

## Planning and Architecture for Office SharePoint Server 2007

Microsoft Corporation

Published: December 2006

Author: Office IT and Servers User Assistance (o12ITdx@microsoft.com)

Editor: Office IT and Servers User Assistance

### Abstract

This book is designed to lead a team through the steps of planning a new solution based on Microsoft Office SharePoint Server 2007. The audiences for this guide are business application specialists, line-of-business specialists, IT generalists, program managers, and infrastructure specialists who are planning a solution based on Office SharePoint Server 2007.



The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred.

© 2006 Microsoft Corporation. All rights reserved.

Active Directory, Excel, Microsoft, Outlook, SharePoint, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

# Contents

[Planning and Architecture for Office SharePoint Server 2007 1](#_Toc153614703)

[Abstract 1](#_Toc153614704)

[Contents 3](#_Toc153614705)

[Planning worksheets for Office SharePoint Server 2007 33](#_Toc153614706)

[Planning worksheets by task 33](#_Toc153614707)

[Planning worksheets by title 43](#_Toc153614708)

[I Plan overall design 56](#_Toc153614709)

[Chapter overview: Plan overall design 57](#_Toc153614710)

[How to use this Planning Guide 57](#_Toc153614711)

[What is Microsoft Office SharePoint Server 2007? 59](#_Toc153614712)

[Examples of solutions based on Office SharePoint Server 2007 60](#_Toc153614713)

[Establishing the planning team 62](#_Toc153614714)

[Plan sites and features 64](#_Toc153614715)

[Plan sites 65](#_Toc153614716)

[Plan portal sites 65](#_Toc153614717)

[Planning portal sites by organizational hierarchy 65](#_Toc153614718)

[Planning application portal sites 66](#_Toc153614719)

[Plan Internet presence sites 67](#_Toc153614720)

[Plan other sites 68](#_Toc153614721)

[Plan customizations 68](#_Toc153614722)

[Plan personalization sites 69](#_Toc153614723)

[Plan site collections 69](#_Toc153614724)

[Plan security 70](#_Toc153614725)

[Plan search needs 70](#_Toc153614726)

[Plan business intelligence integration 71](#_Toc153614727)

[Plan document and records management 71](#_Toc153614728)

[Plan workflows 72](#_Toc153614729)

[Plan forms 72](#_Toc153614730)

[Plan site maintenance 72](#_Toc153614731)

[Worksheet 73](#_Toc153614732)

[Plan Shared Services Providers 74](#_Toc153614733)

[About SSPs 74](#_Toc153614734)

[Determining Shared Services Provider Needs 76](#_Toc153614735)

[Sharing content across multiple SSPs 77](#_Toc153614736)

[II Plan site structure and publishing 79](#_Toc153614737)

[Chapter overview: Plan Web site structure and publishing (Office SharePoint Server) 80](#_Toc153614738)

[Determine the information architecture of your site 82](#_Toc153614739)

[What is information architecture? 82](#_Toc153614740)

[General planning recommendations 83](#_Toc153614741)

[Using information architecture to plan the structure of your site 83](#_Toc153614742)

[Using information architecture to plan for people and personalization 84](#_Toc153614743)

[Using information architecture to plan for business data 84](#_Toc153614744)

[Using information architecture to plan for search 85](#_Toc153614745)

[Determine sites and subsites 86](#_Toc153614747)

[Planning site collections 86](#_Toc153614748)

[Planning sites and subsites 88](#_Toc153614749)

[Site templates included in Office SharePoint Server 2007 88](#_Toc153614750)

[Comparison of the publishing templates 93](#_Toc153614751)

[Recording your site structure decisions 95](#_Toc153614752)

[Plan site navigation [Office SharePoint Server] 96](#_Toc153614754)

[Review of Office SharePoint Server navigation controls 97](#_Toc153614755)

[Navigation controls on master pages 97](#_Toc153614756)

[Global navigation 97](#_Toc153614757)

[Current navigation 98](#_Toc153614758)

[Breadcrumb navigation 99](#_Toc153614759)

[Navigation controls on layout pages 99](#_Toc153614760)

[Summary Links 100](#_Toc153614761)

[Table of Contents 100](#_Toc153614762)

[Content Query 101](#_Toc153614763)

[Navigation Web Parts 101](#_Toc153614764)

[Planning navigation 102](#_Toc153614765)

[Planning the user experience 102](#_Toc153614766)

[Planning navigation on pages 103](#_Toc153614767)

[Plan Web pages 105](#_Toc153614769)

[Elements of Web pages 105](#_Toc153614770)

[Planning master pages 109](#_Toc153614771)

[Planning content pages 111](#_Toc153614772)

[Planning layout pages 112](#_Toc153614773)

[Using layout pages to restrict authoring 114](#_Toc153614774)

[Setting restrictions on field controls 115](#_Toc153614775)

[Allowing or restricting Web Part zones 115](#_Toc153614776)

[Summary 116](#_Toc153614777)

[Plan Web page authoring 118](#_Toc153614779)

[Plan browser-based authoring 120](#_Toc153614780)

[Plan Page Editing toolbar customizations 121](#_Toc153614781)

[Plan HTML Editor toolbar customizations 122](#_Toc153614782)

[Plan reusable content 123](#_Toc153614783)

[Plan dictionary customizations 124](#_Toc153614784)

[Plan additional resources 124](#_Toc153614785)

[Plan smart-client authoring 125](#_Toc153614786)

[Worksheet 127](#_Toc153614787)

[Determine site variations 129](#_Toc153614789)

[About site variations 129](#_Toc153614790)

[Variations and content deployment 131](#_Toc153614791)

[Variations and navigation 131](#_Toc153614792)

[Variations and devices 131](#_Toc153614793)

[Plan structure of variation hierarchy 131](#_Toc153614794)

[Plan content approval and scheduling 133](#_Toc153614795)

[Plan governance 133](#_Toc153614796)

[Plan content moderation or workflow approval 133](#_Toc153614797)

[Plan where and how content can appear 134](#_Toc153614798)

[Plan scheduling 134](#_Toc153614799)

[Governance and scheduling in a content deployment scenario 135](#_Toc153614800)

[Plan content deployment 136](#_Toc153614801)

[What is content deployment? 136](#_Toc153614802)

[About deployment jobs and paths 137](#_Toc153614803)

[Content deployment security 138](#_Toc153614804)

[Configuring content deployment 139](#_Toc153614805)

[Record content deployment plans 140](#_Toc153614806)

[Worksheet 140](#_Toc153614807)

[Plan for collaboration sites 141](#_Toc153614809)

[About collaboration sites 141](#_Toc153614810)

[Determine number of collaboration sites 141](#_Toc153614811)

[Specific paths 142](#_Toc153614812)

[Additional paths 142](#_Toc153614813)

[Worksheet 143](#_Toc153614814)

[Plan for multilingual sites 144](#_Toc153614815)

[Determine your multilingual needs 144](#_Toc153614816)

[Identify language requirements 145](#_Toc153614817)

[Determine internationalized domain name mappings 145](#_Toc153614818)

[Determine whether you want to use site variations 146](#_Toc153614819)

[Plan for multilingual site deployment 147](#_Toc153614820)

[Determine your language pack requirements 147](#_Toc153614821)

[Determine supplemental language support requirements 149](#_Toc153614822)

[Determine requirements for word breakers and stemmers 150](#_Toc153614823)

[White paper: Plan for building multilingual solutions 152](#_Toc153614824)

[III Plan for personalized content and sites 153](#_Toc153614825)

[Chapter overview: Plan for personalized content and sites 154](#_Toc153614826)

[Plan for people and user profiles 154](#_Toc153614827)

[Plan for audiences 155](#_Toc153614828)

[Plan for personalized Web Parts 155](#_Toc153614829)

[Plan for My Sites 155](#_Toc153614830)

[Plan for people and user profiles 157](#_Toc153614831)

[About people and user profiles 157](#_Toc153614832)

[Plan connections to Profile Services 159](#_Toc153614833)

[Plan user profile properties 161](#_Toc153614834)

[Default user profile properties 163](#_Toc153614835)

[Additional user profile properties 163](#_Toc153614836)

[Configure property choice lists 164](#_Toc153614837)

[Plan people and relationships 165](#_Toc153614838)

[Plan policies 166](#_Toc153614839)

[Plan policies for people features 168](#_Toc153614840)

[Plan policies for the properties of user profiles 169](#_Toc153614841)

[Policy replication 171](#_Toc153614842)

[Plan for finding people 172](#_Toc153614843)

[Plan additional personalization functionality 173](#_Toc153614844)

[Worksheets 173](#_Toc153614845)

[Plan for audiences 175](#_Toc153614846)

[About audiences 175](#_Toc153614847)

[Plan key audiences 176](#_Toc153614848)

[Plan content targeting to audiences 178](#_Toc153614849)

[Target by list item or Web Part 178](#_Toc153614850)

[Target by using Trusted My Site host locations 179](#_Toc153614851)

[Target by using the My Site navigation bar 180](#_Toc153614852)

[Target links published to Office client applications 180](#_Toc153614853)

[Filter by audience 181](#_Toc153614854)

[Worksheet 181](#_Toc153614855)

[Plan for personalized Web Parts 182](#_Toc153614856)

[About personalized Web Parts 182](#_Toc153614857)

[Plan for public profile Web Parts 183](#_Toc153614858)

[Default Web Parts for public profiles 183](#_Toc153614859)

[Additional Web Parts for public profiles 184](#_Toc153614860)

[Plan for personal site Web Parts 185](#_Toc153614861)

[Default Web Parts for personal sites 185](#_Toc153614862)

[Additional Web Parts for personal sites 186](#_Toc153614863)

[Plan for personalization site Web Parts 186](#_Toc153614864)

[Default Web Parts for personalization sites 186](#_Toc153614865)

[Additional Web Parts for personalization sites 187](#_Toc153614866)

[Plan additional Web Parts for My Sites 188](#_Toc153614867)

[Plan for suggested Web Parts on My Sites 188](#_Toc153614868)

[Plan for lists and libraries Web Parts on My Sites 190](#_Toc153614869)

[Plan for business data Web Parts on My Sites 191](#_Toc153614870)

[Plan for dashboard Web Parts on My Sites 193](#_Toc153614871)

[Plan for filter Web Parts on My Sites 195](#_Toc153614872)

[Plan for miscellaneous and custom Web Parts on My Sites 195](#_Toc153614873)

[Plan for personalized Web Parts on other sites 196](#_Toc153614874)

[Worksheet 197](#_Toc153614875)

[Plan My Sites 198](#_Toc153614876)

[About My Sites 198](#_Toc153614877)

[About the public profile page 200](#_Toc153614878)

[About personal sites 200](#_Toc153614879)

[About personalization sites 201](#_Toc153614880)

[Plan for personalized sites 202](#_Toc153614881)

[Activate the My Site feature 203](#_Toc153614882)

[Plan for My Sites in the SSP 204](#_Toc153614883)

[Plan My Site policies 207](#_Toc153614884)

[Plan for personalization sites 207](#_Toc153614885)

[Incorporate personalization sites into site collections 208](#_Toc153614886)

[Plan owners of personalization sites 209](#_Toc153614887)

[Plan Web Parts for personalization sites 209](#_Toc153614888)

[Worksheet 209](#_Toc153614889)

[IV Plan workflows 210](#_Toc153614890)

[Chapter overview: Plan workflows 211](#_Toc153614891)

[What are workflows? 212](#_Toc153614892)

[About business processes 212](#_Toc153614893)

[Workflows in Office SharePoint Server 2007 213](#_Toc153614894)

[Plan workflows: Next steps 216](#_Toc153614896)

[Planning workflows: Next steps 216](#_Toc153614897)

[V Plan for forms 217](#_Toc153614899)

[Chapter overview: Plan InfoPath Forms Services 218](#_Toc153614900)

[InfoPath Forms Services planning articles 219](#_Toc153614901)

[Before you begin designing form templates 219](#_Toc153614902)

[Planning form template design 219](#_Toc153614903)

[Planning form template deployment 219](#_Toc153614904)

[Planning server supportability and maintenance 219](#_Toc153614905)

[Scenario planning 220](#_Toc153614906)

[Scenario 1: Expense-Report Submission 221](#_Toc153614907)

[Situation 221](#_Toc153614908)

[Solution: Forms for internal use 221](#_Toc153614909)

[Scenario 2: Insurance claims processing 222](#_Toc153614910)

[Situation 222](#_Toc153614911)

[Solution 1: Forms for internal use 222](#_Toc153614912)

[Solution 2: Customer-facing forms 223](#_Toc153614913)

[Scenario 3: Online government permits 223](#_Toc153614914)

[Situation 223](#_Toc153614915)

[Solution 1: Customer-facing forms 223](#_Toc153614916)

[Solution 2: Forms processing workflow 223](#_Toc153614917)

[Plan what form templates are needed [Office SharePoint Server] 225](#_Toc153614918)

[Create an inventory of current forms 225](#_Toc153614919)

[Survey the advantages of online forms 226](#_Toc153614920)

[Assess the need for new form templates 227](#_Toc153614921)

[Determine form template complexity 227](#_Toc153614922)

[Worksheet 228](#_Toc153614923)

[Plan custom form templates (Office SharePoint Server) 230](#_Toc153614925)

[Plan form template design infrastructure requirements (Office SharePoint Server) 231](#_Toc153614927)

[Server requirements 232](#_Toc153614928)

[Network requirements 232](#_Toc153614929)

[Security requirements 233](#_Toc153614930)

[Plan server-side data connections needed for form templates [Office SharePoint Server] 234](#_Toc153614932)

[Scenarios for the use of data connections 235](#_Toc153614933)

[Scenario 1: Intranet: Authenticated user submitting data through e-mail 235](#_Toc153614934)

[Scenario 2: Extranet: Basic authentication submitting data through e-mail 235](#_Toc153614935)

[Scenario 3: Intranet: HTTP post to application server 235](#_Toc153614936)

[Database data connection 236](#_Toc153614937)

[HTTP post data connection 236](#_Toc153614938)

[SharePoint library submit data connection 237](#_Toc153614939)

[SharePoint list data connection 237](#_Toc153614940)

[Web service data connection 237](#_Toc153614941)

[XML file data connection 237](#_Toc153614942)

[Plan deployment of form templates [Office SharePoint Server] 238](#_Toc153614943)

[Browser-compatible form templates 238](#_Toc153614944)

[Scenario: Insurance claims processing 239](#_Toc153614945)

[Plan deployment of administrator-approved form templates [Office SharePoint Server] 241](#_Toc153614947)

[Determine the impact of anonymously accessible form templates 243](#_Toc153614949)

[Identify the need for anonymously accessible form templates 243](#_Toc153614950)

[Internet scenario 243](#_Toc153614951)

[Corporate scenario 243](#_Toc153614952)

[Security and usage considerations for anonymously accessible form templates 244](#_Toc153614953)

[Bandwidth and capacity considerations for anonymously accessible form templates 245](#_Toc153614954)

[Plan for naming form templates [Office SharePoint Server] 246](#_Toc153614956)

[Plan for upgrading form templates [Office SharePoint Server] 247](#_Toc153614958)

[Plan for retiring form templates [Office SharePoint Server] 248](#_Toc153614959)

[Plan version control for form templates [Office SharePoint Server] 249](#_Toc153614961)

[Document Retention 249](#_Toc153614962)

[Capacity Planning 250](#_Toc153614963)

[Plan for mobile device access to form templates [Office SharePoint Server] 251](#_Toc153614965)

[Plan workflow for form templates 253](#_Toc153614967)

[Custom workflow form templates 253](#_Toc153614968)

[Workflows for form template approval 253](#_Toc153614969)

[Workflows launched from a form 254](#_Toc153614970)

[VI Plan for business intelligence 255](#_Toc153614972)

[Chapter overview: Plan for business intelligence 256](#_Toc153614973)

[Determine business data and business intelligence needs 259](#_Toc153614974)

[About business intelligence 259](#_Toc153614975)

[Plan Office SharePoint Server 2007 features for business intelligence 261](#_Toc153614976)

[Plan data integration features of Office SharePoint Server 2007 261](#_Toc153614977)

[Plan information presentation and reporting features of Office SharePoint Server 2007 263](#_Toc153614978)

[Plan business data scenarios 264](#_Toc153614979)

[Plan purpose-based scenarios 264](#_Toc153614980)

[Plan process-based scenarios 265](#_Toc153614981)

[Plan IT-based scenarios 266](#_Toc153614982)

[Determine business intelligence needs for your organization 266](#_Toc153614983)

[Worksheets 267](#_Toc153614984)

[Determine scope of business intelligence analysis 268](#_Toc153614985)

[About business intelligence scope planning 268](#_Toc153614986)

[Business intelligence principles 269](#_Toc153614987)

[Business intelligence examples 269](#_Toc153614988)

[Plan data connection management 270](#_Toc153614989)

[About data connection management in Office SharePoint Server 2007 270](#_Toc153614990)

[Plan access to external data 270](#_Toc153614991)

[Plan access to data connection libraries 271](#_Toc153614992)

[Plan key performance indicators 272](#_Toc153614993)

[About KPIs 272](#_Toc153614994)

[Plan data sources for KPIs 274](#_Toc153614995)

[Plan KPIs in reports 276](#_Toc153614996)

[Plan KPIs in dashboards 277](#_Toc153614997)

[Plan KPIs in My Site 277](#_Toc153614998)

[Worksheets 279](#_Toc153614999)

[Plan reports 280](#_Toc153615000)

[About reports 280](#_Toc153615001)

[Plan Web Parts for reports 281](#_Toc153615002)

[Plan reports for the Report Center site 283](#_Toc153615003)

[Plan the reports library 285](#_Toc153615004)

[Plan other features of the Report Center site 286](#_Toc153615005)

[Worksheets 287](#_Toc153615006)

[Plan dashboards and filters 288](#_Toc153615007)

[About dashboards and filters 288](#_Toc153615008)

[Plan Web Parts for dashboards 290](#_Toc153615009)

[Plan Excel Web Access Web Parts for dashboards 291](#_Toc153615010)

[Plan business data Web Parts for dashboards 291](#_Toc153615011)

[Plan KPI Web Parts for dashboards 293](#_Toc153615012)

[Plan filters 293](#_Toc153615013)

[Plan automatic filter Web Parts 295](#_Toc153615014)

[Plan filters that use user-specified values 296](#_Toc153615015)

[Plan filters that use values selected from a list 296](#_Toc153615016)

[Worksheets 298](#_Toc153615017)

[Plan Excel Services security 299](#_Toc153615018)

[About Excel Services security 299](#_Toc153615019)

[Plan user authentication 300](#_Toc153615020)

[Plan communication among servers 301](#_Toc153615021)

[Plan external data authentication 301](#_Toc153615022)

[Integrated Windows authentication 303](#_Toc153615023)

[SSO authentication 303](#_Toc153615024)

[None 305](#_Toc153615025)

[Unattended service account 305](#_Toc153615026)

[Security settings 306](#_Toc153615027)

[File access method 306](#_Toc153615028)

[Data encryption 307](#_Toc153615029)

[Trusted file locations 307](#_Toc153615030)

[Trusted data providers 310](#_Toc153615031)

[Trusted data connection libraries 311](#_Toc153615032)

[View Only permissions 311](#_Toc153615033)

[External data connections 312](#_Toc153615034)

[.odc files 313](#_Toc153615035)

[Managing .odc files 314](#_Toc153615036)

[User-defined functions 314](#_Toc153615037)

[Worksheets 315](#_Toc153615038)

[Determine resource requirements to support Excel Services 316](#_Toc153615039)

[About Excel Services topologies 316](#_Toc153615040)

[Data access models 317](#_Toc153615041)

[Excel Services topologies 318](#_Toc153615042)

[Excel Services single-server topology 318](#_Toc153615043)

[Excel Services small farm trusted subsystem topology 320](#_Toc153615044)

[Excel Services small farm Kerberos topology 321](#_Toc153615045)

[Excel Services medium farm trusted subsystem topology 321](#_Toc153615046)

[Excel Services medium farm Kerberos topology 323](#_Toc153615047)

[Excel Services large farm trusted subsystem topology 324](#_Toc153615048)

[Excel Services large farm Kerberos topology 325](#_Toc153615049)

[Excel Services extranet topology 327](#_Toc153615050)

[Excel Services corporate intranet topology 328](#_Toc153615051)

[Excel Services high-performance computing topology 330](#_Toc153615052)

[Plan for simultaneous client connections 331](#_Toc153615053)

[Plan for concurrent Excel Calculation Services session requests 331](#_Toc153615054)

[Excel Services performance testing 333](#_Toc153615055)

[Hardware configuration 334](#_Toc153615056)

[Data set attribute tables 334](#_Toc153615057)

[Performance test scenarios 334](#_Toc153615058)

[Workbooks without external data connections 335](#_Toc153615059)

[Workbooks with OLAP data connections 336](#_Toc153615060)

[Workbooks with relational data connections 337](#_Toc153615061)

[Distribution of workbooks by data sources 338](#_Toc153615062)

[Request mix used in performance tests 339](#_Toc153615063)

[Performance test results 339](#_Toc153615064)

[Excel Services small farm trusted subsystem configuration 339](#_Toc153615065)

[Excel Services large farm trusted subsystem configuration 340](#_Toc153615066)

[Excel Services large farm Kerberos configuration 342](#_Toc153615067)

[Excel Services large farm trusted subsystem configuration using OLAP data with refresh on open and SSO 343](#_Toc153615068)

[Excel Services large farm Kerberos configuration using OLAP data with refresh on open 344](#_Toc153615069)

[Excel Services large farm Kerberos configuration using SQL Server 2005 Analysis Services groups 345](#_Toc153615070)

[Excel Services large farm trusted subsystem configuration using relational data 346](#_Toc153615071)

[Excel Services large farm Kerberos configuration using relational data 347](#_Toc153615072)

[Limit the number and duration of open sessions 349](#_Toc153615073)

[Plan rendering Excel KPI data 350](#_Toc153615075)

[About rendering Excel KPI data 350](#_Toc153615076)

[KPI List Web Parts for Office SharePoint Server 2007 350](#_Toc153615077)

[Excel KPI and SQL Server 2005 Analysis Services 350](#_Toc153615078)

[Plan Excel reports against OLAP cubes 352](#_Toc153615079)

[About building Excel reports against OLAP cubes 352](#_Toc153615080)

[OLAP functions 352](#_Toc153615081)

[OLAP formulas 353](#_Toc153615082)

[Plan access to Excel spreadsheets 354](#_Toc153615083)

[About spreadsheet management 354](#_Toc153615084)

[Plan a strategy to control access to workbooks and ensure data integrity 354](#_Toc153615085)

[Plan a strategy to restrict access to individual data objects within workbooks 355](#_Toc153615086)

[Plan for business data connections with the Business Data Catalog 356](#_Toc153615087)

[About the Business Data Catalog 356](#_Toc153615088)

[Plan connections to the Business Data Catalog 357](#_Toc153615089)

[Plan business data presentation 360](#_Toc153615090)

[Worksheets 361](#_Toc153615091)

[Plan for business data profiles 362](#_Toc153615092)

[About business data profiles 362](#_Toc153615093)

[Plan connections to the Business Data Catalog 362](#_Toc153615094)

[Plan to include business data content sources 363](#_Toc153615095)

[Plan properties of business data profiles 363](#_Toc153615096)

[Worksheets 367](#_Toc153615097)

[Plan business data lists 368](#_Toc153615098)

[About business data lists 368](#_Toc153615099)

[Plan business data columns 369](#_Toc153615100)

[Plan dependent columns 370](#_Toc153615101)

[Plan business actions in business data lists 371](#_Toc153615102)

[Plan Web Parts for business data lists 371](#_Toc153615103)

[Worksheets 372](#_Toc153615104)

[Plan business data Web Parts 373](#_Toc153615105)

[About business data Web Parts 373](#_Toc153615106)

[Plan core business data Web Parts 374](#_Toc153615107)

[Plan specialized business data Web Parts 376](#_Toc153615108)

[Plan KPI Web Parts 376](#_Toc153615109)

[Plan Excel Web Access Web Parts 377](#_Toc153615110)

[Plan SQL Server 2005 Analysis Services Web Parts 378](#_Toc153615111)

[Plan filter Web Parts connected to business data Web Parts 378](#_Toc153615112)

[Plan deployment of Web Parts 378](#_Toc153615113)

[Worksheets 380](#_Toc153615114)

[Plan business data actions 381](#_Toc153615115)

[About business data actions 381](#_Toc153615116)

[Plan the scope of business actions 383](#_Toc153615117)

[Plan properties for business actions 383](#_Toc153615118)

[Plan Business Data Action Web Parts 384](#_Toc153615119)

[Plan custom business actions 385](#_Toc153615120)

[Worksheet 385](#_Toc153615121)

[Plan for business data search 386](#_Toc153615122)

[About business data search 386](#_Toc153615123)

[Plan business data search 387](#_Toc153615124)

[Plan Shared Services Providers for business data 388](#_Toc153615125)

[Plan business data content sources 389](#_Toc153615126)

[Plan search properties for business data 390](#_Toc153615127)

[Plan access and security for business data search results 391](#_Toc153615128)

[Plan search scopes for business data 392](#_Toc153615129)

[Plan keywords for business data 392](#_Toc153615130)

[Plan business data tabs in the Search Center site 393](#_Toc153615131)

[Example 394](#_Toc153615132)

[Worksheets 395](#_Toc153615133)

[Plan external data connections for Excel Services 396](#_Toc153615134)

[About Excel Services connections to external data 397](#_Toc153615135)

[Connections and Excel workbooks 397](#_Toc153615136)

[Embedded and linked connections 397](#_Toc153615137)

[Data providers 398](#_Toc153615138)

[Authentication to external data 399](#_Toc153615139)

[Windows authentication 400](#_Toc153615140)

[SSO 400](#_Toc153615141)

[None 401](#_Toc153615142)

[Data connection libraries and managed connections 401](#_Toc153615143)

[Reusing connections 402](#_Toc153615144)

[Managing connections 402](#_Toc153615145)

[Securing connections 402](#_Toc153615146)

[Excel Services security and external data 403](#_Toc153615147)

[Trusted file locations 403](#_Toc153615148)

[Trusted data connection libraries 404](#_Toc153615149)

[Trusted data providers 404](#_Toc153615150)

[Unattended account 404](#_Toc153615151)

[Trusted subsystem and delegation 405](#_Toc153615152)

[Step-by-step server configuration for external data 406](#_Toc153615153)

[Adding a trusted data provider for Excel Services 407](#_Toc153615154)

[Allowing external data for Excel services 408](#_Toc153615155)

[Setting the unattended account 411](#_Toc153615156)

[Configuring Office Server single sign-on 412](#_Toc153615157)

[Start the Microsoft Single Sign-On service on the server 413](#_Toc153615158)

[Configuring SSO on Office Server 416](#_Toc153615159)

[More on Office Server SSO accounts and privileges 417](#_Toc153615160)

[Creating a new application ID in SSO 419](#_Toc153615161)

[Creating a data connection library 425](#_Toc153615162)

[Trusting a data connection library on Excel Services 428](#_Toc153615163)

[Exposing the data connection library in the Office client 429](#_Toc153615164)

[Publishing the data connection library to the Office client 429](#_Toc153615165)

[Setting a registry key to surface a data connection library in the client 432](#_Toc153615166)

[Step-by-step workbook configuration for external data 435](#_Toc153615167)

[Creating a new connection 435](#_Toc153615168)

[Reusing an existing connection from a data connection library 437](#_Toc153615169)

