
rescue account 475
restrictions on DCOM 450, 452
roles 433, See also *privileges*
about 461
configure vault for Publisher 412
optimizing configuration 338
setup
content indexing 302
user administration 460, See also *user accounts; user groups*
accounts 462
groups 466
role-based security 461
use Enterprise Server for user management 419
security roles See also *privileges; security, roles*
Select Computer dialog 479
Select Users dialog 466
sequence numbers 340
server hardware
configuration 45
CPUs 314
dedicated 312
disk subsystems 317
optimizing 311
physical memory 315
reviewing configuration information 500
virtualization software 313
server privileges 435
server roles 50

server software 326
configure searching for global groups 330
dedicate one process to each vault 331
how many objects per user kept in memory 329
maximum number of actions allowed 328
servers
name requirements 45
optimizing operating system 318
Application response option 319
multiple network adapters 322
multiple network protocols 323
software data encryption 325
software disk compression 324
virtual memory 320
service account 725
services 26
content indexing 30
document content service 31
EDM Server 28, 38
license server 29
registry key settings
SamlISEDMAccount 554
Set method 702, 704
setup 62
client components 92
silent setup 95
Task Server 695
setup.iss file 95
shared
DLL files 135
silent client installation 95
silent server installation 90
Single Sign-On
OpenIDConnect 488
SAML 488
registry key setting 554
single-server deployment strategy 64
site cache See *remote site cache*
SMB protocol 35
SMTP server 477
snapshots 264, 346
SNP files (Hypertrieve) 171
software data encryption 325
software disk compression 324
SQL Azure
database creation 713
SQL Server
accounts
configure 388
create 386
Accruent SQLIO 379
backups 382
database creation script 717
importing vaults 391
installation requirements 84
Login Properties dialog 386
memory 381
migrating Hypertrieve vaults to 390
minimizing log file size 393
moving vaults 391

Properties dialog 225
support for 378
vault performance 392
SSO See *Single Sign-On*
stand-alone configuration 62
status
of vaults 187
Status dialog 257
storage space 52
Stream Recovery Wizard 224, 231
streams
data 38
files 172, 284
moving 245
Stream Recovery Wizard 231
Submit method 702, 705
Submit Working Copy command 172
subscription licenses 141
subscriptions database
create 185
setup permissions 185
Subscriptions Viewer
create subscriptions database 185
install 126
test 126
support information 495
switches 96, 98
synchronizing
data
in Local Workspace 421
Local Workspace documents 429
server time requirements 54
system
event log 504
page table 320
status reports 495-496
workload 312
System Properties dialog 319
system requirements
for Application Server 46
for installation 44
for Meridian clients 57
for optional modules 60
for the Task Server 697
network 55
server 45
software data encryption 325

T

Task Server
advantages/disadvantages 694
install 86
methods 702-705
setting up 695
system requirements 697
using with PowerWeb 701
tasks
file management 700
invoking from scripts 702
preventing creation of duplicate tasks 413
scheduled 268
TCP/IP protocol
interprocess communication 35

multiple network protocols
client computer 352
server operating system 323
technical support
about 25
limitations to support 115
templates
Data Library jobs 254
Explorer Synchronization jobs 254
text files 500
time settings 54
title blocks
disable title block update 668
required optional component for DWG 100
Sync Properties to File command 669
updating
over Citrix remote access connection 668
toolbar buttons (Administrator)
common 168
EDM Server 169
Filters 170
Groups 170
PowerWeb 169
Users 170
tools
Administrator 167, 172, 479
AMRepU
about 495
create system status report 496
review server configuration
information 500
BCSyncUnlock 429
Renditions Updater tool 727
transaction logs 399
troubleshooting
checklist 490
content indexing 303
Diagnostics command 491
typical client setup 92