[Specifying the server authentication for an existing connection 440](#_Toc153615170)

[Saving an existing connection to a data connection library 443](#_Toc153615171)

[Frequently asked questions 444](#_Toc153615172)

[How do I get Microsoft Access data into my workbooks on Excel Services? 444](#_Toc153615173)

[How do I use other workbooks as data sources on Excel Services? 445](#_Toc153615174)

[Why don't my Windows authentication connections work even when I have correctly configured Kerberos in my farm? 445](#_Toc153615175)

[If the credentials are not delegated, how can Excel Services make per-user permission checks on files? 445](#_Toc153615176)

[What is the guidance around using local cubes on the server? 445](#_Toc153615177)

[How can I have more control over how external data is accessed from the server? 446](#_Toc153615178)

[What factors should I consider regarding performance and external data? 446](#_Toc153615179)

[How can I secure my data so that it is viewable only from a workbook published to Excel Services? 447](#_Toc153615180)

[I followed the instructions in this article, but when I load my workbook on the server I see some unsupported features error talking about Query Tables. How can I fix it? 448](#_Toc153615181)

[I have an ODBC connection, and therefore I do not have an .odc file. How can I use my connection with a data connection library so that it will work on Excel Services? 449](#_Toc153615182)

[How do View Only permissions and .odc files in a data connection library work? 449](#_Toc153615183)

[VII Plan search 451](#_Toc153615185)

[Chapter overview: Plan search (Office SharePoint Server) 452](#_Toc153615186)

[Why two search services? 452](#_Toc153615187)

[Plan the search team 453](#_Toc153615188)

[Plan to crawl content 453](#_Toc153615189)

[Plan the end-user search experience 454](#_Toc153615190)

[Identify your search team (Office SharePoint Server) 455](#_Toc153615191)

[About the search planning team 455](#_Toc153615192)

[About the search planning process 456](#_Toc153615193)

[Plan the search deployment and operations teams 456](#_Toc153615194)

[Worksheet 456](#_Toc153615195)

[Plan to crawl content [Office SharePoint Server] 457](#_Toc153615196)

[About crawling content 458](#_Toc153615197)

[Plan content sources 459](#_Toc153615198)

[Plan default content access account 461](#_Toc153615199)

[Plan for external content 462](#_Toc153615200)

[Plan content sources for business data 463](#_Toc153615201)

[Plan crawl settings 464](#_Toc153615202)

[Plan crawl schedules 465](#_Toc153615203)

[Protocol handlers 466](#_Toc153615204)

[Plan crawler impact rules 466](#_Toc153615205)

[Plan crawl rules 468](#_Toc153615206)

[Specify a different content access account 469](#_Toc153615207)

[Plan file-type inclusions and IFilters 470](#_Toc153615208)

[Plan search settings that are managed at the farm level 473](#_Toc153615209)

[Worksheet 474](#_Toc153615210)

[Plan the end user search experience [Office SharePoint Server] 476](#_Toc153615211)

[Plan properties for search 477](#_Toc153615212)

[Plan managed properties based on the information architecture 478](#_Toc153615213)

[Eliminate redundant and duplicate properties by using property mapping 479](#_Toc153615214)

[Add properties to present key concepts in the information architecture 480](#_Toc153615215)

[Plan for business data properties 481](#_Toc153615216)

[Using properties in queries 481](#_Toc153615217)

[Use managed properties in search scopes 482](#_Toc153615218)

[Plan to integrate properties for new file types using filters 482](#_Toc153615219)

[Plan search scopes 483](#_Toc153615220)

[Plan shared scopes 483](#_Toc153615221)

[Plan search scopes for site collections 484](#_Toc153615222)

[Plan display groups 485](#_Toc153615223)

[Plan search scope rules 486](#_Toc153615224)

[Using rules based on location 487](#_Toc153615225)

[Using rules based on managed properties 487](#_Toc153615226)

[Using rules based on content sources 488](#_Toc153615227)

[Using rules based on all content 488](#_Toc153615228)

[Using multiple rules 489](#_Toc153615229)

[Using exclusion rules 489](#_Toc153615230)

[Example of search scope planning 489](#_Toc153615231)

[Plan authoritative pages 491](#_Toc153615232)

[Plan server name mappings 492](#_Toc153615233)

[Plan keywords and best bets 493](#_Toc153615234)

[Use information architecture to identify keywords 494](#_Toc153615235)

[Use properties of keywords 495](#_Toc153615236)

[Plan keywords 496](#_Toc153615237)

[Plan keyword management 497](#_Toc153615238)

[Plan search-based alerts 499](#_Toc153615239)

[VIII Plan communication 500](#_Toc153615240)

[Chapter overview: Plan communication [Office SharePoint Server] 501](#_Toc153615241)

[Communications components 501](#_Toc153615242)

[Plan presence integration [Office SharePoint Server] 502](#_Toc153615243)

[About online presence 502](#_Toc153615244)

[Advantages of incorporating online presence 503](#_Toc153615245)

[Organizational considerations 503](#_Toc153615246)

[Software requirements 504](#_Toc153615247)

[E-mail account requirements 504](#_Toc153615248)

[Plan incoming e-mail [Office SharePoint Server] 505](#_Toc153615249)

[About incoming e-mail 505](#_Toc153615250)

[Key decisions for planning incoming e-mail 505](#_Toc153615251)

[Basic scenario 506](#_Toc153615252)

[Advanced scenarios 507](#_Toc153615253)

[Safe e-mail server 507](#_Toc153615254)

[E-mail drop folder 508](#_Toc153615255)

[Microsoft SharePoint Directory Management service 509](#_Toc153615256)

[Incoming e-mail server display address 509](#_Toc153615257)

[Configuration options and settings modes 510](#_Toc153615258)

[Before configuring incoming e-mail 511](#_Toc153615259)

[Plan the Microsoft SharePoint Directory Management service 511](#_Toc153615260)

[Directory management service configuration options 512](#_Toc153615261)

[Worksheet 513](#_Toc153615262)

[Plan outgoing e-mail [Office SharePoint Server] 514](#_Toc153615263)

[About outgoing e-mail 515](#_Toc153615264)

[General requirements 515](#_Toc153615265)

[Outbound SMTP server 515](#_Toc153615266)

[From and Reply-to addresses 516](#_Toc153615267)

[Character set 516](#_Toc153615268)

[IX Plan document management 517](#_Toc153615269)

[Chapter overview: Plan document management 518](#_Toc153615270)

[What is document management? 520](#_Toc153615272)

[The elements of a document management system 520](#_Toc153615273)

[The planning process 521](#_Toc153615274)

[Identify document management participants and stakeholders 523](#_Toc153615275)

[Worksheet 524](#_Toc153615276)

[Analyze document usage 525](#_Toc153615277)

[Worksheet 527](#_Toc153615278)

[Plan document libraries 528](#_Toc153615279)

[Plan document libraries 528](#_Toc153615280)

[Plan the flow of content 533](#_Toc153615281)

[Promoting document libraries from Office client programs 534](#_Toc153615282)

[Plan content types [Office SharePoint Server] 537](#_Toc153615284)

[What are content types? 537](#_Toc153615285)

[Properties integration with the 2007 Office release 539](#_Toc153615286)

[About column templates 539](#_Toc153615287)

[About folder content types 540](#_Toc153615288)

[Planning document content types 540](#_Toc153615289)

[Planning list content types 543](#_Toc153615290)

[Planning document conversions 544](#_Toc153615291)

[After planning content types: next steps 545](#_Toc153615292)

[Worksheets 546](#_Toc153615293)

[Plan workflows for document management 547](#_Toc153615294)

[Worksheet 548](#_Toc153615295)

[Plan versioning, content approval, and check-outs 549](#_Toc153615296)

[Plan versioning 549](#_Toc153615297)

[Plan content approval 550](#_Toc153615298)

[Plan check-in and check-out 552](#_Toc153615299)

[Worksheet 553](#_Toc153615300)

[Plan Information Rights Management 554](#_Toc153615302)

[Information Rights Management in Office SharePoint Server 2007 554](#_Toc153615303)

[Worksheet 556](#_Toc153615304)

[Plan information management policies 557](#_Toc153615305)

[About information management policies and policy features 557](#_Toc153615306)

[About information management policy reporting 559](#_Toc153615307)

[About information management policy integration with the 2007 Office system applications 560](#_Toc153615308)

[Policy features available in Office SharePoint Server 2007 561](#_Toc153615309)

[Plan information management policies 562](#_Toc153615310)

[Worksheet 563](#_Toc153615311)

[Plan enterprise content storage 564](#_Toc153615312)

[Typical large-scale content management scenarios 565](#_Toc153615313)

[Large-scale authoring environment 565](#_Toc153615314)

[Large-scale content archive 566](#_Toc153615315)

[Extremely large-scale content archive 566](#_Toc153615316)

[Site collections: content storage benefits and limitations 567](#_Toc153615317)

[Benefits of storing content in the same site collection 567](#_Toc153615318)

[Limits on storing content in the same site collection 567](#_Toc153615319)

[Sites: content storage benefits and limitations 568](#_Toc153615320)

[Benefits of storing content in the same site 568](#_Toc153615321)

[The Document Center site 569](#_Toc153615322)

[Limits on storing content in the same site 570](#_Toc153615323)

[Libraries: content storage benefits and limitations 570](#_Toc153615324)

[Benefits of storing content in the same library 570](#_Toc153615325)

[Limits on storing content in the same library 570](#_Toc153615326)

[Using indexed columns to improve view performance 571](#_Toc153615327)

[Folders: content storage benefits and considerations 572](#_Toc153615328)

[Summary of recommendations 572](#_Toc153615329)

[X Plan records management 574](#_Toc153615331)

[Chapter overview: Plan records management 575](#_Toc153615332)

[What is records management? 576](#_Toc153615334)

[Elements of a records management system 576](#_Toc153615335)

[Overview of records management planning 578](#_Toc153615336)

[Identify records management roles (Office SharePoint Server 2007) 581](#_Toc153615338)

[Worksheet 583](#_Toc153615339)

[Develop the file plan (Office SharePoint Server 2007) 584](#_Toc153615340)

[About records, active documents, and archived documents 584](#_Toc153615341)

[Determine what is a record 585](#_Toc153615342)

[Complete the file plan 587](#_Toc153615343)

[Worksheet 589](#_Toc153615344)

[Design the Records Center site (Office SharePoint Server 2007) 591](#_Toc153615345)

[About the Records Center site 591](#_Toc153615346)

[Planning document libraries for records retention 593](#_Toc153615347)

[Planning metadata 594](#_Toc153615348)

[Planning records metadata 594](#_Toc153615349)

[Planning additional metadata 595](#_Toc153615350)

[Planning policies 596](#_Toc153615351)

[Planning the record routing table 598](#_Toc153615352)

[Planning the site's security 600](#_Toc153615353)

[Worksheets 601](#_Toc153615354)

[Plan how records are collected (Office SharePoint Server 2007) 602](#_Toc153615355)

[Techniques for moving files into the Records Center site 602](#_Toc153615356)

[Manually sending content to the Records Center site 602](#_Toc153615357)

[Using managed e-mail folders in Microsoft Exchange Server 2007 to send e-mail and files to the Records Center site 603](#_Toc153615358)

[Using a custom solution to send files to the Records Center site 604](#_Toc153615359)

[Completing your plan 604](#_Toc153615360)

[XI Plan site and content security 607](#_Toc153615361)

[Chapter overview: Plan site and content security [Office SharePoint Server] 608](#_Toc153615362)

[Plan site security [Office SharePoint Server] 609](#_Toc153615363)

[About site security elements 610](#_Toc153615364)

[About assigning permissions 611](#_Toc153615365)

[About fine-grained permissions and permission inheritance 612](#_Toc153615366)

[Permission inheritance and fine-grained permissions 612](#_Toc153615367)

[Permission inheritance and subsites 613](#_Toc153615368)

[Choose which levels of site security to use 613](#_Toc153615369)

[Plan for permission inheritance 614](#_Toc153615370)

[Worksheet 615](#_Toc153615371)

[Determine permission levels and groups to use [Office SharePoint Server] 616](#_Toc153615372)

[Review available default groups 616](#_Toc153615373)

[Review available permission levels 618](#_Toc153615374)

[Determine whether you need additional permission levels or groups 619](#_Toc153615375)

[Do you need custom groups? 619](#_Toc153615376)

[Do you need custom permission levels? 620](#_Toc153615377)

[Worksheet 621](#_Toc153615378)

[Define custom permission levels [Office SharePoint Server] 622](#_Toc153615379)

[Customize an existing permission level 622](#_Toc153615380)

[Copy an existing permission level 622](#_Toc153615381)

[Create a permission level 623](#_Toc153615382)

[Choose which security groups to use [Office SharePoint Server] 624](#_Toc153615383)

[Determine which Windows security groups and accounts to use for granting access to sites 625](#_Toc153615384)

[Decide whether to use all authenticated users 625](#_Toc153615385)

[Decide whether to allow access to anonymous users 625](#_Toc153615386)

[Worksheet 627](#_Toc153615387)

[Choose administrators and owners for the administration hierarchy (Office SharePoint Server) 628](#_Toc153615388)

[Levels of administration 628](#_Toc153615389)

[Worksheet 630](#_Toc153615390)

[Plan for InfoPath Forms Services security [Office SharePoint Server] 631](#_Toc153615391)

[XII Plan for site creation and maintenance 632](#_Toc153615392)

[Chapter overview: Plan for site creation and maintenance [Office SharePoint Server] 633](#_Toc153615393)

[Plan process for creating sites [Office SharePoint Server] 634](#_Toc153615394)

[Determine who can create sites and a method for site creation 634](#_Toc153615395)

[Plan for Self-Service Site Management 636](#_Toc153615396)

[Plan for custom site creation processes 637](#_Toc153615397)

[Worksheet 637](#_Toc153615398)

[Plan for site maintenance and management [Office SharePoint Server] 638](#_Toc153615399)

[Plan for site maintenance 638](#_Toc153615400)

[Plan for managing site collections 639](#_Toc153615401)

[Plan site collection quotas 640](#_Toc153615402)

[Plan site use confirmation and deletion 640](#_Toc153615403)

[Worksheet 641](#_Toc153615404)

[XIII Plan for system requirements 642](#_Toc153615405)

[Subhead 642](#_Toc153615406)

[Subhead 642](#_Toc153615407)

[Determine hardware and software requirements (Office SharePoint Server) 643](#_Toc153615408)

[About hardware and software requirements 643](#_Toc153615409)

[Stand-alone installation 643](#_Toc153615410)

[Hardware requirements 644](#_Toc153615411)

[Software requirements 644](#_Toc153615412)

[Database 645](#_Toc153615413)

[Operating system 645](#_Toc153615414)

[Windows components 646](#_Toc153615415)

[Microsoft .NET Framework 3.0 646](#_Toc153615416)

[Server farm installation 646](#_Toc153615417)

[Application server 647](#_Toc153615418)

[Hardware requirements 647](#_Toc153615419)

[Software requirements 648](#_Toc153615420)

[Front-end Web server 649](#_Toc153615421)

[Hardware requirements 649](#_Toc153615422)

[Software requirements 650](#_Toc153615423)

[Database server 650](#_Toc153615424)

[Plan browser support (Office SharePoint Server) 652](#_Toc153615425)

[About browser support 652](#_Toc153615426)

[Levels of browser support 652](#_Toc153615427)

[Level 1 Web browsers 652](#_Toc153615428)

[Level 2 Web browsers 653](#_Toc153615429)

[XIV Design server farms and topologies 654](#_Toc153615430)

[Chapter overview: Design server farms and topologies [Office SharePoint Server] 655](#_Toc153615431)

[Design extranet farm topology [Office SharePoint Server] 656](#_Toc153615432)

[Design content deployment topology 657](#_Toc153615433)

[Elements of content deployment topologies 657](#_Toc153615434)

[Typical content deployment topologies 658](#_Toc153615435)

[Standard Internet site topology 658](#_Toc153615436)

[Three-stage topology 660](#_Toc153615437)

[Single-farm topology 661](#_Toc153615438)

[Plan for geographically distributed sites 662](#_Toc153615440)

[Design document conversions topology 663](#_Toc153615441)

[About document conversions 663](#_Toc153615442)

[Typical document conversion topologies 665](#_Toc153615443)

[Configuring document conversions in a server farm 667](#_Toc153615444)

[Planning topologies for document conversions 669](#_Toc153615445)

[Worksheet 670](#_Toc153615446)

[Chart the farms within and across your networks 671](#_Toc153615447)

[Plan for availability (Office SharePoint Server) 672](#_Toc153615448)

[About availability 672](#_Toc153615449)

[Define server redundancy requirements 673](#_Toc153615450)

[Plan for a limited server deployment 675](#_Toc153615451)

[Plan for a minimum level of availability 677](#_Toc153615452)

[Four-server farm 677](#_Toc153615453)

[Five-server farm 678](#_Toc153615454)

[Six-server farm 679](#_Toc153615455)

[Three-server farm 680](#_Toc153615456)

[Choosing a baseline server farm topology 681](#_Toc153615457)

[Plan front-end Web server availability 682](#_Toc153615458)

[Plan application server availability 683](#_Toc153615459)

[Roles that can be redundant 684](#_Toc153615460)

[Roles that cannot be redundant 685](#_Toc153615461)

[Evaluating the risks of application server failures 686](#_Toc153615462)

[Plan database availability 688](#_Toc153615463)

[Select a baseline topology 689](#_Toc153615464)

[XV Design logical architecture 691](#_Toc153615465)

[Chapter overview: Design logical architecture 692](#_Toc153615466)

[Logical architecture elements 693](#_Toc153615467)

[A Design an intranet solution architecture 694](#_Toc153615468)

[Subhead 694](#_Toc153615469)

[Subhead 694](#_Toc153615470)

[Chapter overview: Design an intranet solution architecture 695](#_Toc153615471)

[Design team sites architecture 696](#_Toc153615472)

[Design published intranet site architecture 697](#_Toc153615473)

[Design records repository site architecture 698](#_Toc153615474)

[Design additional application sites within your intranet 699](#_Toc153615475)

[Design an Internet solution architecture 700](#_Toc153615476)

[B Design farm-level architecture 701](#_Toc153615477)

[Subhead 701](#_Toc153615478)

[Subhead 701](#_Toc153615479)

[Chapter overview: Design farm-level architecture 702](#_Toc153615480)

[Design user access and zones 703](#_Toc153615481)

[Plan Shared Services Provider architecture 704](#_Toc153615482)

[Plan for administrative sites 705](#_Toc153615483)

[Plan alternate access mappings 706](#_Toc153615484)

[Plan for host-named site collections 707](#_Toc153615485)

[C Design the logical architecture for an extranet solution 708](#_Toc153615486)

[Subhead 708](#_Toc153615487)

[Subhead 708](#_Toc153615488)

[Chapter overview: Design the logical architecture for an extranet solution 709](#_Toc153615489)

[Design the farm-level logical architecture for an extranet solution 710](#_Toc153615490)

[Plan reverse-proxy settings 711](#_Toc153615491)

[Plan for caching across the extranet environment 712](#_Toc153615492)

[D Plan for user accounts and authentication 713](#_Toc153615493)

[Subhead 713](#_Toc153615494)

[Subhead 713](#_Toc153615495)

[Chapter overview: Plan for user accounts and authentication [Office SharePoint Server] 714](#_Toc153615496)

[Plan for user accounts [Office SharePoint Server] 715](#_Toc153615497)

[Plan authentication methods [Office SharePoint Server] 716](#_Toc153615498)

[About authentication 716](#_Toc153615499)

[Supported authentication methods 716](#_Toc153615500)

[Authentication of system accounts 718](#_Toc153615501)

[Configure authentication 719](#_Toc153615502)

[Configure authentication for SharePoint Web applications 719](#_Toc153615503)

[Connect to identity management systems that are external or not based on Windows 724](#_Toc153615504)

[Enabling Anonymous Access 728](#_Toc153615505)

[Using different authentication methods to access a site 728](#_Toc153615506)

[Authentication requirements for crawling content 730](#_Toc153615507)

[Planning zones for your authentication design 730](#_Toc153615508)

[Choose methods of authentication allowed in your environment 731](#_Toc153615509)

[Recommendations for specific security environments 732](#_Toc153615510)

[Recommendations and tradeoffs for authentication methods 733](#_Toc153615511)

[Management of user identity information 735](#_Toc153615512)

[Management of user accounts 737](#_Toc153615513)

[Browser support 739](#_Toc153615514)

[Worksheet 740](#_Toc153615515)

[Plan authentication settings for Web applications in Office SharePoint Server 742](#_Toc153615516)

[Plan authentication settings 742](#_Toc153615517)

[Authentication type 743](#_Toc153615518)

[Anonymous access 744](#_Toc153615519)

[Client integration 744](#_Toc153615520)

[Settings for ASP.NET forms authentication and Web SSO 749](#_Toc153615521)

[Plan authentication exclusions 750](#_Toc153615522)

[Worksheet 751](#_Toc153615523)

[Authentication samples 752](#_Toc153615524)

[SQL membership provider 752](#_Toc153615525)

[Active Directory membership provider 755](#_Toc153615526)

[LDAP membership provider 757](#_Toc153615527)

[Web SSO with AD FS 759](#_Toc153615528)

[XVI Plan for and design security 765](#_Toc153615529)

[Chapter overview: Plan for and design security (Office SharePoint Server) 766](#_Toc153615530)

[Choose your security environment (Office SharePoint Server) 770](#_Toc153615531)

[Internal team or department 770](#_Toc153615532)

[Internal IT-hosted 771](#_Toc153615533)

[External secure collaboration 771](#_Toc153615534)

[External anonymous access 772](#_Toc153615535)

[A Plan server farm security (Office SharePoint Server) 773](#_Toc153615536)

[Subhead 773](#_Toc153615537)

[Subhead 773](#_Toc153615538)

[Chapter overview: Plan server farm security (Office SharePoint Server) 774](#_Toc153615539)

[Review the secure topology design checklists (Office SharePoint Server) 775](#_Toc153615540)

[Server topology design checklist 775](#_Toc153615541)

[Networking topology design checklist 776](#_Toc153615542)

[Logical architecture design checklist 776](#_Toc153615543)

[Operating system design checklist 778](#_Toc153615544)

[Plan for secure communication within a server farm [Office SharePoint Server] 779](#_Toc153615545)

[Plan server-to-server communication 779](#_Toc153615546)

[IPsec 781](#_Toc153615547)

[SSL 781](#_Toc153615548)

[Scenarios to consider for SSL 782](#_Toc153615549)

[Plan client-server communication 782](#_Toc153615550)

[Plan for using SSL 783](#_Toc153615551)

[Plan security hardening for server roles within a server farm [Office SharePoint Server] 784](#_Toc153615552)

[About security hardening 784](#_Toc153615553)

[Application server recommendations 786](#_Toc153615554)

[Secure communication with the Microsoft SQL Server database 787](#_Toc153615555)

[Blocking the standard SQL Server ports 787](#_Toc153615556)

[Configuring SQL Server database instances to listen on a nonstandard port 788](#_Toc153615557)

[Configuring SQL client aliases 788](#_Toc153615558)

[Hardening steps 789](#_Toc153615559)

[Configure SQL Server 789](#_Toc153615560)

[Configure Windows Firewall 792](#_Toc153615561)

[Configure a SQL client alias 793](#_Toc153615562)

[File and Printer Sharing service requirements 794](#_Toc153615563)

[Single sign-on hardening requirements 795](#_Toc153615564)

[Restricting DCOM ports 796](#_Toc153615565)

[Service requirements for e-mail integration 797](#_Toc153615566)

[SMTP service 797](#_Toc153615567)

[Microsoft SharePoint Directory Management Service 797](#_Toc153615568)

[Service requirements for session state 798](#_Toc153615569)

[Office SharePoint Server services 798](#_Toc153615570)

[Accounts and groups 799](#_Toc153615571)

[Web.config file 799](#_Toc153615572)

[Secure snapshot additions 800](#_Toc153615573)

[Plan secure configurations for Office SharePoint Server features 808](#_Toc153615574)

[Recommendations for Office SharePoint Server features 808](#_Toc153615575)

[B Plan environment-specific security (Office SharePoint Server) 822](#_Toc153615576)

[Subhead 822](#_Toc153615577)

[Subhead 822](#_Toc153615578)

[Chapter overview: Plan environment-specific security (Office SharePoint Server) 823](#_Toc153615579)

[Plan security for an internal team or department environment (Office SharePoint Server) 824](#_Toc153615580)

[Secure design checklist 824](#_Toc153615581)

[Plan security hardening for server roles 826](#_Toc153615582)

[Plan secure configurations for Office SharePoint Server features 826](#_Toc153615583)

[Plan security for an internal IT-hosted environment (Office SharePoint Server) 829](#_Toc153615584)

[Secure design checklist 829](#_Toc153615585)

[Plan security hardening for server roles 829](#_Toc153615586)

[Plan secure configurations for Office SharePoint Server features 830](#_Toc153615587)

[Plan security for an external secure collaboration environment (Office SharePoint Server) 831](#_Toc153615588)

[Protect back-end servers 831](#_Toc153615589)

[Secure client-server communication 832](#_Toc153615590)

[Secure the Central Administration site 832](#_Toc153615591)

[Secure Shared Services Provider administration sites 833](#_Toc153615592)

[Secure design checklist 833](#_Toc153615593)

[Plan security hardening for server roles 834](#_Toc153615594)

[Plan secure configurations for Office SharePoint Server features 834](#_Toc153615595)

[Plan security for an external anonymous access environment (Office SharePoint Server) 836](#_Toc153615596)

[Protect back-end servers 836](#_Toc153615597)

[Configure anonymous access 837](#_Toc153615598)

[Secure the Central Administration site 837](#_Toc153615599)

[Secure content deployment 838](#_Toc153615600)

[Disable incoming e-mail 838](#_Toc153615601)

[Use lockdown mode 838](#_Toc153615602)

[Secure design checklist 840](#_Toc153615603)

[Plan security hardening for server roles 840](#_Toc153615604)

[Plan secure configurations for Office SharePoint Server features 841](#_Toc153615605)

[Plan for security roles [Office SharePoint Server] 845](#_Toc153615606)

[Plan for single sign-on 846](#_Toc153615607)

[About single sign-on 846](#_Toc153615608)

[Common SSO scenarios 847](#_Toc153615609)

[Office SharePoint Server SSO architecture 847](#_Toc153615610)

[Microsoft Single Sign-On service 847](#_Toc153615611)

[Enterprise application definitions 849](#_Toc153615612)

[SSO tickets 849](#_Toc153615613)

[SSO administration 850](#_Toc153615614)

[Networking dependencies 850](#_Toc153615615)

[Plan farm-level SSO settings 851](#_Toc153615616)

[SSO encryption-key server 851](#_Toc153615617)

[SSO accounts 852](#_Toc153615618)

[Database settings 859](#_Toc153615619)

[Time-out settings 859](#_Toc153615620)

[Plan enterprise application definition settings 859](#_Toc153615621)

[Application and contact information 860](#_Toc153615622)

[Account type 860](#_Toc153615623)

[Authentication type 861](#_Toc153615624)

[Logon account information for users 861](#_Toc153615625)

[Account information for enterprise application 863](#_Toc153615626)

[Plan for SSO operations 863](#_Toc153615627)

[Managing the encryption key 863](#_Toc153615628)

[Auditing the encryption key 863](#_Toc153615629)

[Regenerating the encryption key 864](#_Toc153615630)

[Backing up the SSO environment 865](#_Toc153615631)

[Restoring the SSO environment 866](#_Toc153615632)

[Change the SSO service account 867](#_Toc153615633)

[Restore only the SSO database server 867](#_Toc153615634)

[Restore the entire SSO environment 868](#_Toc153615635)

[Responding to an SSO security compromise 868](#_Toc153615636)

[Worksheets 869](#_Toc153615637)

[Plan for administrative and service accounts (Office SharePoint Server) 870](#_Toc153615638)

[About administrative and service accounts 870](#_Toc153615639)

[Server farm-level accounts 870](#_Toc153615640)

[SSP accounts 871](#_Toc153615641)

[Windows SharePoint Services Search accounts 873](#_Toc153615642)

[Application pool accounts 874](#_Toc153615643)

[Standard account requirements 874](#_Toc153615644)

[Server farm-level accounts 874](#_Toc153615645)

[SSP accounts 876](#_Toc153615646)

[Windows SharePoint Services Search accounts 879](#_Toc153615647)

[Application pool accounts 881](#_Toc153615648)

[Planning recommendations for accounts 881](#_Toc153615649)

[Secure farm environment 882](#_Toc153615650)

[Server farm-level accounts 882](#_Toc153615651)

[SSP accounts 882](#_Toc153615652)

[Windows SharePoint Services Search accounts 883](#_Toc153615653)

[Application pool accounts 884](#_Toc153615654)

[Single-server environment 884](#_Toc153615655)

[XVII Plan for performance and capacity 886](#_Toc153615656)

[Chapter overview: Plan for performance and capacity (Office SharePoint Server) 887](#_Toc153615657)

[About performance and capacity planning 887](#_Toc153615658)

[Planning for capacity vs. availability 888](#_Toc153615659)

[64-bit vs. 32-bit 888](#_Toc153615660)

[Upgrading from SharePoint Portal Server 2003 889](#_Toc153615661)

[Performance and capacity planning approach 890](#_Toc153615662)

[Performance and capacity planning process 890](#_Toc153615663)

[Terminology 891](#_Toc153615664)

[Plan for software boundaries (Office SharePoint Server) 893](#_Toc153615665)

[Test environment 893](#_Toc153615666)

[Test results 894](#_Toc153615667)

[Throughput changes when creating a site vs. enumerating sites as the number of sites increases 895](#_Toc153615668)

[Throughput vs. number of site collections 896](#_Toc153615669)

[Throughput differences between flat document library vs. document library with folders 897](#_Toc153615670)

[Guidelines for acceptable performance 899](#_Toc153615671)

[Throughput vs. number of Web servers 905](#_Toc153615672)

[User response times 906](#_Toc153615673)

[A Estimate performance and capacity requirements (Office SharePoint Server) 907](#_Toc153615674)

[Subhead 907](#_Toc153615675)

[Subhead 907](#_Toc153615676)

[Chapter overview: Estimate performance and capacity requirements [Office SharePoint Server] 908](#_Toc153615677)

[Windows SharePoint Services collaboration environments (Office SharePoint Server) 909](#_Toc153615678)

[Key characteristics 909](#_Toc153615679)

[Test environment 910](#_Toc153615680)

[Assumptions 910](#_Toc153615681)

[Lab Topology 911](#_Toc153615682)

[Usage profile 911](#_Toc153615683)

[Recommendations 912](#_Toc153615684)

[Hardware recommendations 913](#_Toc153615685)

[Starting-point topologies 913](#_Toc153615686)

[Capacity and performance of scaled-out topologies 914](#_Toc153615687)

[Estimating throughput targets 914](#_Toc153615688)

[Estimate throughput targets 915](#_Toc153615689)

[Estimating disk space requirements 919](#_Toc153615690)

[Database server disk space requirements 919](#_Toc153615691)

[Search server disk space requirements 921](#_Toc153615692)

[Web server disk space requirements 921](#_Toc153615693)

[Performance monitoring 922](#_Toc153615694)

[Web server 922](#_Toc153615695)

[Database server 923](#_Toc153615696)

[Portal collaboration environments 924](#_Toc153615697)

[Excel Services environments 925](#_Toc153615698)

[Document repository environments 926](#_Toc153615699)

[Internet environments 927](#_Toc153615700)

[ISP hosting environments 928](#_Toc153615701)

[Corporate hosting environments 929](#_Toc153615702)

[Additional performance and capacity planning factors (Office SharePoint Server) 930](#_Toc153615703)

[MOSS feature areas 930](#_Toc153615704)

[Search 930](#_Toc153615705)

[Excel Calculation Services 930](#_Toc153615706)

[IPFS 931](#_Toc153615707)

[Client integration 931](#_Toc153615708)

[Outlook 931](#_Toc153615709)

[InfoPath client integration 931](#_Toc153615710)

[Shipped features 931](#_Toc153615711)

[Caching 931](#_Toc153615712)

[Output Caching 932](#_Toc153615713)

[Object Caching 935](#_Toc153615714)

[Disk-based Caching for Binary Large Objects (BLOBs) 938](#_Toc153615715)

[Content Query Web part 939](#_Toc153615716)

[Environmental factors 939](#_Toc153615717)

[Network configuration 940](#_Toc153615718)

[Network security 940](#_Toc153615719)

[Authentication 940](#_Toc153615720)

[Developing custom code 941](#_Toc153615721)

[Tools for performance and capacity planning [Office SharePoint Server] 943](#_Toc153615722)

[About the SharePoint test data load tool 943](#_Toc153615723)

[Constructing a SharePoint test data load configuration file 945](#_Toc153615724)

[Deleting SharePoint test data 945](#_Toc153615725)

[XVIII Plan for and design database storage and management 947](#_Toc153615726)

[TBD Chapter overview: Plan for and design database storage and management 948](#_Toc153615727)

[Plan for backup and restore [Office SharePoint Server] 949](#_Toc153615728)

[Plan for tools 949](#_Toc153615729)

[SharePoint Products and Technologies Backup and Restore Utility 950](#_Toc153615730)

[SQL Server Backup and Restore 950](#_Toc153615731)

[stsadm Utility 950](#_Toc153615732)

[Recycle Bin 951](#_Toc153615733)

[Backup Strategies 952](#_Toc153615734)

[SharePoint Server Database Backups 952](#_Toc153615735)

[Search Index Backups 952](#_Toc153615736)

[Web Front End (WFE) Server Backups 952](#_Toc153615737)

[My Sites Backups 953](#_Toc153615738)

[Windows SharePoint Services Site Backups 953](#_Toc153615739)

[Plan for backup types and schedules 954](#_Toc153615740)

[Backup Types 954](#_Toc153615741)

[Recommended Backup Schedules 954](#_Toc153615742)

[Archiving data for trend analysis 955](#_Toc153615743)

[XIX Plan for server management and operations 956](#_Toc153615744)

[XX Plan for deployment rollout 957](#_Toc153615745)

# Planning worksheets for Office SharePoint Server 2007

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [Planning worksheets by task](#DSDOC_section149cf7edd_14ee_445b_8ab0_1d)

 [Planning worksheets by title](#DSDOC_section249cf7edd_14ee_445b_8ab0_1d)

This article provides links to worksheets that you can use to record information that you gather and decisions that you make as you plan your deployment of Microsoft Office SharePoint Server 2007. Use these worksheets in conjunction with — not as a substitute for — Planning and architecture for Office SharePoint Server 2007.

## Planning worksheets by task

|  |  |  |
| --- | --- | --- |
| For this task | Use this worksheet | To do this |
| [Chapter overview: Plan overall design](#DSDOC_59785dd2_e52e_48f1_9ac0_1d61e6d63c) | [Determine sites worksheet](http://go.microsoft.com/fwlink/?LinkID=73282&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73282&clcid=0x409) | Identify top-level sites needed for the solution and the features to investigate for each site. |
| [Chapter overview: Plan Web site structure and publishing (Office SharePoint Server)](#DSDOC_6a4b0ec4_8802_40f9_87ac_6a6691b544) | [Article pages worksheet](http://go.microsoft.com/fwlink/?LinkId=73316&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73316&clcid=0x409) | Plan fields for content pages. |
|  | [Layout pages worksheet](http://go.microsoft.com/fwlink/?LinkId=73317&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73317&clcid=0x409) | Plan layout pages for Web pages. |
|  | [Master pages worksheet](http://go.microsoft.com/fwlink/?LinkId=73318&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73318&clcid=0x409) | Plan master pages for site collections. |
|  | [Site paths worksheet](http://go.microsoft.com/fwlink/?LinkId=73148&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73148&clcid=0x409) | Record managed paths that need to be created for hosting collaboration sites. |
|  | [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) | Record a plan for creating sites. |
|  | [Welcome pages worksheet](http://go.microsoft.com/fwlink/?LinkId=73320&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73320&clcid=0x409) | Plan fields for welcome pages. |
| [Chapter overview: Plan for personalized content and sites](#DSDOC_50832216_8140_457e_9c4c_8b31eaaef2) | [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) | Plan connections, sources, people features, and audiences. |
|  | [Search properties worksheet](http://go.microsoft.com/fwlink/?LinkID=73272&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73272&clcid=0x409) | Plan properties for search, mapping crawled properties to managed properties. |
|  | [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) | Record a plan for creating sites. |
| [Chapter overview: Plan InfoPath Forms Services](#DSDOC_4ec9c00a_8cb6_407c_9f63_c725ea7c57) | [Data connections for form templates worksheet](http://go.microsoft.com/fwlink/?LinkId=73321&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73321&clcid=0x409) | Plan InfoPath Forms Services data connections. |
|  | [Deploy administrator-approved form template](http://go.microsoft.com/fwlink/?LinkId=73322&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73322&clcid=0x409) | Record information to plan administrator-approved form templates. |
| [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5) | [Authentication methods worksheet](http://go.microsoft.com/fwlink/?LinkID=73278&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73278&clcid=0x409) | Plan and record authentication methods to be allowed in your environment. |
|  | [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) | Plan for information architecture based on the taxonomy of key concepts and business processes. |
|  | [Crawl and query search features worksheet](http://go.microsoft.com/fwlink/?LinkID=73276&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73276&clcid=0x409) | Plan and record crawl and search settings. |
|  | [Custom permission levels and groups worksheet](http://go.microsoft.com/fwlink/?LinkID=73134&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73134&clcid=0x409) | Record custom permission levels and groups that need to be created. |
|  | [Estimate data capacity requirements worksheet](http://go.microsoft.com/fwlink/?LinkID=73274&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73274&clcid=0x409) | Record information to help capacity planning. |
|  | [External data connections worksheet](http://go.microsoft.com/fwlink/?LinkId=73323&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73323&clcid=0x409) | Plan for Excel Services by recording the names of .odc files and the locations of corresponding external data sources. |
|  | [Information architecture worksheet](http://go.microsoft.com/fwlink/?LinkID=73273&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73273&clcid=0x409) | Plan information architecture based on the taxonomy of key concepts and business processes. |
|  | [Search properties worksheet](http://go.microsoft.com/fwlink/?LinkID=73272&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73272&clcid=0x409) | Plan properties for search, mapping crawled properties to managed properties. |
|  | [Site and content security worksheet](http://go.microsoft.com/fwlink/?LinkId=73135&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73135&clcid=0x409) | Record inherited and unique permissions, and record which groups need what level of access. |
|  | [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) | Record a plan for creating sites. |
|  | [Site hierarchy planning tool](http://go.microsoft.com/fwlink/?LinkId=73143&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73143&clcid=0x409) | Create a site hierarchy diagram in Microsoft Office Visio. |
|  | [Trusted data connection libraries worksheet](http://go.microsoft.com/fwlink/?LinkId=73324&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73324&clcid=0x409) | Record the names of trusted data connection libraries. |
|  | [Trusted data providers worksheet](http://go.microsoft.com/fwlink/?LinkId=73325&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73325&clcid=0x409) | Record the names of trusted data providers. |
|  | [Trusted file locations worksheet](http://go.microsoft.com/fwlink/?LinkId=73327&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73327&clcid=0x409) | Record the names of trusted SharePoint sites, Universal Naming Convention paths, and Web sites. |
| [Chapter overview: Plan search (Office SharePoint Server)](#DSDOC_e8c0fccd_8364_4352_8778_c9c46a668b) | [Search team worksheet](http://go.microsoft.com/fwlink/?LinkID=73621&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73621&clcid=0x409) | Determine and record which team members will be involved in planning and implementing your search solution. |
|  | [Plan to crawl content worksheet](http://go.microsoft.com/fwlink/?LinkId=73748&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73748&clcid=0x409) | For each content source, determine what and when to crawl. |
| [Chapter overview: Plan communication [Office SharePoint Server]](#DSDOC_5c9d5c10_a7a8_43d1_ac36_a6f50f2d0c) |  |  |
| [Chapter overview: Plan document management](#DSDOC_cb57d4f7_8353_420b_8a10_d05c9bdf1b) | [Analyze document usage worksheet](http://go.microsoft.com/fwlink/?LinkID=73284&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73284&clcid=0x409) | Record information gathered when analyzing document usage. |
|  | [Content type worksheet](http://go.microsoft.com/fwlink/?LinkID=73288&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73288&clcid=0x409) | Plan a content type. |
|  | [Document libraries worksheet](http://go.microsoft.com/fwlink/?LinkID=73306&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73306&clcid=0x409) | Plan libraries based on sites and on document types. |
|  | [Document management stakeholders and participants worksheet](http://go.microsoft.com/fwlink/?LinkID=73285&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73285&clcid=0x409) | Identify document management planning stakeholders and record document management practices. |
|  | [Policy worksheet](http://go.microsoft.com/fwlink/?LinkID=73307&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73307&clcid=0x409) | Plan information management policies for content types. |
| Plan records management | [Document library for retaining records worksheet](http://go.microsoft.com/fwlink/?LinkID=73298&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73298&clcid=0x409) | Plan a document library for retaining records. |
|  | [Record categories worksheet](http://go.microsoft.com/fwlink/?LinkID=73300&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73300&clcid=0x409) | Plan record categories. |
|  | [Records management stakeholders and participants worksheet](http://go.microsoft.com/fwlink/?LinkId=73330&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73330&clcid=0x409) | Identify records management planning stakeholders and analyze records management practices. |
|  | [Records routing table worksheet](http://go.microsoft.com/fwlink/?LinkID=73303&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73303&clcid=0x409) | Design the records routing table. |
| [Chapter overview: Plan site and content security [Office SharePoint Server]](#DSDOC_85a1866e_2743_4f98_a1ac_9ea61905c6) | [Administrators and owners worksheet](http://go.microsoft.com/fwlink/?LinkId=73126&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73126&clcid=0x409) | Record owners for each site collection and site. |
|  | [Custom permission levels and groups worksheet](http://go.microsoft.com/fwlink/?LinkID=73134&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73134&clcid=0x409) | Record custom permission levels and groups that need to be created. |
|  | [Site and content security worksheet](http://go.microsoft.com/fwlink/?LinkId=73135&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73135&clcid=0x409) | Record inherited and unique permissions, and record which groups need what level of access. |
| [Chapter overview: Plan for site creation and maintenance [Office SharePoint Server]](#DSDOC_58d809cc_8e03_4075_9050_638c976840) | [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) | Record a plan for creating sites. |
|  | [Site maintenance worksheet](http://go.microsoft.com/fwlink/?LinkId=73146&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73146&clcid=0x409) | Record the plan for maintaining sites, including quota values and automatic deletion choices. |
| [Chapter overview: Design server farms and topologies [Office SharePoint Server]](#DSDOC_b474b3dd_b1e3_4d3e_a83c_bc4a6ec4e0) | [Availability plan worksheet](http://go.microsoft.com/fwlink/?LinkId=73333&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73333&clcid=0x409) | Identify redundancy requirements and plan availability options for server roles. |
| [Chapter overview: Design logical architecture](#DSDOC_1a8e707a_a9b9_4cc1_9daa_08d450692d) | [Authentication methods worksheet](http://go.microsoft.com/fwlink/?LinkID=73278&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73278&clcid=0x409) | Plan and record authentication methods to be allowed in your environment. |
|  | [Web application authentication settings worksheet](http://go.microsoft.com/fwlink/?LinkId=73334&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73334&clcid=0x409) | Plan authentication settings for individual Web applications. |
| [Chapter overview: Plan for and design security (Office SharePoint Server)](#DSDOC_3df68222_235b_45de_82fa_b89166c5c6) | [Single sign-on enterprise application definition worksheet](http://go.microsoft.com/fwlink/?LinkId=73335&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73335&clcid=0x409) | Plan settings for individual enterprise application definitions (used with single sign-on). |
|  | [Single sign-on server farm settings worksheet](http://go.microsoft.com/fwlink/?LinkId=73336&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73336&clcid=0x409) | Plan farm-level single sign-on settings. |
| [Chapter overview: Plan for performance and capacity (Office SharePoint Server)](#DSDOC_8dd52916_f77d_4444_b593_1f7d6f330e) | [Estimate data capacity requirements worksheet](http://go.microsoft.com/fwlink/?LinkID=73274&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73274&clcid=0x409) | Record information to help capacity planning. |
|  | [Estimate peak throughput worksheet](http://go.microsoft.com/fwlink/?LinkId=73337&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73337&clcid=0x409) | Record each type of site access to determine peak throughput required. |
| [TBD Chapter overview: Plan for and design database storage and management](#DSDOC_ebbd99e2_98e8_478f_87f3_12f195741b) | [Estimate data capacity requirements worksheet](http://go.microsoft.com/fwlink/?LinkID=73274&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73274&clcid=0x409) | Record information to help capacity planning. |
| Plan for server management and operations |  |  |
| Plan for deployment rollout |  |  |

## Planning worksheets by title

|  |  |  |
| --- | --- | --- |
| Use this worksheet | For this task | To do this |
| [Administrators and owners worksheet](http://go.microsoft.com/fwlink/?LinkId=73126&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73126&clcid=0x409) | [Chapter overview: Plan site and content security [Office SharePoint Server]](#DSDOC_85a1866e_2743_4f98_a1ac_9ea61905c6) | Record owners for each site collection and site. |
| [Analyze document usage worksheet](http://go.microsoft.com/fwlink/?LinkID=73284&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73284&clcid=0x409) | [Chapter overview: Plan document management](#DSDOC_cb57d4f7_8353_420b_8a10_d05c9bdf1b) | Record information gathered when analyzing document usage. |
| [Article pages worksheet](http://go.microsoft.com/fwlink/?LinkId=73316&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73316&clcid=0x409) | [Chapter overview: Plan Web site structure and publishing (Office SharePoint Server)](#DSDOC_6a4b0ec4_8802_40f9_87ac_6a6691b544) | Plan fields for content pages. |
| [Authentication methods worksheet](http://go.microsoft.com/fwlink/?LinkID=73278&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73278&clcid=0x409) | [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5)  [Chapter overview: Design logical architecture](#DSDOC_1a8e707a_a9b9_4cc1_9daa_08d450692d) | Plan and record authentication methods to be allowed in your environment. |
| [Availability plan worksheet](http://go.microsoft.com/fwlink/?LinkId=73333&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73333&clcid=0x409) | [Chapter overview: Design server farms and topologies [Office SharePoint Server]](#DSDOC_b474b3dd_b1e3_4d3e_a83c_bc4a6ec4e0) | Identify redundancy requirements and plan availability options for server roles. |
| [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) | [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5) | Plan for information architecture based on the taxonomy of key concepts and business processes. |
| [Content type worksheet](http://go.microsoft.com/fwlink/?LinkID=73288&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73288&clcid=0x409) | [Chapter overview: Plan document management](#DSDOC_cb57d4f7_8353_420b_8a10_d05c9bdf1b) | Plan a content type. |
| [Crawl and query search features worksheet](http://go.microsoft.com/fwlink/?LinkID=73276&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73276&clcid=0x409) | [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5)  [Chapter overview: Plan search (Office SharePoint Server)](#DSDOC_e8c0fccd_8364_4352_8778_c9c46a668b) | Plan and record crawl and search settings. |
| [Custom permission levels and groups worksheet](http://go.microsoft.com/fwlink/?LinkID=73134&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73134&clcid=0x409) | [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5)  [Chapter overview: Plan site and content security [Office SharePoint Server]](#DSDOC_85a1866e_2743_4f98_a1ac_9ea61905c6) | Record custom permission levels and groups that need to be created. |
| [Data connections for form templates worksheet](http://go.microsoft.com/fwlink/?LinkId=73321&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73321&clcid=0x409) | [Chapter overview: Plan InfoPath Forms Services](#DSDOC_4ec9c00a_8cb6_407c_9f63_c725ea7c57) | Plan InfoPath Forms Services data connections. |
| [Deploy administrator-approved form template](http://go.microsoft.com/fwlink/?LinkId=73322&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73322&clcid=0x409) | [Chapter overview: Plan InfoPath Forms Services](#DSDOC_4ec9c00a_8cb6_407c_9f63_c725ea7c57) | Record information to plan administrator-approved form templates. |
| [Determine sites worksheet](http://go.microsoft.com/fwlink/?LinkID=73282&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73282&clcid=0x409) | [Chapter overview: Plan overall design](#DSDOC_59785dd2_e52e_48f1_9ac0_1d61e6d63c) | Identify top-level sites needed for the solution and the features to investigate for each site. |
| [Document libraries worksheet](http://go.microsoft.com/fwlink/?LinkID=73306&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73306&clcid=0x409) | [Chapter overview: Plan document management](#DSDOC_cb57d4f7_8353_420b_8a10_d05c9bdf1b) | Plan libraries based on sites and on document types. |
| [Document library for retaining records worksheet](http://go.microsoft.com/fwlink/?LinkID=73298&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73298&clcid=0x409) | Plan records management | Plan a document library for retaining records. |
| [Document management stakeholders and participants worksheet](http://go.microsoft.com/fwlink/?LinkID=73285&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73285&clcid=0x409) | [Chapter overview: Plan document management](#DSDOC_cb57d4f7_8353_420b_8a10_d05c9bdf1b) | Identify document management planning stakeholders and record document management practices. |
| [Estimate data capacity requirement](http://go.microsoft.com/fwlink/?LinkID=73274&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73274&clcid=0x409) | [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5)  [Chapter overview: Plan for performance and capacity (Office SharePoint Server)](#DSDOC_8dd52916_f77d_4444_b593_1f7d6f330e)  [TBD Chapter overview: Plan for and design database storage and management](#DSDOC_ebbd99e2_98e8_478f_87f3_12f195741b) | Record information to help capacity planning. |
| [Estimate peak throughput worksheet](http://go.microsoft.com/fwlink/?LinkId=73337&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73337&clcid=0x409) | [Chapter overview: Plan for performance and capacity (Office SharePoint Server)](#DSDOC_8dd52916_f77d_4444_b593_1f7d6f330e) | Record each type of site access to determine peak throughput required. |
| [External data connections worksheet](http://go.microsoft.com/fwlink/?LinkId=73323&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73323&clcid=0x409) | [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5) | Plan for Excel Services by recording the names of .odc files and the locations of corresponding external data sources. |
| [Information architecture worksheet](http://go.microsoft.com/fwlink/?LinkID=73273&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73273&clcid=0x409) | [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5) | Plan information architecture based on the taxonomy of key concepts and business processes. |
| [Layout pages worksheet](http://go.microsoft.com/fwlink/?LinkId=73317&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73317&clcid=0x409) | [Chapter overview: Plan Web site structure and publishing (Office SharePoint Server)](#DSDOC_6a4b0ec4_8802_40f9_87ac_6a6691b544) | Plan layout pages for Web pages. |
| [Master pages worksheet](http://go.microsoft.com/fwlink/?LinkId=73318&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73318&clcid=0x409) | [Chapter overview: Plan Web site structure and publishing (Office SharePoint Server)](#DSDOC_6a4b0ec4_8802_40f9_87ac_6a6691b544) | Plan master pages for site collections. |
| [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) | [Chapter overview: Plan for personalized content and sites](#DSDOC_50832216_8140_457e_9c4c_8b31eaaef2) | Plan connections, sources, people features, and audiences. |
| [Policy worksheet](http://go.microsoft.com/fwlink/?LinkID=73307&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73307&clcid=0x409) | [Chapter overview: Plan document management](#DSDOC_cb57d4f7_8353_420b_8a10_d05c9bdf1b) | Plan information management policies for content types. |
| [Record categories worksheet](http://go.microsoft.com/fwlink/?LinkID=73300&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73300&clcid=0x409) | Plan records management | Plan record categories. |
| [Records management stakeholders and participants worksheet](http://go.microsoft.com/fwlink/?LinkId=73330&clcid=0x409) (http http://go.microsoft.com/fwlink/?LinkId=73330&clcid=0x409) | Plan records management | Identify records management planning stakeholders and analyze records management practices. |
| [Records routing table worksheet](http://go.microsoft.com/fwlink/?LinkID=73303&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73303&clcid=0x409) | Plan records management | Design the records routing table. |
| [Search properties worksheet](http://go.microsoft.com/fwlink/?LinkID=73272&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73272&clcid=0x409) | [Chapter overview: Plan for personalized content and sites](#DSDOC_50832216_8140_457e_9c4c_8b31eaaef2)  [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5)  [Chapter overview: Plan search (Office SharePoint Server)](#DSDOC_e8c0fccd_8364_4352_8778_c9c46a668b) | Plan properties for search, mapping crawled properties to managed properties. |
| [Single sign-on enterprise application definition worksheet](http://go.microsoft.com/fwlink/?LinkId=73335&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73335&clcid=0x409) | [Chapter overview: Plan for and design security (Office SharePoint Server)](#DSDOC_3df68222_235b_45de_82fa_b89166c5c6) | Plan settings for individual enterprise application definitions (used with single sign-on). |
| [Single sign-on server farm settings worksheet](http://go.microsoft.com/fwlink/?LinkId=73336&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73336&clcid=0x409) | [Chapter overview: Plan for and design security (Office SharePoint Server)](#DSDOC_3df68222_235b_45de_82fa_b89166c5c6) | Plan farm-level single sign-on settings. |
| [Site and content security worksheet](http://go.microsoft.com/fwlink/?LinkId=73135&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73135&clcid=0x409) | [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5)  [Chapter overview: Plan site and content security [Office SharePoint Server]](#DSDOC_85a1866e_2743_4f98_a1ac_9ea61905c6) | Record inherited and unique permissions; record which groups need what level of access. |
| [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) | [Chapter overview: Plan for personalized content and sites](#DSDOC_50832216_8140_457e_9c4c_8b31eaaef2)  [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5)  [Chapter overview: Plan for site creation and maintenance [Office SharePoint Server]](#DSDOC_58d809cc_8e03_4075_9050_638c976840)  [Chapter overview: Plan Web site structure and publishing (Office SharePoint Server)](#DSDOC_6a4b0ec4_8802_40f9_87ac_6a6691b544) | Record a plan for creating sites. |
| [Site hierarchy planning tool](http://go.microsoft.com/fwlink/?LinkId=73143&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73143&clcid=0x409) | [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5) | Create a site hierarchy diagram in Microsoft Office Visio. |
| [Site maintenance worksheet](http://go.microsoft.com/fwlink/?LinkId=73146&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73146&clcid=0x409) | [Chapter overview: Plan for site creation and maintenance [Office SharePoint Server]](#DSDOC_58d809cc_8e03_4075_9050_638c976840) | Record the plan for maintaining sites, including quota values and automatic deletion choices. |
| [Site paths worksheet](http://go.microsoft.com/fwlink/?LinkId=73148&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73148&clcid=0x409) | [Chapter overview: Plan Web site structure and publishing (Office SharePoint Server)](#DSDOC_6a4b0ec4_8802_40f9_87ac_6a6691b544) | Record managed paths that need to be created for hosting collaboration sites. |
| [Trusted data connection libraries worksheet](http://go.microsoft.com/fwlink/?LinkId=73324&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73324&clcid=0x409) | [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5) | Record the names of trusted data connection libraries. |
| [Trusted data providers worksheet](http://go.microsoft.com/fwlink/?LinkId=73325&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73325&clcid=0x409) | [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5) | Record the names of trusted data providers. |
| [Trusted file locations worksheet](http://go.microsoft.com/fwlink/?LinkId=73327&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73327&clcid=0x409) | [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5) | Record the names of trusted SharePoint sites, Universal Naming Convention paths, and Web sites. |
| [Web application authentication settings worksheet](http://go.microsoft.com/fwlink/?LinkId=73334&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73334&clcid=0x409) | [Chapter overview: Design logical architecture](#DSDOC_1a8e707a_a9b9_4cc1_9daa_08d450692d) | Plan authentication settings for individual Web applications. |
| [Welcome pages worksheet](http://go.microsoft.com/fwlink/?LinkId=73320&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73320&clcid=0x409) | [Chapter overview: Plan Web site structure and publishing (Office SharePoint Server)](#DSDOC_6a4b0ec4_8802_40f9_87ac_6a6691b544) | Plan fields for welcome pages. |

# I Plan overall design

In this chapter:

 [Chapter overview: Plan overall design](#DSDOC_59785dd2_e52e_48f1_9ac0_1d61e6d63c)

 [Plan sites and features](#DSDOC_cb6871cc_7fc5_4b54_9940_8c0ed51cb0)

# Chapter overview: Plan overall design

In this article:

 [How to use this Planning Guide](#DSDOC_section159785dd2_e52e_48f1_9ac0_1d)

 [What is Microsoft Office SharePoint Server 2007?](#DSDOC_section259785dd2_e52e_48f1_9ac0_1d)

 [Examples of solutions based on Office SharePoint Server 2007](#DSDOC_section359785dd2_e52e_48f1_9ac0_1d)

 [Establishing the planning team](#DSDOC_section459785dd2_e52e_48f1_9ac0_1d)

## How to use this Planning Guide

The content in this planning guide is designed to lead a team through the steps of planning and deploying a new solution based on Microsoft Office SharePoint Server 2007. The audiences for this guide are business application specialists, line of business specialists, information architects, IT generalists, program managers, and infrastructure specialists who are planning a solution based on Office SharePoint Server 2007. Before using this guide, we recommend that you:

 Review the Product Evaluation for Office SharePoint Server 2007 to learn about the features of Office SharePoint Server 2007. This will help ensure that Office SharePoint Server 2007 meets your functional and IT needs, and it will help you envision and plan your solution.