U

unlocking
Local Workspace documents 427, 429
Upgrade Vault Wizard 116
upgrading
client computers
automatically 120
existing installations 106
Meridian 115
vaults
by editing windows registry 118
during restore from backup 118
to newer database engine 118
URLs
shortcuts
in email 693
user accounts See also *security, user administration*
create 462
edit 462

user groups See also *security, user administration*
Active Directory
command line parameters 470
map user properties and groups 471
synchronize user groups 467
create and edit 466
user preferences
PowerWeb
set default 565
User.HasPrivilege method 415
users
accounts 460, 466, 701
default PowerWeb settings 109
groups 466
mapping AD properties 471
required permissions
client computers 434
Meridian security requirements 433
Meridian server 435
PowerWeb 553, 556, 564
PowerWeb server 436
synchronizing with Active Directory 467
toolbar buttons 170

V

vault
access problems 458
backups 187, 263
SQL server vaults 382
cache 225
Oracle 398
SQL Server 381
configuring 412
consistency 224
creating 166, 172
disabling 247
disk space requirements 52
editing properties 181
folder structure 38
importing
exclude existing property values 179
move SQL Server vault 391
initializing 172
locations 232
maintaining 166
migrating Hypertrieve
to Oracle 406
to SQL Server 390
monitoring status of 187
moving 240
Hypertrieve vault 242
SQL Server vault 391
multiple configurations 166
optimizing configuration 332
document type security 339
files per folder 335
folder levels 334
folder structure 333
multiple vaults 336
security role assignments 338
path length 422
performance 341
maximum log size 346

maximum server memory used for vault cache 344
memory caching 342
minimum snapshot interval 348
removing history 237
renaming 238
repairing 227
restoring
move a Hypertrieve vault 242
Oracle vault to another server 407
vault backups 263
security
grant domain privileges to Meridian Server 449
grant domain privileges with a service account 444
problems with Active Directory 443
problems with DCOM 450
settings See *vault settings*
upgrading
newer database engine 118
procedures 116
Vault Archive Wizard
results 292
run the wizard 287
Vault Consistency Wizard (VCW)
logs 229
prepare 225
run 227
toolkit 224
Vault.Task object 703
Vault Archive Wizard 286
results 292
run the wizard 287
Vault Consistency Toolkit 224
Vault Consistency Wizard (VCW)
logs 229
prepare 225
run 227
toolkit 224
vault settings
Enterprise Server 412
Publisher 412
Vault.Task object 703
VBScript
debugging
registry key settings 672
VBScript Objects See *objects*
VCW See *Vault Consistency Wizard (VCW)*
viewer
refreshes 353
virtual directories 551, 707-708
virtual memory 320
virtualization software 313
viruses 356
Visual Basic samples 110
VMware 66, 313

W

Web Access See *PowerWeb*
Web Client 92, 115
web locations for vaults 232

web services
Accruent web service 687
web.config file
API service test install 128
Audit Log Viewer
configure columns 198
open outside of Meridian Enterprise 195
Subscriptions Viewer
open outside of PowerUser 126
webhelp
installing 124
Windows
domain global groups 442
domains 55, 455
event log IDs 721
Event Viewer 492
Indexing Service 293
configuration 295
maintaining an index 298
noise blacklist 300
restoring an indexed vault 301
security 302
Installer package 96
command line switches 98
custom actions 711
optional components 100
Performance Monitor
configuring 493
effects of the CPU 314
SQL Server vaults 392
Server 2003 SP 1 452
Server Support Tools 456
Task Scheduler
Scheduled Jobs.txt 499
Terminal Server 480
version differences affecting restoration 242, 407
wizards
Create Recovery Log 278
Database 250
New Web Location 232
Prepare for Backup 263, 268
Oracle vaults 399
SQL server vaults 382
Registration 145
Restart After Restore 271
Restart After Restore from Backup 263, 271
Stream Recovery 224, 231
Upgrade Vault 116
Vault Archive 286
results 292
run the wizard 287
Vault Consistency (VCW)
logs 229
prepare 225
run 227
toolkit 224
Work Isolation Mode 172
workgroup deployment model 68
write-ahead logs 379, 396

X

XML files 700

MERIDIAN 2026 ENTERPRISE ADMINISTRATOR'S GUIDE – SEPTEMBER 2026

Accruent, LLC
11500 Alterra Parkway
Suite 110
Austin, TX 78758
www.accruent.com