 Define the organizational goals you want to achieve with a solution based on Office SharePoint Server 2007.

 Define the vision and scope of the solution.

This planning guide has been organized into two stages. The first stage guides you in determining the types of Web sites your organization needs, the features of each site, and the interactions among the sites that meet your enterprise goals. Out of this stage of planning, you will develop a set of worksheets that will help determine the details of your site and feature needs. These worksheets will help you record information such as:

 Sites and site hierarchies

 Relationships between sites

 Features of sites

 Site customizations

Along with filling in the worksheets that accompany this document, we recommend that you incorporate your site and feature planning decisions into a conceptual design document that:

 Defines the purpose of the solution you are planning

 Describes the implementation of the solution

 Provides data, flowcharts, illustrations, and other information needed to plan the solution deployment

After you have determined how your solution will work, the second planning stage guides you in making a series of deployment planning decisions. In this stage, you will develop a set of worksheets that will help determine the implementation of your deployment. These worksheets will help you record information such as:

 Deployment design

 Physical topologies

 Database design

 Security design

 Service-level agreements

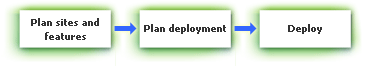
Along with filling in the worksheets that accompany this document, we recommend that you incorporate your deployment planning decisions into a design specification document that:

 Defines hardware requirements

 Describes the physical system design

 Provides data, diagrams, and other information useful to the team implementing the deployment

After you plan your sites and features and plan the deployment, the Deployment for Office SharePoint Server 2007 guide will guide you in implementing your Office SharePoint Server 2007 deployment. The process is illustrated below:



This guide includes a companion set of worksheets for recording information related to your planning and deployment activities. To best achieve your solution planning and deployment goals, use the supplied worksheets to record the results of your planning decisions as you use this guide.

note_ddNote:

For a description of the steps needed to plan the migration and deployment of an existing solution to Office SharePoint Server 2007, see Upgrading to Office SharePoint Server 2007.

## What is Microsoft Office SharePoint Server 2007?

Microsoft Office SharePoint Server 2007 is a rich server application for the enterprise that facilitates collaboration, provides full content management features, implements business processes, and provides access to information essential to organizational goals and processes. It provides an integrated platform to plan, deploy, and manage intranet, extranet, and Internet applications across and beyond the enterprise.

Office SharePoint Server 2007 facilitates the creation and deployment of feature-rich and content-rich Web sites, including organizational portal sites, Internet presence sites, team collaboration sites, and specialized sites such as content repositories or meeting workspaces. Although Office SharePoint Server 2007 is customizable and has a rich object model, it comes with a full set of features, such as ready-to-use Web site and portal templates, Web Parts, lists, libraries, workflows, and site variations to tailor content to different cultures, markets, and geographic regions.

By using Office SharePoint Server 2007, you can plan and implement business processes that integrate with existing systems by means of XML-based electronic forms and the Business Data Catalog. Workflows included in Office SharePoint Server 2007 automate common business processes such as document review and approval, issue tracking, and signature collection. Office SharePoint Server 2007 workflows are based on the Windows Workflow Foundation, and Office SharePoint Server 2007 supports developing and deploying custom workflows to implement enterprise-specific business processes.

Solutions based on Office SharePoint Server 2007 can provide organization-wide access to business intelligence and other information stored in Office SharePoint Server 2007 or in line-of-business systems such as SAP. The Business Data Catalog enables you to include data from back-end systems in lists, Web Parts, pages, and search results. Excel Services provides access to real-time, interactive Office Excel 2007 spreadsheets from a Web browser. You can plan to integrate reports, key performance indicators, and business dashboards into your solution. Office SharePoint Server 2007 search provides access to information, people, and expertise.

You can plan and implement content management solutions based on Office SharePoint Server 2007. Microsoft Content Management Server 2002 functionality has been integrated into Office SharePoint Server 2007 and enhanced to support authoring, staging, and publishing custom Web sites. Office SharePoint Server 2007 document management features support each stage of documents' life cycles, from template creation to document authoring, reviewing, sharing, auditing, and ultimately archiving or destroying. Records management capabilities built into Office SharePoint Server 2007 help your enterprise collect, manage, and dispose of corporate records in a consistent and uniform manner based on your company's policies.

Because Office SharePoint Server 2007 is built on and includes the full features of Microsoft Windows SharePoint Services 3.0, it is an ideal tool for collaboration. Windows SharePoint Services 3.0 provides a consistent, familiar framework for lists and document libraries, site administration, and site customization. The extensible Windows SharePoint Services 3.0 framework facilitates building custom solutions that span multiple sites and complex architectures.

For a full Office SharePoint Server 2007 product and feature overview, see the Product Evaluation for Office SharePoint Server 2007 guide.

## Examples of solutions based on Office SharePoint Server 2007

Here are examples of typical solutions that can be built using Microsoft Office SharePoint Server 2007:

 Online news magazine   A publishing organization uses Office SharePoint Server 2007 to build their branded online magazine site. Article submissions come from inside and outside the organization to be reviewed and accepted by staff editors. This Internet site has a strong community presence because users can log on for personalized information, and it has an extensive search component.

The Internet site includes subsites for current news and editorials; blogs; and regular columns about politics, business, health, people, personal finance, and science and technology. The site also enables users to sign in to interact with each other and to comment on articles published on the site.

 Controlled distribution of financial data to clients and business partners   A bank deploys a solution based on Office SharePoint Server 2007 to take advantage of Excel Services. The solution enables bank managers to communicate efficiently with clients by providing controlled access to specified workbooks that can be rendered with view-only permissions in a Web browser. The workbooks are accessible in document libraries on a portal; this enables the bank to restrict the availability of financial data to clients who have authenticated access to the portal.

 Online permit application   A local government agency uses Office SharePoint Server 2007 and Microsoft Office InfoPath 2007 to provide permit application and approval to contractors over the Internet. Contractors use the Web site to apply for permits using an online service. Data entered into the permit application Web form is submitted to a database in the government's Department of Building Inspections network.

After the application data is submitted, a new permit request (a multi-part Office InfoPath 2007 form) is automatically populated to a workspace. When the form is opened, the requesting contractor's company and permit application data is populated into the form's fields. If the request is approved, an electrical permit (also populated with the requestor's contact data and relevant information) is rendered in HTML and posted to the Department of Building Inspections permit site, where the contractor can view and print the permit for posting at the construction site.

 Departmental portal site   A product development department within a medium-sized company uses Office SharePoint Server 2007 to take advantage of its search, content aggregation, business application integration, collaboration, and personalization features. The department develops a portal site that becomes an essential part of the product development process, hosting their knowledge base, product specifications, an organization chart, individual My Sites for team members, and a home page that broadcasts schedule information, product success stories, and other important news. The installation grows from an isolated small server farm into a well-developed medium server farm implementation that uses a combination of intra-farm and inter-farm shared services within a larger deployment across the entire company.

 Equity research   A large investment bank uses Office SharePoint Server 2007 to develop a set of Web sites that facilitate quickly developing, reviewing, and publishing equities research notes, reports, and models in a variety of formats. Using the integrated Office SharePoint Server 2007 platform, the solution designers implement a portal site for authoring and reviewing research notes and models; an Internet site for presenting the content to customers; a staging site to test the Internet site; and a records repository site for retaining models and research notes to meet regulatory requirements. Using custom features, the set of sites (distributed over multiple server farms) supports the rapid and automated flow of content from site to site and from team member to team member as content moves through its stages toward publication.

 Records management   An appliance manufacturer's legal division implements a records management solution using the Office SharePoint Server 2007 Record Repository site template. Based on their file plan, the division implements and configures policies, content types, and document libraries to retain each type of record the division manages. The records managers adjust easily to the record repository site's familiar SharePoint interface while taking advantage of its built-in records management features. These features support properly storing incoming records, retaining each type of record for the legally mandated period, putting records on hold, and approving of their disposition. The records management programmable interface let teams in the organization integrate their document management and e-mail systems with the record repository site using the Web service APIs.

 Corporate Internet presence site   An international automobile manufacturer has headquarters in Germany; a major subsidiary in Michigan serving the North American market; and regional offices throughout Europe, Asia, and North America. The products are sold internationally, and distinct manufacturing operations serve each regional market. The company's Internet presence Web site is built, administered, and authored using Office SharePoint Server 2007. It is the focal point for the corporate marketing efforts, and it includes subsites for each product line along with areas for press releases, investment information, company information, and career opportunities.

Each corporate brand has its own marketing department with individuals responsible for writing that brand's content and updating it on the Web site. The corporate communication department controls the look and feel of the site to make sure the branding and messaging are consistent. The site includes site variations that tailor its content to different languages, cultures, markets, and geographic regions.

Using Office SharePoint Server 2007 Web sites, the writers for each brand author the site's content and route it for review and approval while managing the creation of multilingual content versions. Using scheduled workflows, the approved and localized content is copied to staging sites where it is tested and ultimately deployed to the public site.

## Establishing the planning team

A well-planned solution based on Microsoft Office SharePoint Server 2007 will promote better collaboration, content management, knowledge discovery, and business processes across your organization while being secure, cost-effective, and manageable for your IT department. To satisfy this broad set of goals, it is important to identify key stakeholders across all relevant disciplines and include them in your planning team. They include:

 Managers and other organizational leaders who understand the requirements of the business processes that Office SharePoint Server 2007 will be used to implement.

 IT professionals and business unit IT specialists who will be tasked with proposing a solution that implements the desired business processes, and with deploying and maintaining the solution across one or more server farms.

 Site designers to plan the user experience and visual design of the sites and the templates that will comprise the solution.

 Developers to determine the scope and design of required custom features, such as workflows, forms, and Web Parts.

 Testers who will ensure that the site's features are correct and that site deployment and administration function as specified.

# Plan sites and features

In this article:

 [Plan sites](#DSDOC_section1cb6871cc_7fc5_4b54_9940_8c)

 [Plan site collections](#DSDOC_section2cb6871cc_7fc5_4b54_9940_8c)

 [Plan security](#DSDOC_section3cb6871cc_7fc5_4b54_9940_8c)

 [Plan search needs](#DSDOC_section4cb6871cc_7fc5_4b54_9940_8c)

 [Plan business intelligence integration](#DSDOC_section5cb6871cc_7fc5_4b54_9940_8c)

 [Plan document and records management](#DSDOC_section6cb6871cc_7fc5_4b54_9940_8c)

 [Plan workflows](#DSDOC_section7cb6871cc_7fc5_4b54_9940_8c)

 [Plan forms](#DSDOC_section8cb6871cc_7fc5_4b54_9940_8c)

 [Plan site maintenance](#DSDOC_section9cb6871cc_7fc5_4b54_9940_8c)

 [Worksheet](#DSDOC_section10cb6871cc_7fc5_4b54_9940_8)

One outcome of planning a solution based on Microsoft Office SharePoint Server 2007 is a determination of the types of Web sites and portal sites to implement, and a list of the features that you need to plan for each site. Record this information in the Determine Sites and Portals planning worksheet.

As you fill out the worksheet, use the guidelines in this article to list the types of portal sites, Internet presence sites, and other site types you need for your solution, and then list for each site:

 The sets of users who will participate in the site or portal. When you know who the site serves, you can more easily determine the appropriate security settings for the site.

 Requirements for searching.

 Customization needs.

 Personalization needs.

 Features that you need to plan for each portal or site, such as business intelligence, document management, forms, or workflows.

## Plan sites

The first step in planning a solution based on Microsoft Office SharePoint Server 2007 is to determine the set of portal sites, Internet presence sites, team sites, and specialized sites that your organization and its customers need. Determining this affects subsequent planning decisions, such as where the sites will be implemented in your server topology, what features to plan for each site, how processes that span multiple sites are implemented, and how information is made available across one or more sites.

|  |
| --- |
| Worksheet action |
| As you plan the set of portal sites, Internet sites, and other sites, list each site separately in the [Determine Sites and Portals planning worksheet](http://go.microsoft.com/fwlink/?LinkId=73282&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73282&clcid=0x409). |

### Plan portal sites

Portal sites based on Office SharePoint Server 2007 provide a focal point for finding relevant, personalized information in an organization. You can plan divisional and rollup portal sites that are based on the scale and structure of your organization and that aggregate organizational information, and you can plan interactive application portals where team members can perform tasks in your organization.

#### Planning portal sites by organizational hierarchy

Plan the basic portal sites you need based on the scale and structure of your organization. Each of these portal sites should contain information needed for a project or division within your larger organization, and each will link to collaboration sites relevant to that project or division. Some portal sites for larger divisions or projects will also aggregate information found on all the smaller portal sites devoted to smaller divisions or projects.

Use the following guidelines when planning portal sites based on your organizational structure:

Divisional or team portal sites   Plan to create one portal site for an entire small organization, or one for every division or project of 50–100 people within a medium-sized to large organization. In large organizations, there might be several levels of portal sites, with each portal site focusing on the content created and managed at its level of the organization.

You can design a portal site for members of your organization to collaborate on content related to your business or organizational goals. These can be self-contained or they can work with other sites as part of a publishing process. Often, these portal sites will have a mixture of collaborative content used internally and content intended for publication to an audience.

Rollup portal sites   A rollup portal site contains general cross-organization content. It lets users across divisions find information, experts, and access to organization-wide processes. It often contains subsites that are scoped to the overall organizational information architecture and are usually mapped to the structure of the divisional or project portal sites. For each organization or distinct Shared Services Provider (SSP), plan to create a centralized rollup portal site with an aggregated view of all related portal sites.

#### Planning application portal sites

An application portal organizes team processes and provides mechanisms for running them. Application portals often include digital dashboards and other features for viewing and manipulating data related to the portal's purpose. The information presented in an application portal site usually comes from diverse sources, such as databases or other SharePoint sites.

For example, the human resources organization in an enterprise could design an application portal site to provide employees with:

 Access to general information such as employee handbooks and career opportunities.

 Ways to do common tasks, such as submitting timecards and expense reports.

 Dashboards for viewing personalized information such as an employee's salary and benefits history.

As another example, the internal technical support organization in an enterprise could design a Help Desk application portal to provide technical support to members of the enterprise. Features of the application portal could include:

 Access to a knowledge base of past support incidents and best-practices documentation.

 Ways to do common tasks, such as starting a support incident or reviewing the status of an ongoing incident.

 Integration with communications features that support online meetings and discussions.

 Personalized views of data. For example, support managers could view dashboards providing views of their team members' productivity and customer satisfaction ratings. Support engineers could view their current unresolved incidents.

In the Determine Sites and Portals planning worksheet, list each divisional, rollup, and application portal site that you plan to create. Be sure to identify the name and purpose of the portal site. For more information about planning portal sites, see Chapter overview: Plan site structure and navigation.

### Plan Internet presence sites

Internet presence sites are customer-facing sites. They are usually branded and are characterized by consistent stylistic elements, such as colors, fonts, and logos in addition to structural elements such as navigation features and the structure of site pages. Although the appearance of an Internet site is tightly controlled, the content of the site may be dynamic and may change frequently.

For example, a corporate presence Internet site communicates important company information to customers, partners, investors, and potential employees, including descriptions of products and services, company news, annual reports, public filings, and job openings. As another example, an online news Internet site provides frequently updated information, along with interactive features such as stock tickers and blogs.

Because an Internet presence site represents your enterprise to an external audience, you might stage and test the site and then publish it — either based on a schedule or as needed — to its public "production" location. A staging site is a mirror of the production site that you use to test content before it's published. Using a staging site can help ensure that published content meets stringent standards. Staging sites also allow content authors to work on servers located on your company's intranet, while Internet users are using production servers in your perimeter network. A built-in content deployment feature makes it easy to move content from the staging to the production servers.

Record your staging and production Internet presence sites in the Determine Sites and Portals planning worksheet. For more information about planning Internet presence sites, see [Chapter overview: Plan Web site structure and publishing (Office SharePoint Server)](#DSDOC_6a4b0ec4_8802_40f9_87ac_6a6691b544).

### Plan other sites

You can plan to allow portal site or Internet site users to create additional sites. For example, you can plan to give each team member who uses a portal site a My Site, which is a team site based on Microsoft Windows SharePoint Services 3.0 with public and private views. You can also allow team members to create other sites, such as Document Workspace sites, as they collaborate. Similarly, you can give users of an Internet site access to collaboration sites as part of a Web-based service. For example, you can give them permissions to create Meeting Workspace sites and participate in online meetings as part of their experience of using your site.

In addition to portal sites and Internet sites, Office SharePoint Server 2007 includes the ability to create the following specialized sites of use in the organization:

Document Center site   This is a large-scale library useful as an enterprise-wide knowledge base or historical archive. It includes features that can help users navigate, search, and manage a large number of documents in a deep hierarchy by using a set of specialized Web Parts.

Records Center site   Records management is the management of files and documents that provide evidence of activities or transactions performed by the organization. The Records Center site is designed to implement the storage component of a records management solution based on Office SharePoint Server 2007.

Record your other site needs in the Determine Sites and Portals planning worksheet. For more information about collaboration site planning, see [Plan for collaboration sites](#DSDOC_437a9043_e55b_4b52_b578_dd3fdee340). For more information about Document Center sites, see [Plan document libraries](#DSDOC_33b67ac7_54c3_42d8_87cd_5d7a00f729). For more information about Records Center sites, see [Design the Records Center site (Office SharePoint Server 2007)](#DSDOC_03702c06_3e32_409d_ad8c_7e84eae386).

### Plan customizations

You can plan to customize your portal sites, Internet sites, or team sites. For example, if you are planning a site to provide an Internet presence for your enterprise, you can brand the site by customizing its master pages to include your organization's logo and color scheme.

You can also customize your site by adding functionality. Office SharePoint Server 2007 has a complete object model and is built on the .NET framework. For more information about programming Office SharePoint Server 2007, see the Office SharePoint Server 2007 Software Development Kit.

For each site or portal that requires customization, make a note in the Customization column of the Determine Sites and Portals planning worksheet. For more information about customization, see [Chapter overview: Plan Web site structure and publishing (Office SharePoint Server)](#DSDOC_6a4b0ec4_8802_40f9_87ac_6a6691b544).

### Plan personalization sites

A personalization site is a filtered view of the content of a portal site or Internet site that provides users of that site with targeted content based on the user's role or preferences. When you plan a portal or Internet site based on Office SharePoint Server 2007, you can design a personalization site based on that site. Users can then choose to view the general content displayed by the portal or Internet site or they can view the related personalization site, which filters the content so that it is more relevant to a particular user's specific information needs or tasks.

If you plan to design a personalization site for any site you listed in the Determine Sites and Portals planning worksheet, record your decision in the Personalization column of the worksheet. For more information about personalization sites, see [Chapter overview: Plan for personalized content and sites](#DSDOC_50832216_8140_457e_9c4c_8b31eaaef2).

## Plan site collections

After you determine which sites and portal sites your solution requires, the next step is to plan how these sites and portals are implemented across site collections. A site collection is a hierarchical set of sites that can be managed together. Sites within a site collection have common features, such as shared permissions, galleries for templates, content types, and Web Parts, and they often share a common navigation. All sites in a site collection are stored together in the same SQL database. A portal site is often implemented as a site collection with the top-level Web site as the home page of the portal.

In general, when planning a solution based on Microsoft Office SharePoint Server 2007, put each of the following types of sites in separate site collections:

 Portal sites

 Internet sites (staging)

 Internet sites (production)

 All team sites related to a portal site or Internet site

 Document Center sites

 Records Center sites

For more information about planning Office SharePoint Server 2007 site collections, see [Chapter overview: Plan Web site structure and publishing (Office SharePoint Server)](#DSDOC_6a4b0ec4_8802_40f9_87ac_6a6691b544).

## Plan security

Planning security includes planning for authentication and authorization of users and groups of users. Authentication is the process by which Office SharePoint Server verifies who a user is. Authorization determines what actions a user is allowed to perform on a given object such as a list item, a library, or a site.

Elements of security planning include:

 Determining the authentication methods to use.

 Determining the categories of users of your solution.

 Determining permission levels to assign to users and groups.

 Planning groups of users and assigning those groups permissions.

 Planning the scopes at which permissions will be applied, such as lists, libraries, or sites.

For more information about planning Office SharePoint Server 2007 security, see Chapter overview: Plan site and content security.

## Plan search needs

Planning search includes determining the scope of content that can be searched from each site, configuring your server farms to index the content and search for it efficiently and securely, and optionally planning customizations of the search user interface. Depending on your requirements, the search scopes in different sites can vary widely. For example, in a portal site used to plan and create products, the scope of searching could include product specifications, internal marketing documents, meeting notes, and other information of internal value. The scope of search in the Internet site in which the public learns about these products would be limited to content describing your organization's products and services, but not the internal content.

In preparation for search planning, for each site or portal site in your Determine Sites and Portals planning worksheet, indicate the scope of what can be searched for by each set of users. For more information about search planning, see [Chapter overview: Plan search (Office SharePoint Server)](#DSDOC_e8c0fccd_8364_4352_8778_c9c46a668b).

## Plan business intelligence integration

Business intelligence enables the members of an organization to gather, store, analyze, and access business data. Office SharePoint Server 2007 includes business intelligence capabilities that help organizations preserve data integrity while enabling powerful data searching, integration, analysis, rendering, and sharing.

In preparation for business intelligence planning, in the Business Intelligence column of your Determine Sites and Portals planning worksheet, indicate all sites and portal sites that require business intelligence integration. For more information about business intelligence planning, see [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5).

## Plan document and records management

A document management system is implemented to control the flow of documents in your organization — how they are created, reviewed, published, and consumed, and how they are ultimately disposed of or retained. Because nearly all solutions will include these activities, expect to plan a document management implementation. Document management planning considerations include how content will be organized in document libraries, the metadata to define for each type of content, the workflows that will be required during the content's lifecycle, and the policies to apply to the content.

A record is a document or other physical or electronic entity in an organization that serves as evidence of an activity or transaction performed by the organization. Records management is the process by which an organization determines what types of information are records, how to manage them through their retention periods, and how to ultimately destroy or archive them. Office SharePoint Server 2007 includes features that help organizations implement records management systems and processes. Work with your organization's legal department to determine if records management should be included in your solution.

In preparation for document and records management planning, in the Document and Records Management column of your Determine Sites and Portals planning worksheet, indicate all sites and portals that require document or records management planning. For more information about document management planning, see [Chapter overview: Plan document management](#DSDOC_cb57d4f7_8353_420b_8a10_d05c9bdf1b). For more information about records management planning, see [Chapter overview: Plan records management](#DSDOC_271017e8_7f23_4166_9501_140ad2fc55).

## Plan workflows

Workflows implement business processes on documents, Web pages, and list items in Microsoft Office SharePoint Server 2007. For example, a workflow can route a document for review, track an issue through its various stages of resolution, or guide a contract through an approval process. Office SharePoint Server 2007 includes workflows that address primary content management needs, such as reviewing or approving documents for publication, along with specialized workflows for tracking issues, managing multiple language translations of content, and managing other processes. You can create custom workflows using Microsoft Visual Studio 2005 or Office SharePoint Designer 2007.

To prepare for workflow planning, in the Workflows column of your Determine Sites and Portals planning worksheet, indicate all sites and portals that require workflow planning. For more information about planning workflows, see Plan workflows (2).

## Plan forms

In a solution based on Office SharePoint Server 2007, forms can be used to gather information and display data from a variety of sources, to automate business processes, and to enhance collaboration scenarios. For example, for an Internet site, you can plan to use forms to survey current users and to sign up new users. For a human resources portal site, you can plan to use forms for submitting timecard information, selecting benefits, or reviewing the performance of employees.

To prepare for forms planning, in the Forms column of your Determine Sites and Portals planning worksheet, list all sites and portals that require forms planning. For more information about planning for forms, see [Chapter overview: Plan InfoPath Forms Services](#DSDOC_4ec9c00a_8cb6_407c_9f63_c725ea7c57).

## Plan site maintenance

Site maintenance includes:

 Planning for site cleanup and general site management.

 Determining how you will let site users create team sites and other subsites, and how to track these sites.

 Finding and removing stale sites.

 Keeping the performance of your portals and Internet sites at an acceptable level.

Because you need to plan site maintenance for all your sites and portals, you do not need to register this in your Determine Sites and Portals planning worksheet. For a full discussion of site maintenance planning, see [Chapter overview: Plan for site creation and maintenance [Office SharePoint Server]](#DSDOC_58d809cc_8e03_4075_9050_638c976840).

## Worksheet

Use the following worksheet to record the information discussed in this article:

 [Determine Sites and Portals planning worksheet](http://go.microsoft.com/fwlink/?LinkId=73282&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73282&clcid=0x409)

# Plan Shared Services Providers

This content is preliminary content. It might be incomplete and is subject to change.

A Shared Services Provider (SSP) provides a common set of services and service data to a logical grouping of Web applications and their associated sites. This article describes how SSPs work in Microsoft Office SharePoint Server 2007 and includes recommendations on planning for SSPs.

## About SSPs

##### Services provided by an SSP

The following shared services are provided by each SSP:

 Personalization services — provides user profiles based on data imported from directory services, My Sites with personal information that can be shared by all users in the SSP and managed by privacy policies, and content targeting by audience, Office client application, or personalization site links.

 Business Data Catalog — provides a single unified schema for data stored in line-of-business applications.

 Excel Services — provides shared worksheets and a way to analyze business data from data connection libraries by using reports in dashboard pages.

 Office SharePoint Server Search — crawls all sites on Web applications using the SSP to create a single index of all content, data, and metadata.

 Portal usage reporting — enables SSP administrators to view aggregated information about site usage across the entire site hierarchy. SSP administrators can also enable usage reporting for administrators of individual sites and site collections.

##### Consuming services from an SSP

When a server-farm is installed, you create the default SSP as one of the first post-setup tasks. Each Shared Service Provider contains all of the available (installed) shared services.

 You associate Shared Service Providers with specific SharePoint Web applications.

 A SharePoint Web application can only be associated with one Shared Service Provider.

 All site collections and sites within a SharePoint Web application consume services from the same Shared Service Provider.

 Shared services cannot be enabled or disabled at the site collection or site level. All services that are available from the SSP are available to all sites within the Web application.

##### Farm-level SSP configuration

A server farm can host one or more SSPs. Or, a server farm can consume services provided by an SSP on a different server farm.

 Intra-farm shared services — The server farm uses the services of an SSP hosted on the server farm.

 Inter-farm shared services The server farm uses the services of an SSP on a different server farm. A server farms that is consuming services from a different farm might not contain any SSPs. The one limitation to this configuration is that Excel Services is not available outside the farm that hosts this service. If Excel Services is required by a farm, the farm must host shared services locally.

In most single-farm environments, one SSP provides services for an entire organization. Multiple SSPs are only used in deployments that have a proven need for securely isolated content.

##### Geographic SSP configuration

Providing shared services over the WAN is not supported. For example, a regional farm in Africa cannot consume shared services from a central farm in Europe. The Africa farm must host its own SSP. However, users in Africa can connect to a central farm in Europe and consume shared services from the central farm.

While hosting shared services over the WAN is not supported, a central farm can be configured to crawl content across the WAN. For example, a central farm in Europe can crawl the content of a regional farm in Africa. This configuration provides a method of hosting enterprise-wide search. In this scenario, the central farm is not hosting shared services to the regional farm and the regional farm is not consuming shared services from the central farm.

## Determining Shared Services Provider Needs

The biggest design decision around providing shared services is how many SSPs to plan for.

##### Planning for a single SSP

In many cases, a single SSP can provide services for an entire organization:

 A single SSP in a farm provides shared services to Web applications hosted on that farm.

 All users in the SSP can share personal information, search for content, and access business data, according to each of their permissions.

 Access to content can be limited by content targeting, privacy policies, and other features based on SharePoint groups and security.

A single SSP should be used if:

 There is no explicit reason to use multiple SSPs.

 Users will collaborate or share content and data across the organization.

 Users will search organization-wide for people working in the organization.

##### Planning for multiple SSPs

The single-most important criteria that determines if you need more than one SSP is your requirements for isolation of content. For example, if your server farm hosts applications for more than one class of users, separate SSPs can help create the secure isolation between these classes of users. Plan on using a separate SSP for each of the following types of applications:

 Intranet — Intranet content includes team sites, My Sites, and published intranet content. This type of application is typically available only to users within your organization that have an account within your directory management system.

 Partner Web — A partner Web application typically hosts site collections and sites for collaboration between both internal employees and partner users. Using a separate SSP ensures that partner users cannot search on or access sensitive information within your Intranet environment.

 Customer Web site — A customer web site that is available for anonymous users requires a dedicated SSP. The configuration of services within the SSP will be very different than those configured for other types of applications that you use for collaboration within your organization.

Because each additional SSP that you add decreases the overall performance of the server farm, carefully consider your needs for implementing more than one SSP.

The following deployment scenarios might require the use of two or more SSPs:

 Deployments with legal requirements for content isolation, such as financial services organizations, or deployments with one or more confidential projects that require full content isolation.

 Geographically distributed deployments with each location having a discrete set of users and content more easily managed separately in each region.

 Hosted deployments with customers that do not share any content or data.

Before creating multiple SSPs, consider using other means to isolate content:

 Use SharePoint groups to limit permissions and authorization to the correct users and groups.

 Use exclusive search scopes to prevent people from searching for certain content.

 Use audiences to target content to certain groups of users.

 Limit access to sites to certain users or groups. Some content on these sites will appear in search results.

Use multiple SSPs if all of the following criteria are met by your deployment:

 Groups of users work on isolated projects, do not share personal information, do not have a business need to view sites for other projects, and do not collaborate across teams or projects.

 The users have no business need to search for content, data, or metadata in other groups, and might actually have a compelling business reason to not view content or data.

## Sharing content across multiple SSPs

Even with the full content isolation of multiple SSPs, it is possible to override that isolation in rare cases if it is necessary.

 Content on sites using one SSP can be crawled by another SSP by adding the start address to an external content source.

 Trusted My Site host locations can be used to enable users to view personalized information about users in other SSPs.

These practices add additional administration costs while compromising the advantages of multiple SSPs. Typically, they are only done during ongoing operations, such as when a user changes locations in a geographically distributed deployment, or when content is relevant across an organization with groups that are otherwise isolated. Good planning for deployment and careful use of multiple SSPs can reduce the necessity of these practices.

# II Plan site structure and publishing

In this chapter:

 [Chapter overview: Plan Web site structure and publishing (Office SharePoint Server)](#DSDOC_6a4b0ec4_8802_40f9_87ac_6a6691b544)

 Determine user needs and identify feature sets to enable

 Determine the number of users and user types (roles)

 [Determine the information architecture of your site](#DSDOC_7a74c8bf_83a2_4ee1_82e7_c2e9dee789)

 [Determine sites and subsites](#DSDOC_462e12d6_1a5d_4b7c_a0d5_14c551262b)

 [Plan site navigation [Office SharePoint Server]](#DSDOC_89bc3f15_d823_445f_9bea_27d5abf3b4)

 [Determine site variations](#DSDOC_45264de9_6859_45c1_9d6d_70035c471a)

 [Plan for multilingual sites](#DSDOC_22d5dc9c_66bd_40d7_8c60_2a2a066db2)

# Chapter overview: Plan Web site structure and publishing (Office SharePoint Server)

Microsoft Office SharePoint Server 2007 includes features you can use to implement the structure, navigation, and appearance of Web sites and to control how your sites are authored, approved, and published. The articles in this chapter will guide you in planning your Web site's structure, authoring environment, and publishing environment.

The articles in this chapter include:

 [Determine the information architecture of your site](#DSDOC_7a74c8bf_83a2_4ee1_82e7_c2e9dee789) suggests methods for surveying and recording the information requirements of your Web site. This is an important preliminary step in Web site planning.

 [Determine sites and subsites](#DSDOC_462e12d6_1a5d_4b7c_a0d5_14c551262b) introduces Office SharePoint Server 2007 site collections, sites, and subsites, and recommends a method for planning and recording your site's structure.

 [Plan site navigation [Office SharePoint Server]](#DSDOC_89bc3f15_d823_445f_9bea_27d5abf3b4) reviews the Office SharePoint Server 2007 navigation model and provides guidance about planning your site's navigational experience.

 [Plan Web pages](#DSDOC_a8a67b0e_2223_4493_b18d_1a72c529d5) first introduces the elements of Web pages: master pages, content pages, layout pages, style sheets, Web Parts, and server field controls. Next, this article provides guidance about how to plan each element of the Web pages in your publishing site.

 [Plan Web page authoring](#DSDOC_e028f0a7_f9cf_45c1_a8b9_bfb2051352) describes the two methods of authoring Web sites based on Office SharePoint Server 2007 — browser-based authoring and smart-client authoring — and it also describes how to plan and configure your Web site's authoring environment.

 [Determine site variations](#DSDOC_45264de9_6859_45c1_9d6d_70035c471a) describes how to plan and implement a set of Web sites that all derive from a source site, so that content can be tailored to suit different cultures, markets, or geographic regions.

 [Plan content approval and scheduling](#DSDOC_b43e9421_66b8_4cfc_ba06_f772ae7420) describes how to plan your team's method of approving content for publication and how to configure that content's publication schedule.

 [Plan content deployment](#DSDOC_edcdacca_8013_460e_95a0_d2b83b6cc7) describes how to plan the deployment of Web site content from an authoring or staging server environment to a production environment.

 [Plan for collaboration sites](#DSDOC_437a9043_e55b_4b52_b578_dd3fdee340) describes how to plan collaboration sites in your authoring or production environment to be available for teams or groups of users to collaborate on projects or to share information.

 [Plan for multilingual sites](#DSDOC_22d5dc9c_66bd_40d7_8c60_2a2a066db2) describes how to determine the multilingual needs of your Web sites and plan for multilingual site deployment.

# Determine the information architecture of your site

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [What is information architecture?](#DSDOC_section17a74c8bf_83a2_4ee1_82e7_c2)

 [General planning recommendations](#DSDOC_section27a74c8bf_83a2_4ee1_82e7_c2)

 [Using information architecture to plan the structure of your site](#DSDOC_section37a74c8bf_83a2_4ee1_82e7_c2)

 [Using information architecture to plan for people and personalization](#DSDOC_section47a74c8bf_83a2_4ee1_82e7_c2)

 [Using information architecture to plan for business data](#DSDOC_section57a74c8bf_83a2_4ee1_82e7_c2)

 [Using information architecture to plan for search](#DSDOC_section67a74c8bf_83a2_4ee1_82e7_c2)

## What is information architecture?

A Web site's information architecture determines how the information in that site — its Web pages, documents, lists, and data — is organized and presented to the site's users. Information architecture is often recorded as a hierarchical list of site content, search keywords, data types, and other concepts.

Analyzing the information to be presented in an Internet or intranet Web site is an important early step in the site planning process, and this step provides the basis for planning:

 How the site will be structured and divided into a set of subsites.

 How data will be presented in the site.

 How site users will navigate through the site.

 How information will be targeted at specific audiences.

 How search will be configured and optimized.

Although this article provides some guidance on how to analyze the information requirements of your Internet or intranet site, you will want to include an information architect or analyst on your site's planning and design team to ensure that your Web site plans fully take into account the information architecture needs of your organization.

## General planning recommendations

It is useful to divide information analysis for Web site planning into the following stages:

 Survey existing content and Web site structure   Your current Internet or intranet site reflects its current information architecture. Analyze and record how information and content are distributed across your current sites and subsites. Look at logs or other analysis tools to see what content is most and least frequently accessed.

 Survey user requirements   Survey the current and intended site users and record the types of information they create or use. What information do they need in their daily work? Are they able to find that information easily? Does the current Web site structure help them understand the relationships among the different types of information the site contains? Is there missing information? Note any problems the users are having in finding or using information with the site's current architecture.

 Survey business requirements   Survey the managers of the business unit or organization that the Web site is being designed for. What are the business needs of the site? Should the units or divisions of the business be reflected in the information architecture of the site? How will information be shared across business units or isolated within one unit? If the site is targeted at customers, what information should they first encounter? How will they explore information about products or services?

Use your analysis to create a detailed outline of your organization's content needs.

## Using information architecture to plan the structure of your site

Your information architecture analysis will determine the structure of your Internet or intranet site. By dividing the information architecture into business processes, projects, or large content groupings, and by using those divisions to sketch out a hierarchy of subsites and content within each site, you can plan where information belongs within that hierarchy. For more information about planning the structure of Internet and intranet sites based on Microsoft Office SharePoint Server 2007, see [Determine sites and subsites](#DSDOC_462e12d6_1a5d_4b7c_a0d5_14c551262b).

## Using information architecture to plan for people and personalization

Your information architecture should include information about users. This information can come from Microsoft products and technologies, such as Microsoft® Exchange, the Active Directory® directory service, and Microsoft SQL Server™. It can also come from industry standard directories for tracking people, such as Lightweight Directory Access Protocol (LDAP), or from line-of-business applications.

Collecting user information will enable you to create unified and consistent user profiles across the organization. This will in turn help you in planning My Sites, which are special SharePoint® sites personalized for each user.

The people-related concepts recorded with your information architecture will also help you determine how to group site users based on the business processes they participate in, the distribution lists and social networks they belong to, the content they are likely to create or view, or the organizational structure in which they work. For more information about planning for people and personalization, see Plan for personalized content and sites.

## Using information architecture to plan for business data

Your information architecture includes the business data your enterprise uses. By using Office SharePoint Server 2007, business data can be presented in the context of your site structure, so that it is available to those audiences that need it. For example, in an enterprise's intranet portal solution, employee payroll data — which must be available across the enterprise's divisional boundaries — could be presented in the central portal site for the enterprise.

Data that is used by a limited audience could be presented in the subsites or portals used by that particular audience. For example, a customer support team could view and interact with customer support incidents in a portal site used only by that team, and a sales team could view customer data in a portal dedicated to managing customer relationships.

Use your information analysis research to help you determine where the data in your existing business applications should be exposed in your enterprise's portals and Internet sites, so that it is available to site users who need it. For more information about business data planning, see [Determine business data and business intelligence needs](#DSDOC_c1725ade_b558_47d9_9749_6ce68b8df0).

## Using information architecture to plan for search

As you plan your information architecture, keep track of concepts, search terms, and properties that your site's users will use when searching for information on your site. You will want this data when creating the search schema for the site.

Keep in mind that users may search for content by using broad conceptual terms to describe what they need. Your information architecture survey will be useful as a tool to help map users' terminology and concepts to the underlying information they are looking for. For more information about search planning, see Plan search.

## [[1]](#footnote-2)#See Also

[Determine sites and subsites](#DSDOC_462e12d6_1a5d_4b7c_a0d5_14c551262b)

[Determine business data and business intelligence needs](#DSDOC_c1725ade_b558_47d9_9749_6ce68b8df0)

# Determine sites and subsites

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

To determine the sites and subsites of your Internet or intranet site based on Microsoft Office SharePoint Server 2007, use your information architecture research (see [Determine the information architecture of your site](#DSDOC_7a74c8bf_83a2_4ee1_82e7_c2e9dee789)) to help plan one or more Office SharePoint Server 2007 site collections, each consisting of a top-level site and a set of subsites. This article introduces Office SharePoint Server 2007 site collections, sites, and subsites, and it recommends a method for recording your site structure decisions.

Note that we do not provide full guidance about how to map the results of your information architecture research to a particular site structure. However, the concepts and methods described in this article should help your design team members successfully convert their information architecture analysis into a useful solution based on Office SharePoint Server 2007.

In this article:

 [Planning site collections](#DSDOC_section1462e12d6_1a5d_4b7c_a0d5_14)

 [Planning sites and subsites](#DSDOC_section2462e12d6_1a5d_4b7c_a0d5_14)

 [Site templates included in Office SharePoint Server 2007](#DSDOC_section3462e12d6_1a5d_4b7c_a0d5_14)

 [Recording your site structure decisions](#DSDOC_section4462e12d6_1a5d_4b7c_a0d5_14)

## Planning site collections

A site collection is a set of Web sites that has the same owner, shared administration settings, common navigation, and other common features and elements. Each site collection contains a top-level Web site and (usually) one or more subsites.

Grouping your Internet or intranet site's content and features into a site collection provides the following benefits:

 For site designers, a site collection's galleries and libraries (such as the Master Page Gallery or the Site Collection Images library) provide a means for creating a unified, branded user experience across all of the site collection's subsites.

 For site administrators, a site collection provides a unified mechanism and scope for administration. For example, site security, policies, and features can be managed for an entire site collection; site collection usage reports, audit log reports, and other data can help administrators track site security and performance.

 For site authors, a site collection's shared content types, Web Parts, authoring resources, workflows, and other features provide a consistent authoring environment.

 For site users, a site collection's unified navigation, branding, and search tools provide a unified Web site experience.

Below are some examples of solutions that benefit from being implemented as site collections:

 Authoring and collaboration portal site   A site collection to support people in your organization who are working together to produce content useful for your organizational goals. Often, this type of portal site will include collaborative content that is not published but is only used internally, along with content intended for publication to an outside audience.

 Publishing site   A site collection configured to let the content's audience view and interact with the site's content. Publishing sites are often implemented as two site collections — a production site collection that is the published site used by the content's audience and a staging site collection that is a mirror of the production site, used by the authoring team to view site content and test site features. For details on deploying content from a staging to a production site collection, see [Plan content deployment](#DSDOC_edcdacca_8013_460e_95a0_d2b83b6cc7).

 Application portal sites   Portal sites that provide a Web-based view of business applications. Examples include:

 Project Server portal site   A portal site in a large organization devoted to schedules and processes tracked in Microsoft Office Project Server 2007.

 Microsoft Excel Web access portal site   A portal site that makes shared spreadsheets available to site users, and that often includes other business data made available by using the data connection library and the business data catalog.

 Custom business application portal site   A portal site devoted to a business application used in your organization, such as a timecard reporting application.

## Planning sites and subsites

A site collection consists of a top-level site and one or more subsites. Each subsite can be based on any Office SharePoint Server 2007 site template and can have other unique settings, along with unique content. Partition your site collection content into subsites to get finer control of the appearance, content, and features of the various pages in your site collection. The features of subsites that you can configure uniquely include:

 Templates   A subsite can have a unique template. See [Site templates included in Office SharePoint Server 2007](#DSDOC_section3462e12d6_1a5d_4b7c_a0d5_14), below, for details.

 Security   You can define unique groups of users for a subsite. See Plan site and content security for details.

 Navigation   To fine-tune your site's navigation experience, you can configure unique navigation links in each part of your site's hierarchy. Site navigation primarily reflects the relationships among the sites and subsites in a site collection. Therefore, planning navigation and planning sites and subsites are closely related activities. See [Plan site navigation [Office SharePoint Server]](#DSDOC_89bc3f15_d823_445f_9bea_27d5abf3b4) for details.

 Web pages   Each subsite can have a unique Welcome page and other pages. See [Plan Web pages](#DSDOC_a8a67b0e_2223_4493_b18d_1a72c529d5) for details.

 Site layouts   You can make unique layouts or master pages available in a subsite. See [Plan Web pages](#DSDOC_a8a67b0e_2223_4493_b18d_1a72c529d5) for details.

 Search   A subsite can have unique search settings. For example, you can specify that a particular subsite never appears in search results. See Plan search for more information about search planning.

 Content types   A subsite can have unique content types. See [Plan content types [Office SharePoint Server]](#DSDOC_63bb092a_00fe_45ff_a4b8_d8be998d1a) for details.

 Workflows   A subsite can have unique workflows. See Plan workflows for details.

## Site templates included in Office SharePoint Server 2007

Use the information in this section to help you identify which Office SharePoint Server 2007 site template to use for each site in your Office SharePoint Server 2007 solution. Although you can use a Office SharePoint Server 2007 template as it is initially configured, you can also modify any template's default settings by using the Office SharePoint Server 2007 site administration pages. In addition, you can modify a template's design and features by using Microsoft Office SharePoint Designer 2007 or Microsoft Visual Studio®.

The table below lists each template included in Office SharePoint Server 2007 and describes its purpose and general category. The categories are:

 Publishing   Sites for presenting information to an audience. These templates include features that support creating and publishing pages based on page layouts.

 Enterprise   Sites that provide features of use in the enterprise, either because of their scale or because they provide features commonly used in large organizations.

 Meetings   Sites that provide features to support planning and running meetings.

 Collaboration   Sites to support teams collaborating and disseminating information.

|  |  |  |
| --- | --- | --- |
| Template | Purpose | Category |
| Collaboration Portal | A starter site hierarchy for an intranet divisional portal. It includes a home page, a News site, a Site Directory, a Document Center, and a Search Center with Tabs. Typically, this site has an equal number of contributors and readers. Collaboration portals often include subsites based on templates in the Collaboration category. | Publishing |
| Publishing Portal | A starter site hierarchy for an Internet-facing site or a large intranet portal. This site can be customized easily to supply distinctive branding. It includes a home page, a sample press releases subsite, a Search Center, and a login page. Typically, this site has many more readers than contributors.  This site enables content approval workflows by default for a more formal and controlled publishing process. It also restricts the rights of anonymous users to only be able to see content pages, but not to be able to view Office SharePoint Server 2007 application pages. | Publishing |
| Document Center | A site to centrally manage documents in your enterprise. | Enterprise |
| Records Center | A site designed for records management. Records managers can configure the routing table to direct incoming files to specific locations. The site prevents records from being modified after they are added to it. | Enterprise |
| Site Directory | A site for listing and categorizing other sites in your organization. | Enterprise |
| Search Center | A site for delivering the Office SharePoint Server 2007 search experience. The site includes pages for search results and advanced searches. | Enterprise |
| Search Center with Tabs | A site for delivering the search experience. The welcome page includes a search box with two tabs: one for general searches, and another for searches for information about people. You can add and customize tabs to focus on other search scopes or result types. | Enterprise |
| My Site Host | A site used for hosting personal sites. The home page will always redirect to the user's My Site. | Enterprise |
| Basic Meeting Workspace | A site to plan, organize, and capture the results of a meeting. It provides lists for managing the agenda, meeting attendees, and documents. | Meeting |
| Blank Meeting Workspace | A blank meeting site for you to customize based on your requirements. | Meeting |
| Decision Meeting Workspace | A site for meetings that track status or make decisions. It provides lists for creating tasks, storing documents, and recording decisions. | Meeting |
| Social Meeting Workspace | A site to plan social occasions. | Meeting |
| Multipage Meeting Workspace | A site to plan a meeting, and to capture the meeting's decisions and other results. It provides lists for managing the meeting agenda and attendees, along with two blank pages for you to customize based on your requirements. | Meeting |
| Team Site | A site for a team to quickly organize, author, and share information. It provides a document library and lists for managing announcements, calendar items, tasks, and discussions. | Collaboration |
| Blank Site | A blank site for you to customize based on your requirements. | Collaboration |
| Document Workspace | A site for colleagues to work together on a document. It provides a document library for storing the primary document and supporting files, a tasks list for assigning to-do items, and a links list to point to resources related to the document. | Collaboration |
| Wiki Site | A site for a community to brainstorm and share ideas. It provides Web pages that can be quickly edited to record information and then linked together through keywords. | Collaboration |
| Blog Site | A site for a person or team to post ideas, observations, and expertise that site visitors can comment on. | Collaboration |

The following section provides more details about the publishing site templates.

### Comparison of the publishing templates

Most solutions based on Office SharePoint Server 2007 will include one or more site collections based on a publishing template. The table below lists additional information to help you understand and evaluate the two main publishing site templates: Collaboration Portal, for intranet divisional or team portal sites and Publishing Portal, for Internet presence sites or large enterprise portal sites.

|  |  |  |
| --- | --- | --- |
| Element | Collaboration Portal | Publishing Portal |
| Initial structure | A top-level site and four subsites, including a Document Center site, a News site, a Search site, and a Site Directory site. | A top-level site and two subsites, including a Press Releases site and a Search site. |
| Publishing via workflow? | No | Yes |
| Master page | Default.master | BlueBand.master |
| Top-level site default layout page | defaultlayout.aspx | WelcomeSplash.aspx |
| Search visibility? | Yes | Yes |
| Site collection features | Collect Signatures Workflow, Disposition Approval Workflow, Office SharePoint Server Publishing Infrastructure, Office SharePoint Server Standard Site Collection Features, Reporting, Routing Workflows, Translation Management Workflow | Collect Signatures Workflow, Disposition Approval Workflow, Office SharePoint Server Publishing Infrastructure, Routing Workflows, Translation Management Workflow |
| Top-level site features | Office SharePoint Server Publishing, Office SharePoint Server Standard Site Features, Team Collaboration Lists, Translation Management Library | Office SharePoint Server Publishing |
| Anonymous and Restricted Readers rights | Same as Reader. | Anonymous users and Restricted Readers cannot see 2nd application pages, they can only see content pages. |

## Recording your site structure decisions

For each site collection in your solution based on Office SharePoint Server 2007, use a spreadsheet program such as Microsoft Office Excel 2007 to record your site and subsite planning decisions. Enter each site on a separate row of the spreadsheet. If you have multiple site collections in your solution, use a separate worksheet for each site collection.

The map that you create of your sites and subsites will provide essential data to use in your subsequent planning activities, such as planning site navigation, site features, and site security. Here are some recommended columns of information to record for each row in your sites and subsites spreadsheet:

 Parent Site   The site directly above the current site in the site collection's hierarchy. For example, in sites based on the Collaboration Portal, the top-level site is the parent site of the Document Center site.

 Purpose   The purpose of the current site. For example, for a site based on the Document Center site template, "a site to store product specifications and related marketing materials."

 Template   The site template to use when creating the site, such as "Record Center."

 Primary Audience   The group of users the site is primarily intended for, such as "product development group."

 Site Owner   The individual or team responsible for administering the site. For example, for a site based on the Record Center site template, the site owner could be "Corporate Legal Department IT."

As needed, add other columns unique to your solution's goals. Then, as you plan your site structure, record your decisions in your sites and subsites spreadsheet.

## [[2]](#footnote-3)#See Also

[Determine the information architecture of your site](#DSDOC_7a74c8bf_83a2_4ee1_82e7_c2e9dee789)

[Plan site navigation [Office SharePoint Server]](#DSDOC_89bc3f15_d823_445f_9bea_27d5abf3b4)

# Plan site navigation [Office SharePoint Server]

In this article:

 [Review of Office SharePoint Server navigation controls](#DSDOC_section189bc3f15_d823_445f_9bea_27)

 [Planning navigation](#DSDOC_section289bc3f15_d823_445f_9bea_27)

Site navigation provides the primary interface for site users to move about the sites, subsites, and pages that compose your Internet or intranet portal site. Microsoft Office SharePoint Server 2007 includes a set of customizable and extensible navigation features that help orient users of your Internet or intranet portal site and enable them to move among its sites and pages.

Office SharePoint Server 2007 bases its navigation model on the hierarchical structure of the site collection. By using the navigation features, you can link to the following:

 A site's subsites

 A site's peer sites

 Sites higher in the site structure

 Web pages in a site

Additionally, you can create links to arbitrary locations, such as to an external Web site.

Navigation links in Office SharePoint Server 2007 are security-sensitive. If a site user does not have permissions to a site or page that is linked from the site navigation, the user will not see the link. Also, pages and subsites can be configured to be available only to members of an audience. Users who are not members of that audience will not see links to sites and pages targeted at that audience.

As described in [Plan Web pages](#DSDOC_a8a67b0e_2223_4493_b18d_1a72c529d5), pages in sites based on Office SharePoint Server 2007 are composed of three elements: master pages, layout pages, and page content. In planning your portal's navigation, you make decisions about all of these elements:

 You configure global portal navigation elements, and site-level (current) navigation elements on master pages.

 You can add navigation elements that provide tables of contents, dynamic access to content based on a query, or authored links to layout pages.

 You can allow tables of contents, dynamic access to content based on a query, or authored links in page content. Note that letting authors add navigation elements to page content lessens site designers' control of a portal's navigation experience.

 Additionally, you can use breadcrumbs to display a set of links that show the site hierarchy starting from the current page up to the top-level site in the portal.

Office SharePoint Server 2007 navigation is based on the Microsoft ASP.NET 2.0 model which enables you to customize:

 The site map provider.

 The data source (which anchors and filters the structure provided by the site map provider).

 The menus (which control the visual appearance of the navigation elements and how deep a hierarchy to show).

## Review of Office SharePoint Server navigation controls

Navigation controls can be displayed on master pages, layout pages, and—by using Web Part zones—directly in a page's content.

### Navigation controls on master pages

A master page defines the outer frame of the Web page in an Internet or intranet portal site. Master pages contain the elements that you want all pages in your site to share, such as branding information, common commands such as Search, and navigation elements that you want to be available throughout the site. This includes global navigation, which is typically constant throughout the portal, and current navigation, which is typically relative to the site that the user is currently viewing.

Master pages also provide the menu style of the navigation controls. You can configure master page menu style by using Microsoft Office SharePoint Designer or Microsoft Visual Studio.

#### Global navigation

Global navigation, which appears as "top link bars" in default site templates, typically links to the primary sites in a portal site. It is common for the global navigation to appear at the top of each page in a portal site. To give users the flexibility to switch from one primary site to another from anywhere within the portal site, the global navigation usually stays constant in all of the portal's sites and subsites. For example, an Internet portal site that is used to market an enterprise's products could have a subsite for each line of its products. By exposing each product's subsite in the portal site's global navigation, site designers can enable users to easily switch from one subsite to another without having to return to the portal site home page.

By default, all subsites one level below the top-level site of a portal site are added to the global navigation. Site administrators can remove a site from the global navigation by using the Site Navigation Settings page, and they can configure global navigation so that no subsites are displayed (that is, only the home page link is shown). Other global navigation configuration features include:

 Linking to all of the top level site's Web pages.

 Linking to specified external sites.

 Linking to specified sites or pages that are anywhere in the portal site.

 Organizing links under headings.

 Manually sorting the items on the global navigation bar.

In a portal site, a subsite's owners can override the global navigation settings of the top-level site and define different global navigation settings for their subsite and the sites below it. All global navigation features, such as linking to external sites and organizing links below headings, can be defined uniquely in a subsite.

By using Office SharePoint Designer or Microsoft Visual Studio 2005, you can further customize the appearance and functionality of global navigation. For example, you can:

 Customize the cascading style sheets to change the appearance of global navigation.

 Modify the data source, for example to trim the number of sites shown in global navigation.

 Modify the menu style of the navigation. For example, you can select fly-out menus or specify how many levels of the site hierarchy to show in navigation.

#### Current navigation

Current navigation, which is called the Quick Launch in default site templates, typically highlights the important content in the current site and links to related sites. It is common for current navigation to appear on the left of each page in a portal site.

By default, current navigation shows a site's pages and its sibling sites (that is, the sites that share the same parent site). This enables users to explore the content of the current site or move to a site on the same level in the site hierarchy. Portal site administrators can configure current navigation to inherit its navigation items from its parent site. Other current navigation configuration features include:

 Linking to sibling sites.

 Linking to all pages in the current site.

 Linking to specific external sites or to pages in the current site.

 Organizing links under headings.

 Manually sorting the items in the current navigation.

As with global navigation, you can further customize the appearance and functionality of current navigation by using Office SharePoint Designer or Microsoft Visual Studio 2005.

#### Breadcrumb navigation

Breadcrumb navigation displays a dynamically generated set of links at the top of Web pages, to show users their current position in the site hierarchy. Most master pages have a single breadcrumb navigation control. By using Office SharePoint Designer or Microsoft Visual Studio, you can configure the breadcrumb navigation control. For example, you can specify a custom navigation provider, and you can remove breadcrumb navigation from a layout page.

note_ddNote:

The default.master master page, which displays form and view pages, includes two breadcrumb controls, a global breadcrumb which contains sites only, and a content breadcrumb, which contains sites and the current page. Some collaboration site templates, such as the Team Site template, also include two breadcrumbs on all Web pages.

### Navigation controls on layout pages

A layout page defines a layout for a Web page by providing Microsoft ASP.NET controls in which the contents of pages are displayed. To customize layout page, use Microsoft Office SharePoint Designer 2007 or Microsoft Visual Studio. You can add navigation controls to a layout page to support navigation links in Web pages.

When a navigation control is inserted on a layout page, Web pages that use that layout page will display the control along with the page's contents. For example, you can define a layout page that includes a Summary Links navigation control (see below) so that a set of links to relevant pages and sites always appears when a page is displayed.

Office SharePoint Server 2007 includes the following navigation controls that can be added to layout pages:

 Summary Links

 Table of Contents

 Content Query

#### Summary Links

The Summary Links control provides a way to add a set of links to a page. You can control the appearance, organization, and presentation of the links that you add to a Summary Link control.

You can add a Summary Link control to a layout page in three ways:

 You can add it directly to the layout page and configure the links. When you do this, any page that uses the layout page will display the links.

 You can add it as a field control on the layout page. When you do this, you can optionally configure the links, and you can optionally allow authors to modify the links and add new ones.

 You can add it as a Web Part to a Web Part zone. When you do this, authors can modify the links, add news ones, and delete the Summary Link control.

For example, in a portal site in which you publish topics from a technical support knowledge base, you can add a Summary Link field control to the layout pages used for articles, to provide links to related sites containing relevant information, and you can permit authors to add links. This enables authors add links to content that is related to a page's content. For more information about configuring Summary Link controls, see the Office SharePoint Server 2007 online Help.

#### Table of Contents

The Table of Contents control provides a way to add a table of contents of all or part of your portal site to a layout page, so that pages using that layout include the table of contents. It uses the same navigation provider as the global and current navigation in the site's master pages. When you add a Table of Contents control to a layout page, you specify which part of your site collection the control should expose, how the links are presented, and how they are organized.

You can add a Table of Contents control to a layout page in two ways:

 You can add it directly to the layout page and configure it. When you do this, any page that uses the layout page will display the table of contents.

 You can add it as a Web Part to a Web Part zone. When you do this, authors can modify the scope of the Table of Contents control or it.

For example, if you are presenting a set of articles in an online news site, you can add a Table of Content control directly to the article pages' layout so that users can switch from one article to another from any article page. For more information about configuring Table of Contents controls, see the Office SharePoint Server 2007 online Help.

#### Content Query

You can use a Content Query control to link to pages or other items that are displayed based on a query that you design. For example, if you are presenting articles in an online news site, you could add a Content Query control to your site's Welcome Page layout so that new articles are highlighted on that page. You can build complex queries by using the Content Query field control. For example, you can specify which sites in your site collection to query, which lists to use, and what audience to target. You can also filter queries based on lists or libraries metadata.

You can add a Content Query control to a layout page in two ways:

 You can add it directly to the layout page and configure it. When you do this, any page that uses the layout page will display the results of the query.

 You can add it as a Web Part to a Web Part zone. When you do this, authors can modify the query or delete the Content Query control.

For more information about configuring Content Query controls, see the Office SharePoint Server 2007 online Help.

### Navigation Web Parts

A Web Part is a control that authors can insert into a Web Part zone on a page and configure. The Summary Links, Table of Contents, and Content Query controls each have Web Part counterparts that page authors can insert into Web Part zones on pages. The Web Parts have the same configuration features and the same functionality as their related controls, but are configurable when the writer inserts them on the page rather than when the site designer inserts them on the page's layout. To make navigation Web Parts available for page authors to insert on a page, you must include one or more Web Part zones on the page's layout page.

If you allow authors to insert navigation Web Parts onto pages, you reduce the control you have over your portal site's navigation because authors can then control part of the navigation experience of site users. This might be appropriate in a loosely controlled environment such as a collaboration site within an organization, where individual authors need the ability to point users to content related to the author's work. It is less appropriate in a more tightly controlled environment such as an Internet presence site, in which the navigation experience is planned and implemented in a consistent, controlled way by the site's designers and planners.

note_ddNote:

If you want to include Web Part zones on layout pages but prevent authors from inserting navigation Web Parts into these zones, you can change the permissions required to use navigation Web Parts in your site's Web Parts gallery to make those Web Parts unavailable to authors based on their permission level.

## Planning navigation

Navigation planning includes planning the user experience you want to create in your Internet or intranet portal site and deciding whether or not authors will be able to insert navigation elements directly onto their pages.

### Planning the user experience

Your navigation decisions are closely related to your decisions about the structure of sites and subsites in your site hierarchy. For each site in your site hierarchy, you can choose to inherit the global or current navigation from its parent site, or you can plan unique settings. To help record your decisions, use the same spreadsheet that you used to record you site and subsite decisions in the topic [Determine sites and subsites](#DSDOC_462e12d6_1a5d_4b7c_a0d5_14c551262b).

The site structure worksheet should include a row for each site in your site hierarchy. In the worksheet, record the following additional columns of information for each site and subsite:

 Global navigation Record whether the site has unique global navigation settings or inherits its global navigation from its parent. If the site has unique global navigation, specify which subsites and additional sites to display.

 Current navigation Record whether the site has unique current navigation settings or inherits its current navigation from its parent. If the site has unique current navigation, specify whether to display its subsites, its peer sites, or additional sites. Also specify whether to include links to the site's Web pages.

The decisions you make about your portal site's navigation will reflect its unique purpose and structure. When you plan navigation, consider the tradeoff between having too many navigation links, which could make your site confusing, and having too few, which could make it hard for site users to locate critical information. Also, keep the following in mind:

 Inheriting the parent site's navigation can place the current site in a larger context. In an intranet site, this can help information workers use the other sites in the site collection to accomplish their tasks. On the other hand, if users of a site do not have to go to other sites to complete their tasks, consider defining a unique global navigation at the site so that site users are not distracted by irrelevant global navigation links. For example, records managers using a Records Center site might not need to go outside of the Records Center to accomplish their tasks, and so would not benefit from a set of inherited global navigation links.

 Showing peer sites on the current navigation can imply that the peer sites have a similar purpose as the current site. For example, in an Internet site that markets a set of products, this can help site users go to descriptions of related products and services. On the other hand, if users of a site are not likely to want to visit peer sites, consider not displaying them in the current navigation. For example, a university's Internet site with subsites for each graduate school could omit peer links from each site's current navigation because students interested in a particular discipline, such as medicine, are unlikely to want to visit sites related to other disciplines.

### Planning navigation on pages

You can add navigation field controls to layout pages. You can also add Web Part zones to layout pages and allow authors to add navigation Web Parts to these zones. As with other page element planning decisions, you should plan navigation on pages based on how much control you want to have over the page-viewing experience:

 To tightly control site navigation, you can put navigation field controls directly on layout pages and eliminate Web Part zones from page layouts, or restrict the use of navigation Web Parts in those zones. For example, in a corporate Internet presence site with millions of site users, you might decide to restrict authors from inserting navigation controls.

 To allow a more varied, albeit less consistent, site navigation, you can put Web Part zones on layout pages and allow authors to insert navigation Web Parts onto their pages. For example, in an intranet portal site in which authors and site users are part of the same workgroup, you might decide to let authors control the navigation experience of their content by adding navigation Web Parts to their pages.

You should plan navigation on pages as part of your general Web page planning. The topic [Plan Web pages](#DSDOC_a8a67b0e_2223_4493_b18d_1a72c529d5) includes worksheets in which you can record your page navigation decisions for each type of page layout in your portal.

## [[3]](#footnote-4)#See Also

[Plan Web pages](#DSDOC_a8a67b0e_2223_4493_b18d_1a72c529d5)

[Determine sites and subsites](#DSDOC_462e12d6_1a5d_4b7c_a0d5_14c551262b)

# Plan Web pages

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [Elements of Web pages](#DSDOC_section1a8a67b0e_2223_4493_b18d_1a)

 [Planning master pages](#DSDOC_section2a8a67b0e_2223_4493_b18d_1a)

 [Planning content pages](#DSDOC_section3a8a67b0e_2223_4493_b18d_1a)

 [Planning page layouts](#DSDOC_section4a8a67b0e_2223_4493_b18d_1a)

 [Using layout pages to restrict authoring](#DSDOC_section5a8a67b0e_2223_4493_b18d_1a)

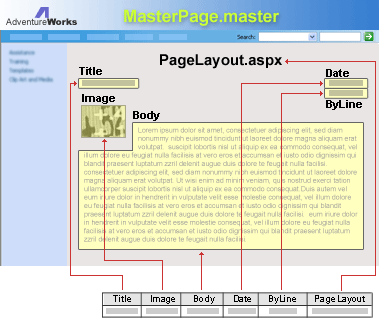
Planning Web pages includes designing the appearance of your published content, determining where writers can add content on pages, and controlling which authoring features writers can use. An effective plan for Web pages helps to ensure that each type of content that your organization will publish is properly designed and available to achieve your publishing goals.

To help you understand your design options, this article first introduces the elements of pages: master pages, content pages, layout pages, style sheets, Web Parts, and server field controls. Next, this article provides guidance on how to plan each element of the Web pages in your publishing site. Because the design and configuration of layout pages helps restrict what authors can do on Web pages, this article includes guidance about using layout pages to restrict authoring.

## Elements of Web pages

When a Microsoft Office SharePoint Server 2007 site user opens a Web page in a SharePoint site, that page is rendered based on a set of elements that have each been planned and designed separately in the Web site. Separating elements of a page in this way allows site planners and designers to treat different elements of the site in unique ways. For example, a site's branding and navigation can be planned and designed separately from the design of the site's content pages, so that the branding can be applied across all site content and can be updated in one place. Similarly, layout of pages can be designed separately from page content, allowing the same content to be displayed in different ways as appropriate.

A Web page based on Office SharePoint Server 2007 is an ASPX page that is dynamically rendered out of its constituent parts. The parts of the page are illustrated below:



The following elements compose a Web page on a SharePoint site:

 Master page   Defines the outer frame of the Web page. A master page contains the elements that you want all pages in your site to share, and it provides a single place to control all of those elements. Typically, a site uses a single site master page, although large Internet sites might use more. For example, a corporate Web site that is used to publicize more than one product could use separate master pages so that the content for each product is properly branded.

note_ddNote:

There are two types of master pages: site master pages and system master pages. The site master page is used on published Web pages in your site. It is the master page that site users and visitors see when viewing published pages. The system master page supplies the layout of pages in the site used by site designers and authors when interacting with the site's user interface and is also used in some team site templates, such as the Wiki Site and the Document Workspace site templates. This article primarily describes planning considerations for site master pages.

Master pages for all sites in a site collection are stored in the Master Page Gallery in the top-level site in the site collection. Because the Master Page Gallery is a SharePoint library, master pages have all the features of documents in Office SharePoint Server 2007, such as versioning, auditing, workflow, check-in and check-out, and content approval.

Typically, master pages include the following elements:

 Branding elements, such as corporate logos and color schemes.

 Shared navigation elements.

 Shared features, such as search commands and Help commands.

 Links to cascading style sheets. (Cascading style sheets control page appearance, colors, and fonts.)

The publishing site templates included in Office SharePoint Server 2007 include site master pages that you can use as a starting point in your page design. To customize an existing master page or create a new one, use Microsoft Office SharePoint Designer 2007 or Microsoft Visual Studio.

 Page content   A single Pages library contains all of a site's content pages. Each item in a Pages library is a single Web page. Because the Pages library is a SharePoint library, the Web pages it contains have all the features of documents in Office SharePoint Server 2007, such as versioning and content approval.

note_ddNote:

Although all pages in a site are in a single Pages library, Web solutions based on Office SharePoint Server 2007, such as intranet portal sites and Internet presence sites, typically consist of a tree of sites, each with its own Pages library.

Authors can create and edit Web pages by using either of the following methods:

 Browser-based editing. Authors create pages using the Create Page command and edit them using the Edit Page command. When creating a page, an author picks a content type and page layout, such as "(Article Page) Article page with image on right." When editing a page, authors use the editing commands available on the page to add content, pick images, and do other editing tasks.

 Converting documents. Authors can convert documents of supported formats into Web pages. Office SharePoint Server 2007 includes converters for documents of .docx and .docm file formats.

See [Plan Web page authoring](#DSDOC_e028f0a7_f9cf_45c1_a8b9_bfb2051352) for more information about planning how Web pages will be authored, including information about configuring document converters.

The columns associated with a Web page's content type contain the page's HTML content. They also contain links to images to display with the page and a link to the page's layout. For example, pages of the default Article Page content type include the following columns:

|  |  |
| --- | --- |
| This column | Contains this content |
| Byline | The author's name |
| Article Date | The date the article is published |
| Page Content | The body of the article |
| Page Image | A graphic to accompany the article |
| Image Caption | A caption for the page image |
| Rollup Image | A graphic to display in search results |
| Page Layout | The page containing the article's layout |

Each column of content for a page is associated with a particular field control in the page's layout pages in which the content for that column is authored and displayed.

 Layout Page   An Active Server Pages (ASPX) page that defines a layout for a type of content page. When a SharePoint site user opens a page in a browser, that page's associated layout page is first combined with the active master page (which supplies the outer frame of the page) and then the contents of the page are poured into the field controls on the layout page.

Because a layout page must display content that is stored in the columns of a content type, it must be designed for a particular content type. For example, a layout page that is associated with the Article Page content type would have several field controls, including:

 A Page Content field control to hold the contents of the Page Content column in the Article Page content type.

 A Page Image field control to hold the image linked to from the Page Image column of the Article Page content type.

Although a layout page must be designed for a single content type, a content type can be associated with multiple layouts. For example, Office SharePoint Server 2007 includes two layout pages for the Article Page content type: one that displays the image on the left side of the page and another that displays the image on the right.

Along with controls to display the contents of a page, a layout page can include other page elements, including:

 Web Parts

 Web Part zones

 Server controls

 Cascading style sheet links to control page appearance, colors, and fonts

For example, a page layout for a business article could include a server control that displays a stock ticker. The stock ticker would be displayed along with a page's contents whenever that layout page is used.

Layout pages for all sites in a site collection are stored in the Master Page Gallery in the top-level site in the site collection. Because the Master Page Gallery is a SharePoint library, layout pages also have all the features of documents in Office SharePoint Server 2007, such as versioning and content approval.

Publishing sites that you create using Office SharePoint Server 2007 include layout pages that you can use as a starting point in your page design. To customize an existing layout page or create a new one, use Microsoft Office SharePoint Designer 2007 or Microsoft Visual Studio.

## Planning master pages

Master pages supply the shared framing elements of the page, including the branding of the site, its navigation features, and other common elements such as search fields and help commands. This article can help you plan your site master pages. It does not provide guidance on designing master pages' appearance or functionality. For information about master page design, see the Office SharePoint Server 2007 Customization Guide. For a full description of the master pages that are included in Office SharePoint Server 2007, see the Office SharePoint Server 2007 Reference Guide.

The site master page supplies the context of the page and should remain consistent as the user interacts with your site. We recommend that you do not change the site master page as a site user navigates from one page to another within a single site in your site collection. To supply consistent branding and user interface, you can use the same site master page across all sites in your site collection.

You might decide to change the master page in subsites in your site hierarchy to change the branding in some subsites. For example, an enterprise's Internet presence site might consist of subsites that each present a different brand of products. You can change the site master page for each subsite to reflect the distinct product brand that each subsite presents.

Before you plan master pages, plan your site structure, as described in Plan site structure and navigation (Office SharePoint Server). By using the site information that you recorded in the topic [Determine sites and subsites](#DSDOC_462e12d6_1a5d_4b7c_a0d5_14c551262b), list the name of each site in your site collection in the Site column of the [Plan master pages](http://go.microsoft.com/fwlink/?LinkId=73318&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73318&clcid=0x409). Then, for each site, fill in the following information in the worksheet:

1. In the Master page column, list the name of the master page to use in the site, such as "BlueBand.Master."

2. In the Custom column, specify the information that applies to your situation.

 If the master page will be customized for the current site, select Yes.

 In the Based on column, type the name of the template that it will be based on, or type None if the master page will be completely custom.

 If the master page will not be custom for the current site, select No.

 If the site will inherit its master page from its parent site, type the name of the parent site in the Inherits from field. (Your documenting site inheritance now will be useful later if you decide to customize the master page elsewhere in your site hierarchy and you want to identify the sites that will be affected by the changes to the master page.)

 If the master page will be applied at the current site, leave the Inherits from field blank.

3. Optionally in the Notes column, list instructions about how to customize the master page or about the tool to use to customize the master page, such as Office SharePoint Designer 2007.

## Planning content pages

Each content page in Office SharePoint Server 2007 consists of text, images, and other content stored as an entry in a Pages library. Planning content pages includes:

 Determining the page content types that meet your content needs.

 For each page content type, determining the columns to use for storing content.

Office SharePoint Server 2007 includes three page content types:

 Welcome Page   Typically, the home page of a publishing site. It includes:

 Columns for images to display.

 A column for page content.

 Columns for links to display with the page.

 Article Page   The primary content page type. This page is designed for general-purpose Web page content. It includes:

 Columns for images and image captions.

 A column for page content.

 Columns for links to display with the page.

 A byline column.

 Redirect Page   A page to redirect the reader to another page.

Additionally, because all three page content types inherit from the generic Page content type, they all include:

 Columns to schedule the page's start and end dates.

 Columns describing contact information for the author.

 An image to display with the page when it is listed in a table of contents or other list.

 Audience targeting information.

When planning content pages, we recommend that you use the page content types that are included in Office SharePoint Server 2007 as a starting point. The Welcome Page and Article Page content types have been designed to be generally useful and to apply across a wide range of contexts. The primary content column in both content types is the Page Content column, which is capable of holding any HTML content. Authors and site designers can control the appearance of their content by using HTML and the cascading style sheets framework. By so doing, they may not need to design other content types." Also, by carefully choosing which layout (see [Planning page layouts](#DSDOC_section4a8a67b0e_2223_4493_b18d_1a)) to use for each type of content based on the Article Page or Welcome Page, you can introduce more variety in your content presentation without requiring the introduction of additional content types.

To modify a page content type, add columns to it that will contain the new HTML, image, or other type of content. (Create columns in the Site Column Gallery to use them on multiple page types.) For example, you may want to add an "About the author" field to certain article pages, to include biographical information about page authors. To do this, add a column, of type "Publishing HTML," to the Site Column Gallery (so that it can be used in other content types), and then add that column to the Article Page content type.

After modifying a page content type, you must modify its associated layout pages by adding field controls to display the additional columns of content. For example, after adding an About the Author column to the Article Page content type, you would add an About the Author field control to associated layout pages to display the contents of that column. Planning layout pages is discussed below, in the section [Planning page layouts](#DSDOC_section4a8a67b0e_2223_4493_b18d_1a).

To plan article pages, use the [Plan article pages](http://go.microsoft.com/fwlink/?LinkId=73316&clcid=0x409)  (http://go.microsoft.com/fwlink/?LinkId=73316&clcid=0x409). The leftmost column in the worksheet contains all the columns in the Article Page content type. Use the other columns in the worksheet to list each type of content that you want to present in your site, such as Article, Press Release, and Job Posting. After you list the types of content across the top of the worksheet, indicate, for each type of content, the columns that you want to use for that type of content, such as "Article date" and "Page content." If you determine that you need a column that is not available, add it in the first column of the Plan article pages worksheet.

It is less likely that you will need more than one welcome page to use across your site, but if you do, use the [Plan](http://go.microsoft.com/fwlink/?LinkId=73320&clcid=0x409)  (http://go.microsoft.com/fwlink/?LinkId=73320&clcid=0x409) to plan which columns to display in each type of welcome page. However, for each subsite in your portal or Internet presence site, you will most likely want to provide a unique welcome page.

## Planning layout pages

A layout page defines a layout for a content page by providing field controls into which the contents of the content page are displayed. Each layout page is associated with a particular content type, and multiple layout pages are often available for a single content type (for example, to provide alternate layouts for localized versions of content or to add or remove the display of certain fields and features from a page layout. You can create or customize a layout page, including adding new controls to display page content along with additional controls such as Web Parts and server controls, using Microsoft Office SharePoint Designer 2007 or Microsoft Visual Studio.

Office SharePoint Server 2007 includes a set of page layouts for the Welcome Page and Article Page content types. The layouts for article pages include:

|  |  |
| --- | --- |
| This page layout ... | Contains these page elements ... |
| Article page with body only | A basic page with a title and page content area. |
| Article page with image on left | A page with a title, page content, a page image on the left, and areas for a byline, article date, and image caption. |
| Article page with image on left | A page with a title, page content, a page image on the right, and areas for a byline, article date, and image caption. |
| Article page with summary links | A page with a title, page content, article date, byline, and a Summary Links Web Part, in which site authors can add a list of hyperlinks. |

For the Welcome Page, the page layouts include:

|  |  |
| --- | --- |
| This page layout ... | Contains these page elements ... |
| Welcome page with summary links | A welcome page with content and image areas, along with two Summary Links Web Parts. |
| Welcome page with table of contents | A welcome page with content and image areas, along with a Table of Contents Web Part to display a hyperlinked table of contents of the site. |
| Welcome splash page | A simple welcome page with just an image and two Summary Links Web Parts in which your authors can add hyperlinks. |

If you are using the page content types and layouts that are included with Office SharePoint Server 2007, there are no additional planning steps needed. Authors will be able to choose page types and associated layouts when they create new pages. However, if you either add new fields to a page content type or if you create entirely custom content types for publishing pages, you should plan layout pages that reflect the new or changed content types.

You can also modify a layout page by adding Microsoft ASP.NET 2.0 controls, such as Web Parts and Web Part zones, to the page. For example, you can add a Content Query Web Part, which displays a set of links returned by a configurable query, to a layout page. Note that if you place a Web Part on a layout page outside of a Web Part zone, you must configure the Web Part, and authors will not be able to change its configuration. For example, if you add a Content Query Web Part directly to a layout page, you would "lock in" the query it uses and authors would not be able to modify it.

To plan layouts for Article Pages, Welcome Pages and other page content types, use the [Plan l](http://go.microsoft.com/fwlink/?LinkId=73317&clcid=0x409) ([Plan l](http://go.microsoft.com/fwlink/?LinkId=73317&clcid=0x409)). Create a separate worksheet for each page content type in your site, such as Article Page. For each page type, list its associated layout pages, provide descriptions of the layouts, and add notes on customizing or creating the layout pages. For example, if you add a second image field to the Article Page content type, you should specify to add a second image-displaying field control to each page layout associated with the Article Page content type.

## Using layout pages to restrict authoring

Depending on your publishing goals, you can restrict how much freedom authors have to format their Web page content or to add items such as images and hyperlinks to pages in your site. For example, in a highly controlled Internet presence site, you may want all formatting to be defined in cascading style sheets associated with your layout pages and you may want to block writers from overriding style definitions by using inline formatting. In contrast, in a collaborative site, such as an intranet portal, you may want to give authors full freedom to format their pages and add other page items, such as Web Parts providing views of data. For example, in an intranet portal used to collaborate on product specifications, you may want to enable writers to freely use styles, hyperlinks, images, and Web Parts to maximize their ability to communicate their ideas.

You can place restrictions on layout pages in the following ways:

 You can set properties on field controls in layout pages that restrict what authors can do.

 You can remove Web Part zones from layout pages to restrict authors from inserting and configuring Web Parts on their pages, or you can set restrictions on Web Part zones to limit how authors can use them.

### Setting restrictions on field controls

By opening your site in Microsoft Office SharePoint Designer 2007 or Microsoft Visual Studio 2005 you can edit the tags associated with field controls to restrict the types of Office SharePoint Server 2007 authoring features writers can use when editing pages in the browser window. For example, in field controls that are bound to columns of type Publishing HTML, features you can allow or restrict include:

 Setting fonts

 Inserting images

 Inserting tables

 Adding hyperlinks

 Adding text markup, such as bold and italics

You can set authoring restrictions on other column types. For example, in field controls that are bound to columns of type Publishing Image, you can allow or restrict hyperlinks from images.

When you restrict an authoring feature on a layout page in Microsoft Office SharePoint Designer 2007 or Microsoft Visual Studio 2005, the related page editing commands in Office SharePoint Server 2007 become unavailable. For example, if you restrict table editing in a field control that contains content of type Publishing HTML, table editing commands, such as Edit Table will be unavailable in the Edit Content toolbar.

For information on using Microsoft Office SharePoint Designer 2007 or Microsoft Visual Studio 2005 to set restrictions on field controls, see the Office SharePoint Server 2007 Customization Guide.

### Allowing or restricting Web Part zones

A Web Part is a server control that authors can insert into Web Part zones on pages. Web Parts display information based on their functionality, such as presenting site navigation links, SharePoint list contents, or database analytical information.

When a layout page includes one or more Web Part zones, the Web Part zones are available on pages using that layout, which enables authors to insert available Web Parts onto their content pages. If you allow authors to insert Web Parts on pages, you reduce your control over users' experience of the site. For example, a writer could insert a Table of Contents Web Part onto a page that exposes parts of your site that your do not want users to navigate to from the current page.

You can restrict authors from adding Web Parts to pages by opening the associated layout pages in Microsoft Office SharePoint Designer 2007 or Microsoft Visual Studio 2005 and removing Web Part zones from them. Similarly, when designing new layout pages, omit Web Part zones to limit authors' ability to add functionality to the pages associated with those layout pages.

You can also include Web Part zones in layout pages but restrict their usage. By setting a Web Part zone's properties, you can populate the Web Part zone with one or more Web Parts and allow authors to edit the properties of those Web Parts but not let them add other Web Parts to the Web Part zone.

For information about using Microsoft Office SharePoint Designer 2007 or Microsoft Visual Studio 2005 to edit Web Part zones on layout pages, see the Office SharePoint Server 2007 Customization Guide.

### Summary

The following table shows layout restriction recommendations for tightly controlled, moderately controlled, and loosely controlled authoring environments:

|  |  |  |
| --- | --- | --- |
| Level of control | Typical site | Restriction recommendations |
| Tight | Internet presence | Strict limitations on editing field controls; other field control limitations, such as no hyperlinks from image field controls; Web Parts are placed directly on the layout page and not in Web Part zones |
| Moderate | Enterprise intranet portal site | Moderate or no limitations on editing field controls; Web Part Zones containing Web Parts, but authors are restricted from adding/removing Web Parts |
| Loose | Divisional or team portal site | No limitations on editing field controls; Web Part Zones allowed |

To record your decisions about authoring restrictions on layout pages, use the [Plan l](http://go.microsoft.com/fwlink/?LinkId=73317&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73317&clcid=0x409). Edit the worksheet for each page content type in your site on which you want to place restrictions. Record your restriction requirements in the Notes field for each layout type.

## [[4]](#footnote-5)#See Also

[Plan Web page authoring](#DSDOC_e028f0a7_f9cf_45c1_a8b9_bfb2051352)

[Plan content approval and scheduling](#DSDOC_b43e9421_66b8_4cfc_ba06_f772ae7420)

# Plan Web page authoring

In this article:

 [Plan browser-based authoring](#DSDOC_section1e028f0a7_f9cf_45c1_a8b9_bf)

 [Plan smart-client authoring](#DSDOC_section2e028f0a7_f9cf_45c1_a8b9_bf)

 [Worksheet](#DSDOC_section3e028f0a7_f9cf_45c1_a8b9_bf)

Web page authoring is the process by which writers add content to a publishing site such as a corporate Internet site or intranet portal site. Web page authoring is available in a site when the Office SharePoint Server publishing features are activated in the site. For information about which site templates include the publishing features, see [Determine sites and subsites](#DSDOC_462e12d6_1a5d_4b7c_a0d5_14c551262b).

note_ddNote:

Before reading this topic, review [Plan Web pages](#DSDOC_a8a67b0e_2223_4493_b18d_1a72c529d5), which describes layout pages, field controls, and other elements of Web pages mentioned in this topic.

Microsoft Office SharePoint Server 2007 supports two methods of Web page authoring:

 Browser-based authoring   Content creators work directly in the Web browser by using Office SharePoint Server 2007 browser-based features such as the Page Editing toolbar and the HTML Editor toolbar.

 Smart-client authoring   Content creators work in an authoring application and use the Office SharePoint Server 2007 document conversions feature to convert from the document's native format to Web page (that is, HTML) format.

Determining whether to use browser-based authoring or smart-client authoring and conversions depends on how your team produces content, along with other factors. The following table describes some of the pros and cons of each method.

|  |  |  |
| --- | --- | --- |
| Authoring method | Pros | Cons |
| Browser-based authoring |  Convenient. Allows editing a Web site in place.   Incorporates Office SharePoint Server 2007 document management features such as versioning, approval, workflows, and check-in and check-out.   Simpler. Does not require the steps of approving content in client applications, then converting the content, then approving the content again as Web pages. |  Can't take advantage of templates available in client authoring applications.   Authors may be more comfortable working in familiar client authoring applications. |
| Smart-client authoring. |  Facilitates publishing an existing body of content.   Useful when the team that authors content is separate from the team that designs and publishes the Web site.   Authors don't need to learn a new user interface.   May be a more appropriate tool for writing lengthy, complex documents.   After a document is converted, all browser-based document management features become available on the converted Web page. |  Converted content must be reviewed and possibly edited in the Pages library, adding a separate step.   Converters for a client application may need to be developed and tested.   Converter programs used by the document conversion feature require server administration and load balancing.   No support for reusable content. |

Before reading about the planning options for browser-based and smart-client authoring, you should review the elements of Web pages in Office SharePoint Server 2007 by reviewing [Plan Web pages](#DSDOC_a8a67b0e_2223_4493_b18d_1a72c529d5).

## Plan browser-based authoring

Planning browser-based authoring includes planning which resources and commands to make available to authors, and planning the editing experience in the field controls in which authors create content.

note_ddNote:

A related set of planning considerations — planning how content will be approved and published — is discussed in [Plan content approval and scheduling](#DSDOC_b43e9421_66b8_4cfc_ba06_f772ae7420).

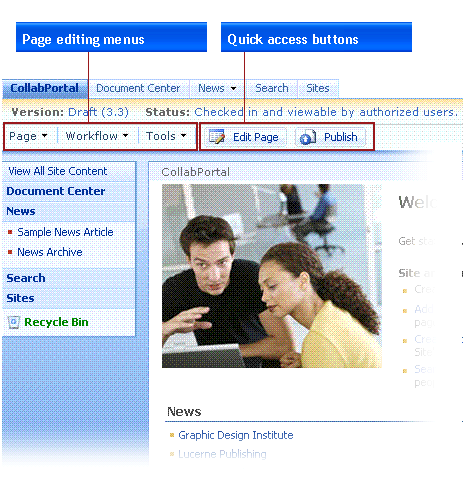
### Plan Page Editing toolbar customizations

The Page Editing toolbar contains UI elements that provide access to page editing commands and related tools, along with workflow commands. This toolbar is available to team members who have at least the Contribute permission level.

The Page Editing toolbar contains two areas that you can customize:

 Page editing menu commands   The set of commands for writing, reviewing, and approving Web pages.

 Quick access buttons   Make frequently used commands available, based on the page's context. For example, the Check In to Share Draft button is only available when a page is checked out.



You can plan and implement page editing menu commands and quick access buttons to provide functionality to your content team. For example, if your organization has an art order process that you want to automate, you could add an Art Order command to the Tools menu on the Page Editing toolbar or implement an Art Order quick access button. Note that you can implement a command as both a menu command and a button.

For more information about implementing commands and buttons in the Page Editing toolbar, see the Office SharePoint Server 2007 [Software Develop](http://go.microsoft.com/fwlink/?LinkId=71218&clcid=0x409).

### Plan HTML Editor toolbar customizations

The HTML Editor toolbar provides the commands used by authors to edit Web page content in a field control:

HTMLEditingToolbar

Note   This image is not available in this preliminary version of the content.

You can customize the HTML Editor toolbar to provide additional editing features to authors or to restrict them from using some features.

 Add buttons to provide new functionality You can add new editing features to Office SharePoint Server 2007 and provide buttons on the HTML Editor toolbar to give authors access to the features. For example, if your publishing portal is used to create highly technical content, you could add an equation editor feature and provide a button for authors to access it.

 Add inline styles You can replace the default styles of page elements by adding references to style sheets in layout pages. When you do this, authors will be able to pick the styles available for the current page element by using the Styles menu on the HTML Editor toolbar.

 Add table formats The HTML Editor comes with a set of predefined table formats that can be customized to fit the styling of an individual page. Each table format consists of a collection of cascading style sheets classes for each table tag. For example, you can customize the appearance of the first and last rows of a table, the odd and even rows, or the first and last column.

 Add custom image pickers In any field that includes an Insert Image command, you can replace the default image picker with a custom one. For example, if you have a very large, searchable repository of images, you can create an interface that lets authors search that repository when they edit Web pages.

 Restrict access to editing features As described in [Plan Web pages](#DSDOC_a8a67b0e_2223_4493_b18d_1a72c529d5), you can restrict how much freedom authors have to format their Web page content or to add items such as images and hyperlinks to pages in your site by restricting access to editing features. By opening your site in Microsoft Office SharePoint Designer 2007 or Microsoft Visual Studio 2005 you can edit the tags that are associated with field controls to restrict the types of Office SharePoint Server 2007 authoring features writers can use when editing pages. For example, you can prevent authors from:

 Setting fonts

 Linking to external addresses

 Adding headings to content

 Making text bold, italic, underlined, or italicized

 Adding tables

For more information about customizing the HTML Editor toolbar, see the Office SharePoint Server 2007 [Software Develop](http://go.microsoft.com/fwlink/?LinkId=71218&clcid=0x409).

### Plan reusable content

The top-level site in a publishing portal or Internet presence portal includes a Reusable Content list that is available in every site in the site collection in which the Office SharePoint Server publishing feature is enabled. Reusable content items can be implemented as HTML or text. By using the Open a new window to insert reusable content button on the HTML Editor toolbar, authors can browse the available reusable content and then insert it.

When you create a reusable content item in the Reusable Content list, you can specify whether or not it can be automatically updated.

 If you specify that an item is automatically updated authors will not be able to change it after they insert it on a page. For example, you can implement a copyright statement or an enterprise's name, address, and other contact information as automatically updatable items. Doing this helps to prevent authors from incorrectly using those items.

When an author inserts an automatically updated item on a page, the URL of the item is inserted instead of the item's contents. When a Web browser loads a page that contains an automatically updated item, the Web browser replaces the URL with the contents of the item. Therefore, changes to automatically updated items in the Reusable Content list do not have to be propagated to pages that use them. They are immediately available the next time a page is opened in a Web browser.

 If you do not specify that an item is automatically updated authors will be able to change it after they insert it on a page. This is useful if you want to define the proper form for a block of content but you want authors to provide the content itself. For example, in a site that provides product descriptions, in which you want each description to follow a particular tabular form, you could create a generic Product Description Table item in the Reusable Content list, which authors could insert and then overwrite.

### Plan dictionary customizations

The Office SharePoint Server 2007 Page Editing toolbar includes a Spelling command that checks the spelling of content in all fields on a page that contain HTML content. The Spelling command indicates spelling errors and provides commands for fixing or ignoring them.

You can add a custom dictionary to your publishing Internet or intranet portal site, to prevent words that are unique to your content from being reported as spelling errors. For example, if your site includes unique product names, you can add them to the custom dictionary.

note_ddNote:

To create a custom dictionary to supplement the dictionaries included in Office SharePoint Server 2007, create a document library named "Spelling" in the top-level site of your portal's site collection. In that library, upload a text file named "Custom Dictionary.txt". Add each properly spelled word to the Custom Dictionary.txt file on a separate line of plain text in the file. Only one Custom Dictionary.txt file is supported for a site collection. Words of any language supported by your site can be added to the Custom Dictionary.txt file.

### Plan additional resources

When you create a publishing site, Office SharePoint Server 2007 creates the libraries listed in the following table that you can use to store additional resources that content creators can use.

|  |  |  |
| --- | --- | --- |
| Use this location | To store these items | That apply to this level in the site hierarchy |
| Master Page Gallery | Master pages and layout pages | Site collection |
| Documents | Documents used in page authoring | Current site |
| Site Collection Documents | Documents used in page authoring | Site collection |
| Images | Images used in page authoring | Current site |
| Site Collection Images | Images used in page authoring | Site collection |
| Style Library | Custom cascading style sheets and Extensible Stylesheet Language (XSL) styles | Site collection |

Note that the default image picker used in Office SharePoint Server 2007 allows users to browse the contents of the Site Collection Images library and the current site's Images library.

## Plan smart-client authoring

Smart-client authoring is the method whereby content creators work in an authoring application and use the Office SharePoint Server 2007 document conversions feature to convert from the document's native format to Web page (that is, HTML) format. Office SharePoint Server 2007 includes converters that create Web pages from Office Word 2007 documents and from Microsoft Office InfoPath 2007 forms. Office SharePoint Server 2007 also includes a generic Extensible Stylesheet Language Transformation (XSLT) converter that enables users to apply an XSL transformation to an XML document. You can develop and install converters for other document formats. (For more information about document conversions, see "Planning document conversions," in [Plan document libraries](#DSDOC_33b67ac7_54c3_42d8_87cd_5d7a00f729).)

note_ddNote:

In smart-client authoring, the document library containing the source documents and the library containing the converted Web pages must be in the same site collection.

You implement smart-client authoring in the following steps:

1. Plan the content type Associate a document template and matching document converter with a content type that is based on the Document content type.

2. Configure the document converter A document converter's configuration must specify:

 The Pages library in which to store the converted content. Because there is a single Pages library in each site in your publishing site hierarchy, this also identifies where in your site hierarchy the content will go.

 The layout page in which the converted content will be displayed. Every Web page must point to a single layout page that defines how the page will be displayed. Pick an appropriate layout page from the Master Page Gallery, which is in the top-level site in the site collection.

 The field on the selected layout page in which the contents of the converted page will be displayed. Layout pages can have one or more Page Content field controls to hold the contents of a Web page. You must indicate a single Page Content field control for displaying the contents of the converted document.

 When the conversions should run. Conversions can run immediately or based on a schedule controlled by the server's administrators. It is recommended that you schedule conversions in a production environment. Contact your server administrators and set this option according to their instructions.

3. Plan cascading style sheets handling The Office SharePoint Server 2007 converters that transform Office Word 2007 documents into Web pages do the following things:

 Extract a set of cascading style sheets style definitions based on the Office Word 2007 paragraph definitions in the source document and, by default, store them in a specified field of the converted Web page.

 Insert class references in the converted Web page to apply the extracted cascading style sheets style definitions.

 Convert inline styles in Office Word 2007 documents, such as font formatting, into inline cascading style sheets styles in converted Web pages

To more tightly control the appearance of Web pages on your site, you can configure the Office SharePoint Server 2007 Word-to-HTML converters to remove the extracted set of cascading style sheets style definitions and not store them with converted Web pages. When you do this, the converter will still insert class references in converted Web pages. To resolve those class references, you can define a set cascading style sheets style definitions and associate them with layout pages or master pages in which the converted Web pages will be displayed. (A set of those styles based on the default Office Word 2007 paragraph styles is defined in the file Rca.css and is associated by default with the layout pages included in Office SharePoint Server 2007.)

note_ddNote:

The Office SharePoint Server 2007 Word-to-HTML converters cannot be configured to remove inline cascading style sheets styles generated for inline formatting in the source document. To prevent inline styles from overriding your cascading style sheets style definitions, prohibit authors from using inline formatting in their source documents.

note_ddNote:

The Office SharePoint Server 2007 Word-to-HTML converters cannot convert inline images into images in the output Web pages, and inline images in source documents will be missing from the converted Web pages. To avoid this, authors should store their images in a picture library in the site collection and insert images into their source documents as hyperlinks to the stored images.

## Worksheet

Use the following worksheet record your Web page authoring decisions for a type of content:

 [Plan Web page](http://go.microsoft.com/fwlink/?LinkId=74540&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=74540&clcid=0x409)

In the worksheet:

1. Record the site URL. This is the site containing the Pages library in which Web pages will be stored.

2. Provide a content description. For example, "product descriptions" or "feature articles."

3. Indicate the authoring team responsible for creating the content.

4. Describe new resources or commands to add. For example, "Add Art Order button to Page Editing toolbar."

5. Indicate if smart-client authoring will be used to author pages in this site.

6. If smart-client authoring will be used, record the source Document library URL, the source document content type, and the document template to use.

7. If smart-client authoring will be used, record the layout page that will contain the converted content and the content field that will display the converted content.

8. If smart-client authoring will be used, indicate whether or not cascading style sheets style definitions should be retained for use with the converted content. If cascading style sheets style definitions will be retained, indicate the field in which to store the extracted cascading style sheets style definitions. If cascading style sheets style definitions will not be retained, indicate where the cascading style sheets styles for the converted page will be defined.

## [[5]](#footnote-6)#See Also

[Plan content approval and scheduling](#DSDOC_b43e9421_66b8_4cfc_ba06_f772ae7420)

[Plan document libraries](#DSDOC_33b67ac7_54c3_42d8_87cd_5d7a00f729)

[Plan Web pages](#DSDOC_a8a67b0e_2223_4493_b18d_1a72c529d5)

# Determine site variations

note_ddNote

 This content is preliminary content. It might be incomplete and is subject to change.

## About site variations

Many organizations have a global reach, but even in domestic markets organizations must reach a diverse customer base that may speak multiple languages, or need to target specific information based on regional differences, mobile devices, or corporate branding. These types of organizations need Web sites that deliver tailored content to suit different cultures, markets, and geographic regions. The job of producing and maintaining variations of a site can be difficult and time consuming. To simplify the process for site architects and site administrators, Microsoft Office SharePoint Server 2007 uses a site variation management system.

Variations in Office SharePoint Server 2007 make the same content available to specific audiences across different sites by copying content from the source variation to each target variation. If necessary, the content can then be customized in the target variation. For example, if a target site is a language variation, the content can be localized in the target site.

You initially define variations of a site by creating variation labels, one for each variation. You select one label as the source label, which is where most of the new content enters the system. The corresponding labels are the target labels. In the simple example shown below, three variation sites, labeled "A," "B," and "C," are one level below the top-level site in a site collection. Variation "A" is the source. Pages authored and published (approved as a new major version) in that site are copied to the destination variations.

<graphic 1>

Only one set of variations can be defined for a site collection. The variations can start anywhere in the site hierarchy. The source label and the target labels are always created as subsites one level below the original site.

If a site has a set of variations, Office SharePoint Server 2007 redirects site users to the appropriate variation. By default, this redirection is based on the language setting of the browser from which the user is visiting the site. For instance, if a user's default browser language is set to use French, Office SharePoint Server 2007 will redirect that user to the French target site (assuming a French variation label exists in the hierarchy). This behavior can be customized by replacing the default redirection page (VariationRoot.aspx) with a different page. This new page, for instance, can implement additional business logic to identify the user’s preferred language, the user's device, or another basis for varying sites. For information on customizing variations redirection, see the article: How to: Customize the Variation Root Landing Logic: http://msdn2.microsoft.com/en-us/library/ms562040.aspx).

When you first create variations from a site, the contents of the original site are copied to the source variation and then propagated to the destination variations. However, subsites of the original site are not automatically copied to the source variation and must be copied using the Manage Content and Structure command to make them available in the destination variations. This is illustrated below:

<graphic2>

1. Content from the original top-level site is copied to the source variation site.

2. The content is automatically propagated to the destination variation sites (a single site in this example).

3. Sub-sites of the original site are manually copied to the source variation site using the Manage Content and Structure command.

4. The sub-sites are then automatically propagated to the destination variation sites.

Once all variations are created and any content has been moved from the original site to the source variation, only changes to the source variation (not to the original site) are propagated to the destination variations. Changes to the original site, or content from other sources, must be copied to the source variation before they can be propagated as variations

<START HERE>.

cover that only published (approved major versions) are auto-propagated based on a timer job and that they arrive as minor versions in the destination.

To ensure seamless synchronization, when a change is made to a page within the source label you can set it so that the updated page is copied either manually or automatically to the other target labels. The change can be as minor as correcting a spelling error or as major as a complete rewrite of the content. This copy appears as a new draft item in the target site; it does not replace the existing content. The content owner for the target label makes the decision to accept the change as-is, translate the change, or ignore the change. The same applies if a user in the source label creates a new site or publishes a new page. Site administrators can choose to ensure the automatic or manual creation of a variation's corresponding site and pages.

Site architects also have the option to make all variations share the same page layouts and master pages, or to specify that each label for a variation use different page layouts and master pages. For more information about planning page layouts and master pages see [Plan Web pages](#DSDOC_a8a67b0e_2223_4493_b18d_1a72c529d5).

## Variations and content deployment

## Variations and navigation

## Variations and devices

## Plan structure of variation hierarchy

To use the variation feature, the site administrator must make four key design decisions:

1. Decide how many variation labels you want and what the purpose of each label is. For example, do you need variations for different languages, regional differences, or mobile devices? Office SharePoint Server 2007 supports up to 50 labels.

2. Decide which variation label you want to make the source label. To ease synchronization, you can set it so that when an author creates content in the source label it is automatically copied to the target label. Note that you cannot automatically copy content from any of the target labels, it must come from the source label.

3. Decide what portion of the site collection you want to include variations in. You can select the entire site or a portion of the site. What you decide depends on the nature of your site and your business objectives. If you want the entire site to participate in variations, you must designate the root of your site collection as the variation root. You then create labels for each of your variants immediately below the root. If only a portion of your site will participate in variations, for example the press release area, you must designate the press release subsite as your variation root and create your labels as children of that subsite.

note_ddNote:

You can only have one variation root in a site collection.

4. Decide whether you want to have content automatically or manually copied to the target variation label. If you enable automatic page creation, when a page is approved in the source variation label its corresponding linked page is automatically created. Target variation content owners can set up an alert on the source page list to be notified when a page has changed. This is useful if you want to disable automatic page creation and manually create pages from your source label in the target labels.

# Plan content approval and scheduling

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [Plan governance](#DSDOC_section1b43e9421_66b8_4cfc_ba06_f7)

 [Plan scheduling](#DSDOC_section2b43e9421_66b8_4cfc_ba06_f7)

 [Governance and scheduling in a content deployment scenario](#DSDOC_section3b43e9421_66b8_4cfc_ba06_f7)

In addition to planning how much control you want users to have over altering the appearance of your Microsoft Office SharePoint Server 2007 Web site, you also need to plan how much governance you want content contributors to have over your site content. Governance refers to the rules and processes that you want to establish for your site. For example, you may want users to impose restrictions and functionality when authors create content. You have the option of giving users no control, simple moderation, or the ability to launch a workflow after they submit content. You can also plan restrictions on where and what type of content an author can place in certain areas of your site.

At this time you also need to understand how the scheduling process works. Users can set a publish and unpublish date by setting the appropriate schedule.

## Plan governance

There are two steps in planning governance. The first step is to determine how and if you want content to go through an approval process. The second step is to determine what content can appear in specific areas of your site.

### Plan content moderation or workflow approval

Content moderation and workflow approval is the method by which site members with Approver permissions control the publication of content. In Microsoft Office SharePoint Server 2007 governance can fall within three moderation and workflow approval categories:

1. None If you choose to implement no moderation or workflow then once an author submits content for publishing it goes live immediately. If a document library is configured to support major and minor versions of content and no content moderation is used, users who have Read permissions will be able to see minor versions of the content.

2. Simple moderation You configure this if you want content manually approved by a member of the Approver group after an author submits it for publishing. Simple moderation is the default in the Corporate Intranet Presence Template Office SharePoint Server 2007. In the Intranet Presence Template, document libraries and image libraries are also configured to use simple moderation.

3. Approval workflow You configure this if you want a workflow to run the approval process. Using a workflow makes the approval process more automated and takes advantage of the built-in workflow features, such as automatically emailing approvers, adding approval tasks to approvers' task lists, and letting authors track the status of the approval process. The pages list in the Internet Presence Template includes a default approval workflow. Users can also develop their own custom approval workflow. See the Office SharePoint Server 2007 object model documentation for more information on creating custom workflows.

### Plan where and how content can appear

Governance also dictates where you want content to appear on your site by introducing restrictions over where certain types of content can appear. You specify this by configuring the site settings for what site templates or page layouts you want authors to use. For example, you may want authors to use a publishing site template, but restrict them from using a Team Site template. Likewise, you can also force users to use the page layout where a graphic always appears on the left-side of the page as opposed to the right-side.

## Plan scheduling

Users have the ability to schedule when they want content to appear, but they can only do this if they create content that uses major or minor versioning. For more information about versioning, see the article Plan Content Control.

The scheduled start times and dates are initiated by a timer service that has a one minute lag time. It runs on a 24-hour clock and it continually checks for pages and items in the document library or image library that is ready for publishing.

## Governance and scheduling in a content deployment scenario

The content deployment feature is designed for sites using a multi-farm topology. For more information about multi-farm topologies see the Office Server 2007 Deployment Guide. A multi-farm topology consists of separate authoring, publishing, and possibly staging farms. If you are implementing a multi-farm topology then you need to apply all the governance considerations outlined in this article for each farm in your environment.

# Plan content deployment

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [What is content deployment?](#DSDOC_section1edcdacca_8013_460e_95a0_d2)

 [About deployment jobs and paths](#DSDOC_section2edcdacca_8013_460e_95a0_d2)

 [Content deployment security](#DSDOC_section3edcdacca_8013_460e_95a0_d2)

 [Configuring content deployment](#DSDOC_section4edcdacca_8013_460e_95a0_d2)

 [Record content deployment plans](#DSDOC_section5edcdacca_8013_460e_95a0_d2)

## What is content deployment?

Content deployment copies content from a source Microsoft Office SharePoint Server 2007 site collection to a destination site collection. The entire source site collection can be copied, or a subset of sites can be copied. In either case, content deployment is incremental by default, deploying only changed pages and related assets (such as images). A Quick Deploy feature supports deployment of a single page by authors.

note_ddNote:

For the content deployment Quick Deploy feature to work, the source and destination site collections must have the Office SharePoint® Server Publishing Infrastructure feature enabled.

In most content deployment scenarios, the source site collection, from which content is being deployed, is in a separate server farm from the destination site collection. Typically, the destination server farm (the "production" farm) will have tightened security to minimize the actions that can be done in the production environment, and it is not expected that authoring will be done in the production environment (changes to the production environment might be overwritten by the content deployment feature). In most content deployment scenarios, the source farm and the production farm are in independent Active Directory® directory service domains. For a full discussion of content deployment topologies, see [Design content deployment topology](#DSDOC_1d6d6040_6cbb_4685_a40e_1e9086d426).

In content deployment, the base URL of the source site collection can be different from the base URL of the destination site collection. The Content Deployment feature will fix links in the source content to work correctly in the destination location.

Content deployment only copies content — Web pages and resources used by the copied pages. It does not deploy programs, assemblies, features, configuration information such as web.config files. When a Web page is deployed, any items in the content database that the page depends on — such as images, style sheets, or layout pages — will also be deployed.

Content deployment deploys the most recent major and minor versions of a content item. For example, if version 2.7 of a Web page is being deployed, the most recent major version (2.0) of the page, along with the most recent minor version (2.7), will be copied to the destination site.

If an item has an associated publishing schedule (see [Plan content approval and scheduling](#DSDOC_b43e9421_66b8_4cfc_ba06_f772ae7420)), the scheduling information is deployed along with the item so that the schedule is followed in the destination site collection. For example, if an item that is scheduled to be published at 6:00 A.M. is deployed at 3:00 A.M., site users on the destination site will not be able to view the content until 6:00 A.M.

## About deployment jobs and paths

In content deployment, a content deployment job copies specified content on a specified schedule by using a specified path.

A content deployment path defines a source site collection from which content deployment can initiate, along with a destination site collection, and it also provides the following:

 Authentication information that gives content deployment jobs permissions to the destination site collection. To deploy content to the destination site collection, deployment jobs must have SharePoint Central Administration credentials on the destination server. Jobs can connect by using the source farm's Central Administration application pool account, Integrated Windows authentication, or basic authentication.

 Information about whether or not to deploy user names associated with the content (such as authors' names).

 Information about how to deploy permissions on the content. See [Content deployment security](#DSDOC_section3edcdacca_8013_460e_95a0_d2) for details.

After a path is defined, one or more content deployment jobs can be defined, which deploy content by using the path. A deployment job specifies:

 The sites within the source site collection to deploy.

 The frequency at which to run the job and deploy the content.

 Whether to deploy all content, or just content that has been changed or added since the last time the job ran.

 Whether to send e-mail when a job succeeds or fails, and the e-mail address or addresses to use.

Each time a path is defined in a site that has the Office SharePoint Server Publishing Infrastructure feature enabled, a Quick Deploy job is created for use on that path. A Quick Deploy job is a deployment job that runs on a specified schedule (every 15 minutes by default) and deploys all Web pages in the site's Pages library that have been marked for deployment since the last time the Quick Deploy job ran. Any member of the Quick Deploy users group (which is created in sites that have the Office SharePoint Server Publishing Infrastructure feature enabled) can mark a Web page for deployment by using the Quick Deploy command.

note_ddNote:

It is possible to have a path defined in sites that do not have the Office SharePoint Server Publishing Infrastructure feature enabled. However, paths created in this way will not have associated Quick Deploy jobs. If you want to add a Quick Deploy job to a path that was defined in a site that does not have the Office SharePoint Server Publishing Infrastructure feature enabled, first enable the Office SharePoint Server Publishing Infrastructure feature on the source site collection, then delete the current path and recreate it. The path will then have a Quick Deploy job associated with it.

## Content deployment security

Permissions to content on the destination server farm will usually be different from permissions to content on the source farm. In many publishing solutions, the destination farm authenticates users by using a different Active Directory domain than the one used in an authoring or staging environment, and there may not be a trust relationship between the two domains.

When configuring a content deployment path, you can choose from the following security options:

 All   Deploys all security-related information with content, including role definitions, access control lists (which map users and roles to the content they have permissions to view or edit), and users. This option is useful if the same set of users has the same permissions on the source and destination farms. For example, when deploying from an authoring farm to a staging farm, this option might be best because the same users need access to both sets of content.

 Role Definitions Only   Deploys role definitions and access control lists that map the roles to the content, but does not deploy users. In this option, the same roles apply in the source and destination server farms, but different users are assigned to those roles in each farm.

 None   Deploys no security information. Security on the destination farm must be managed by the administrators of that farm by assigning users and roles to the farm's sites and content. For example, when deploying from a staging farm to a corporate Internet presence site, this option helps ensure that the security of the two farms is managed separately.

For more information about Office SharePoint Server 2007 roles and security, see [Plan for security roles [Office SharePoint Server]](#DSDOC_81b06f7d_430f_4387_8a29_122cc5928f).

## Configuring content deployment

Configure content deployment between two server farms by using the following steps:

1. On the destination server farm, create an empty site collection based on the Blank Site template to receive the initial deployment job.

2. On the destination farm, on the Content Deployment Settings page in Office SharePoint Server 2007 Central Administration, configure the farm to accept incoming deployment jobs, assign a front-end server as the import server to manage incoming deployment jobs, and specify whether or not to require encryption on the connection between the source and destination farms.

3. On the source farm, on the Content Deployment Settings page, assign a front-end server as the export server to manage outgoing deployment jobs.

4. On the source farm, on the Manage Content Deployment Paths and Jobs page in Office SharePoint Server 2007 Central Administration, create one or more deployment paths.

5. On the source farm, on the Manage Content Deployment Paths and Jobs page, create one or more deployment jobs for each path.

6. Run the initial deployment job to initiate the content on the destination farm.

7. If the path does not deploy all security information, then on the destination farm, create the initial set of users, roles, and permissions on content and sites.

## Record content deployment plans

Use the [Plan content deployment worksheet](http://go.microsoft.com/fwlink/?LinkId=77804&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=77804&clcid=0x409) to record your content deployment plans:

 In the first section of the worksheet, record each server farm in your content deployment topology and note its purpose. For each farm, provide the URLs of the export server, the import server, or both. Also record the Active Directory domain used by the farm.

 In the next section of the worksheet, record each path to create. For each path, supply the source and destination Web applications and site collections. Also record how much security information to deploy along the path: all, roles only, or none.

## Worksheet

[Plan content deployment](http://go.microsoft.com/fwlink/?LinkId=77804&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=77804&clcid=0x409)

## [[6]](#footnote-7)#See Also

[Design content deployment topology](#DSDOC_1d6d6040_6cbb_4685_a40e_1e9086d426)

# Plan for collaboration sites

In this article:

 [About collaboration sites](#DSDOC_section1437a9043_e55b_4b52_b578_dd)

 [Determine number of collaboration sites](#DSDOC_section2437a9043_e55b_4b52_b578_dd)

 [Specific paths](#DSDOC_section3437a9043_e55b_4b52_b578_dd)

 [Additional paths](#DSDOC_section4437a9043_e55b_4b52_b578_dd)

 [Worksheet](#DSDOC_section5437a9043_e55b_4b52_b578_dd)

## About collaboration sites

With Microsoft Office SharePoint Server 2007, you have the ability to support collaboration sites in your environment. These sites do not need to be associated with a particular portal site collection or part of a publishing site collection. They can be stand-alone sites, available for teams or groups of users that need to collaborate on projects or share information, for either a short or a long period of time. For example, a team at an engineering firm might want a collaboration site to discuss current project status, assign tasks, or arrange group lunches, without having this internal information published to the corporate intranet.

Collaboration sites can be made available for searching from your portal or publishing site, so that information from these sites is not lost to your organization. However, for easier data recovery and maintenance, collaboration sites should be hosted either on a separate Web application or in separate content databases in the same Web application as your portal or publishing site.

You can create these sites for your users, or you can allow the users to create these sites on their own. For more information about planning site creation, see [Plan process for creating sites [Office SharePoint Server]](#DSDOC_f7b617fc_cc45_41bf_bb71_f3d49ed4a5).

## Determine number of collaboration sites

Estimate approximately how many collaboration sites to expect in your environment, and how many such sites you are willing to support. If you require users to request a collaboration site, you can control how many are created. If you allow users to create their own collaboration sites, you will have many of these sites in your environment.

## Specific paths

You have the ability to use specific paths in Microsoft Windows SharePoint Services 3.0 to contain your SharePoint site collections, similar to the way that folders contain files or documents in the file system. By default, when you create a Web application, two paths are created for you:

 Root path (/)   This is an explicit inclusion that can contain one site collection. For example, if you want a URL to appear as http://company\_name/default.aspx, you would create the site collection at this root path.

 Sites path (/sites)   This is a wildcard inclusion that can contain many site collections. For example, when you use the /sites path, the URL for a site named Site\_A would be similar to http://server\_name/sites/Site\_A/default.aspx.

note_ddNote:

The name of the /sites path varies depending on the installation language.

## Additional paths

You can also create additional paths, allowing you to group site collections. Then, when you create a site collection, you can choose to:

 Create the site collection at the root of the Web application (if no site collection has already been created there).

 Create the site collection under the /sites path.

 Create the site collection under any additional paths that have been made available for that Web application.

In general, the /sites path should be sufficient for most installations. However, consider using other paths for the following situations:

 You have a complex installation and anticipate having a large number of site collections, and you want to group similar sites together. For example, you could use /personal for individual user sites and /team for group collaboration sites, rather than using /sites for all.

 You want to be able to add a filter to your firewall or router to constrain a specific namespace to internal access only. For example, you could expose the /team path for external collaboration but not /personal.

## Worksheet

Use the following worksheet when you determine paths for sites:

 [Site paths worksheet](http://go.microsoft.com/fwlink/?LinkId=73149&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73149&clcid=0x409)

# Plan for multilingual sites

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [Determine your multilingual needs](#DSDOC_section122d5dc9c_66bd_40d7_8c60_2a)

 [Plan for multilingual site deployment](#DSDOC_section222d5dc9c_66bd_40d7_8c60_2a)

Microsoft Office SharePoint Server 2007 has several features that enable you to support users in different regions or users who speak different languages. You can use these features to create Web sites in different languages, map internationalized domain names (IDNs) to your Web sites, and configure site variation settings that make it easy to track site updates and changes across several duplicate sites.

If your organization needs to support users in different regions or users who speak different languages, you need to do the following as you plan your overall site structure and navigation:

Determine your multilingual needs   This includes identifying all of the languages that you want your Web sites to support, understanding how Office SharePoint Server 2007 multilingual features can help you support users in different regions or users who speak different languages, and identifying the specific Office SharePoint Server 2007 multilingual features you want to use.

Plan for multilingual site deployment   This includes identifying the components that you need to deploy in order to support multilingual sites, such as language packs, operating system language support, and word breakers.

## Determine your multilingual needs

To determine your multilingual needs, you need to:

 Identify the languages that you need to support.

 Identify the internationalized domain names (IDNs) that you need to support.

 Determine whether you want to use the site variations feature.

### Identify language requirements

Usually, you need to create sites in multiple languages if:

 You want to provide Web site content to users in different regions.

 You are required by government regulation or organizational policy to provide Web site content in more than one language.

Be sure to consult all potential site owners as you determine your language requirements, and be sure to list all languages that you might need to support in the future. It's easier to install language support during initial deployment rather than waiting to install language support when your servers are running in a full production environment.

Also, do not assume that you need to create a Web site or a site collection in multiple languages just because your document library contains documents in multiple languages. A document library can contain documents in multiple languages without requiring you to create Web sites or site collections in multiple languages. For example, the document library for an English site collection can contain documents that are written in French and documents that are written in Japanese.

### Determine internationalized domain name mappings

Internationalized domain names (IDNs) are special domain names that can contain non-ASCII characters. Although the Internet's current Domain Name System (DNS) cannot handle host names that contain non-ASCII characters, a special encoding known as Punycode is used to convert the non-ASCII characters into a structured ASCII representation that the Domain Name System can handle. Office SharePoint Server 2007 enables you to use IDNs in your Web site addresses, but to do so you must use the alternate access mappings (AAM) feature to map the IDN to the Punycode representation of the IDN. When you do this, users can access your Web sites by using non-ASCII characters in Uniform Resource Locators (URLs). Assuming you configure alternate access mappings for IDNs correctly, Office SharePoint Server 2007 supports IDN URLs in:

 Address bars that are used to navigate to sites.

 Link fields and rich text boxes.

 Links in 2007 Microsoft Office system clients.

 Links that are created for lists and document libraries.

Office SharePoint Server 2007 does not support IDN URLs for Web pages that provide design functionality or administration functionality. For example, you can't specify an IDN for SharePoint Central Administration. In addition, Office SharePoint Server 2007 does not support IDN URLs for host header–based site collections or URLs that contain anything that System.Uri does not define as a character, such as some bidirectional language characters and complex script characters. System.Uri is a class within Microsoft .NET Framework 2.0.

If you want users to access your Web sites with IDN URLs, you need to configure alternate access mappings that map the internal URL (that is, your Web site's IDN URL) to the public URL (that is, the Internet-facing Punycode URL). To determine the alternate access mappings, do the following:

 Create a two-column table, label the first column Internal (IDN) URL, and label the second column Public (Punycode) URL.

 List each of the IDNs you intend to use in the first column. Be sure to contact every site administrator so you get a complete list of IDNs.

 Determine the Punycode representation for each of your IDNs, and put the result in the second column next to the IDN. Most domain name registrars have free Web-based tools that will convert an IDN to its Punycode representation.

You can use this table to configure alternate access mappings when you deploy Office SharePoint Server 2007.

note_ddNote:

To access a Web site with an IDN URL, users must use a Web browser that supports IDN URLs, such as Windows Internet Explorer 7.0.

### Determine whether you want to use site variations

Variations, a feature of Office SharePoint Server 2007, enable site administrators to make the same information available to specific audiences across different sites by maintaining customizable copies of the content from the source variation in each target variation. A variation consists of a label, which is a set of subsites and pages in a named tree within a site collection. For example, if you want four language variations of your site, you need to create four labels, one for each language. The site administrator selects one label to be the source label, which is where most of the new content enters the system. The corresponding labels are the target labels. For a multi-language site, you may want to use the primary language of your organization as the source label; you can only have one source label.

To ensure seamless synchronization, when a change is made to a page within the source label, you can set it so that the updated page is copied either manually or automatically to the target labels. The change can be as minor as correcting a spelling error or as major as a complete rewrite of the content. The copy appears as a new draft item in the target site; it does not replace the existing content. The content owner for the target label makes the decision to accept the change as is, translate the change, or ignore the change. The same applies if a user in the source label creates a new site or publishes a new page. Site administrators can choose to ensure the automatic or manual creation of a variation's corresponding site and pages.

To learn more about the variation feature, see [Determine site variations](#DSDOC_45264de9_6859_45c1_9d6d_70035c471a).

## Plan for multilingual site deployment

To plan for multilingual site deployment, you need to identify which language features and components need to be installed or configured on your servers. These can include:

 Language packs.

 Supplemental language support.

 Word breaker support.

### Determine your language pack requirements

Based on your language needs, identify the language packs that need to be installed on your front-end Web servers. Language packs enable you to create SharePoint sites and site collections in multiple languages without requiring separate installations of Office SharePoint Server 2007. Language packs are installed on your front-end Web servers and contain language-specific site templates. When you create a site or a site collection based on a language-specific site template, the text that appears on the site or the site collection is displayed in the site template's language. For example, when you choose to create a site in French, the site's toolbars, navigation bars, lists, and column headings appear in French. Likewise, if you choose to create a site in Arabic, the site's toolbars, navigation bars, lists, and column headings appear in Arabic, and the default left-to-right orientation of the site changes to a right-to-left orientation to properly display Arabic text.

The list of available languages that you can use to create a site or site collection is generated by the language packs that are installed on the front-end Web servers. By default, sites and site collections are created in the language in which Office SharePoint Server 2007 was installed. For example, if you install the Spanish version of Office SharePoint Server 2007, the default language for sites, site collections, and Web pages is Spanish. If you need to create sites, site collections, or Web pages in a language other than the default Office SharePoint Server 2007 language, you must install the language pack for that language on your front-end Web servers. For example, if you are running the French version of Office SharePoint Server 2007 and you want to create sites in French, English, and Spanish, then you need to install the English and Spanish language packs on your front-end Web servers.

note_ddNote:

By default, when you create a new Web page within a site, the Web page uses the site's language-country ID to display text.

Language packs for Office SharePoint Server 2007 are not bundled or grouped into multilingual installation packages: you must install a specific language pack for each language you want to support. Also, language packs must be installed on all of your front-end Web servers to ensure that each Web server can render content in the specified language.

The following table lists the language packs that are available for Office SharePoint Server 2007:

|  |  |
| --- | --- |
| Language | Language-Country ID |
| German | 1031 |
| Japanese | 1041 |

note_ddNote:

Additional language packs might be available in the future. Also, if you need to support a language for which there is no language pack, you can still create a Web site or site collection in that language by creating custom Web pages.

Even though you specify a language for a site, some user interface elements such as error messages, notifications, or dialog boxes may not display in the language that you choose. This is because Office SharePoint Server 2007 relies on several supporting technologies — such as Microsoft .NET Framework, Microsoft Windows Workflow Foundation, Microsoft ASP.NET, and Microsoft SQL Server 2005 — and some of these supporting technologies are localized into only a limited number of languages. If a user interface element is generated by one of the supporting technologies, and if the supporting technology is not localized into the language that the site administrator specified for the site, the user interface element will appear in English. For example, if a site administrator creates a site in Hebrew and the Microsoft .NET Framework component displays a notification message, the notification message will not display in Hebrew because Microsoft .NET Framework is not localized into Hebrew. This situation can occur when sites are created in any language except the following: Chinese, French, German, Italian, Japanese, Korean, and Spanish.

In addition, some text might originate from the original installation language, which can create a mixed-language experience. This type of mixed-language experience is typically seen only by content creators or site administrators and is not seen by site users.

For more information about installing language packs, see Deploy Language Packs in Office SharePoint Server 2007 (Beta 2).

### Determine supplemental language support requirements

Based on your language needs, you might have to install supplemental language support on your servers for complex script languages or East Asian languages. The components that support these types of languages are part of the operating system and must be installed before you install any Office SharePoint Server 2007 language features or components.

You need to install supplemental language support for complex script and right-to-left languages if you want to create Web sites in any of the following languages:

 Arabic

 Armenian

 Georgian

 Hebrew

 Indic

 Thai

 Vietnamese

You need to install supplemental language support for East Asian languages if you want to create Web sites in any of the following languages:

 Chinese

 Japanese

 Korean

If necessary, you must install supplemental language support on each of your servers, including your front-end Web servers and your application servers. For more information about installing supplemental language support, see the documentation for your operating system or see Deploy Language Packs in Office SharePoint Server 2007 (Beta 2).

### Determine requirements for word breakers and stemmers

Word breakers and stemmers find word boundaries (word breaking) and conjugate verbs (stemming) in full-text indexed data. The rules for word breaking and stemming differ for different languages, and you can specify different rules for different languages. Word breakers for each language enable the resulting terms to be more accurate for that language. In the case where there is a word breaker for the language family, but not for the specific sub-language, the major language is used. For example, the French word breaker is used to handle text that is French Canadian. If no word breaker is available for a particular language, the neutral word breaker is used. With the neutral word breaker, words are broken at neutral characters such as spaces and punctuation marks.

As a best practice, make sure that you install the appropriate word breaker and stemmer for each of the languages that you need to support. Word breakers and stemmers must be installed on all of the servers that are running the Office SharePoint Server Search service.

The following table lists the languages for which Office SharePoint Server 2007 provides word breakers and stemmers:

|  |  |  |
| --- | --- | --- |
| Language | Language | Language |
| Arabic | Hindi | Portuguese Portugal |
| Bengali | Hungarian | Punjabi |
| Bulgarian | Icelandic | Romanian |
| Catalan | Indonesian | Russian |
| CHS | Italian | Serbian Cyrillic |
| CHT | Japanese | Serbian Latin |
| Croatian | Kannada | Slovak |
| Czech | Korean | Slovenian |
| Danish | Latvian | Spanish |
| Dutch | Lithuanian | Swedish |
| English | Malay | Tamil |
| Finnish | Malayalam | Telugu |
| French | Marathi | Thai |
| German | Neutral | Turkish |
| Greek | Norwegian | Ukrainian |
| Gujarati | Polish | Urdu |
| Hebrew | Portuguese Brazil | Vietnamese |

# White paper: Plan for building multilingual solutions

This white paper provides information and guidelines for using Microsoft Office SharePoint Server 2007 in scenarios where content is managed across different languages. It details most of the functionality provided by Office SharePoint Server 2007 and suggests how to use it to manage multilingual scenarios. It also provides examples for creating custom Web Parts by using Microsoft Visual Studio 2005 and how to configure and manage them by using Microsoft Office SharePoint Designer 2007, the next generation of Web designer tools specifically designed for SharePoint sites. Microsoft Windows SharePoint Services 3.0 features and functionality, and how they add value to the end-user experience, are also described.

[Plan for building multilingual solutions by using SharePoint Products and Technologies](http://go.microsoft.com/fwlink/?LinkId=79322) (http://go.microsoft.com/fwlink/?LinkId=79322).

# III Plan for personalized content and sites

In this chapter:

 [Chapter overview: Plan for personalized content and sites](#DSDOC_50832216_8140_457e_9c4c_8b31eaaef2)

 [Plan for people and user profiles](#DSDOC_267523c2_703f_455e_bbb5_d75f1e2f66)

 [Plan for audiences](#DSDOC_18f26340_695a_40fd_bb4d_1a05f7b5cc)

 [Plan My Sites](#DSDOC_4edf74cf_8808_4277_ba10_b1f925d7c4)

 [Plan for personalized Web Parts](#DSDOC_c976bea3_148c_4be6_96b7_6400c12692)

# Chapter overview: Plan for personalized content and sites

In this article:

 [Plan for people and user profiles](#DSDOC_section150832216_8140_457e_9c4c_8b)

 [Plan for audiences](#DSDOC_section250832216_8140_457e_9c4c_8b)

 [Plan for personalized Web Parts](#DSDOC_section350832216_8140_457e_9c4c_8b)

 [Plan for My Sites](#DSDOC_section450832216_8140_457e_9c4c_8b)

Microsoft Office SharePoint Server 2007 enables users to easily share information about themselves and their work. This sharing of information encourages collaboration, builds and promotes expertise, and targets relevant content to the people who need to see it. You can tailor content to each user in any organization, while enabling administrators to set policies to protect privacy.

These features are built upon a database of properties that integrates data about people from many kinds of business applications and directory services.

Good understanding and planning of personalization features is crucial for creating effective Office SharePoint Server 2007 applications.

## Plan for people and user profiles

Profile Services is the shared service for people and personalization features. Profile Services connects to databases of information about people from various sources, and integrates that information into user profiles that are the basis for powerful personalization features. Planning for people and user profiles includes:

 Planning connections to Profile Services.

 Planning user profiles.

 Planning personalization features.

 Planning policies.

 Planning to find people.

 Using the [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409).

For more information about planning for people and user profiles, see [Plan for people and user profiles](#DSDOC_267523c2_703f_455e_bbb5_d75f1e2f66).

## Plan for audiences

You use audiences to target content to the users who most need to see it, based on properties, organizational relationships, distribution lists, or SharePoint groups. Planning for audiences includes:

 Planning key audiences.

 Planning content targeting to audiences.

 Using the [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409).

For more information about planning for audiences, see [Plan for audiences](#DSDOC_18f26340_695a_40fd_bb4d_1a05f7b5cc).

## Plan for personalized Web Parts

You use personalized Web Parts to provide personalized content to sites and Web pages, starting with My Sites. Different Web Parts target content in different ways. Planning for personalized Web Parts includes:

 Planning for public profile Web Parts.

 Planning for personal site Web Parts.

 Planning for personalization site Web Parts.

 Planning additional Web Parts for My Site.

 Planning for personalized Web Parts on other sites.

For more information about planning for personalized Web Parts, see [Plan for personalized Web Parts](#DSDOC_c976bea3_148c_4be6_96b7_6400c12692).

## Plan for My Sites

My Sites are special SharePoint sites that are personalized for each user. SharePoint sites have three distinct views: a public profile anyone can see, a personal site for each person for document storage and easy collaboration, and a unified experience linking to all personalization sites for that person. Planning for My Sites includes:

 Using My Site templates.

 Activating the My Site feature.

 Planning My Site policies.

 Planning for personalization sites.

For more information about planning for My Sites and the many kinds of personalized sites, see [Plan My Sites](#DSDOC_4edf74cf_8808_4277_ba10_b1f925d7c4).

# Plan for people and user profiles

In this article:

 [About people and user profiles](#DSDOC_section1267523c2_703f_455e_bbb5_d7)

 [Plan connections to Profile Services](#DSDOC_section2267523c2_703f_455e_bbb5_d7)

 [Plan user profile properties](#DSDOC_section3267523c2_703f_455e_bbb5_d7)

 [Plan people and relationships](#DSDOC_section4267523c2_703f_455e_bbb5_d7)

 [Plan policies](#DSDOC_section5267523c2_703f_455e_bbb5_d7)

 [Plan for finding people](#DSDOC_section6267523c2_703f_455e_bbb5_d7)

 [Plan additional personalization functionality](#DSDOC_section7267523c2_703f_455e_bbb5_d7)

 [Worksheets](#DSDOC_section8267523c2_703f_455e_bbb5_d7)

Information about the users in your organization is stored in user profiles within Profile Services. Profiles Services is managed by a services administrator that has additional permissions that are not available to Shared Services Provider (SSP) administrators. Services administrators import information about users from directory services, such as Active Directory directory service and Lightweight Directory Access Protocol (LDAP).

When planning an initial deployment of Microsoft Office SharePoint Server 2007, you must plan connections between directory services and Profile Services, plan the properties of user profiles, plan the policies for displaying and changing user profiles, and plan how user profiles are used by other personalization features, such as personalized sites.

## About people and user profiles

Before you can personalize the sites and content within your organization, you have to understand who the users are in your organization, how they work together, and what information they want to know about each other.

Information about users can come from Microsoft products and technologies, such as Microsoft Exchange, Active Directory, and Microsoft SQL Server. It can come from industry standards for tracking people, such as LDAP. It can also come from line-of-business applications, such as SAP. This enables you to bring all of the properties from these diverse data sources together to create unified and consistent user profiles across the organization.

The properties and data from these sources are stored in user profiles that are managed by Profile Services. User profiles identify connections among users, such as common managers, workgroups, group membership, and sites. In this way, the relationships among users in your organization can be used to encourage more efficient collaboration with colleagues and across teams. This collaboration includes the ability for users to find each other by using user-specific search features.

User profiles and user profile properties can also be used in implementing personalization features, such as building My Sites and content targeting. User profiles are more than just groupings of imported and custom properties about users in your organization. The properties are also used in the public page of My Site to display information about the relationships of each user to other users and content in your organization. This also includes a list of documents shared by each user, and the policies that define how information about users is displayed and shared.

Each user's public profile includes sections that have the following information:

 Properties   Some of these properties are public and appear on the public profile page, but many of these properties are only visible to administrators. SSP administrators are the only users who can see and edit all user profile properties at the SSP level. Site collection administrators can see values of SSP-level properties in the user information list on the site collection, but cannot edit the actual user profiles and properties. They can edit site-level properties that are included in the user information list, but these are not added to user profiles stored in Profile Services.

 Social networking   This includes the sites, distribution lists, and security group memberships for the user, and a separate section listing the user's current colleagues. When viewing someone else's public profile, users can also see the colleagues they have in common with that user.

 Documents   A list of shared documents for the user, including documents on all sites where the user is a member, and organized in tabs by site.

 Policies   This is available to administrators only unless the administrators grant users the ability to override certain policies. This section is used to set how the information in other sections is displayed, and who can see it.

All of these features are presented to encourage collaboration and reinforce connections among users in your organization. A quick review of the public profile tells the viewer who somebody is, what they are working on, and who they work with. It also enables administrators to make decisions about who can see all of this information and how it is shared. Good planning for users and personalization consists of considering the best way to deploy Office SharePoint Server 2007 to effectively present all of this information. This information should include:

 A list of connection sources for user profiles, including Active Directory, LDAP, and business applications, such as SAP or Siebel that track users. Include the location, authentication type, accounts, and any other information needed to connect Profile Services to each source.

 A list of the people features that are available from within user profiles, along with the policy setting, default access policy, and override and replication policies for each feature.

 A list of user profile properties managed by the SSP administrator, along with the same policy information used for features. Add columns for each connection source to record the property mappings that you want to use.

 A list of portal sites and site collections and a note recording who is planning the user information list properties for each site collection.

 If the SSP administrator is planning user properties at the site collection level, record a list of properties and decide if they are best stored in the user profile so they are available for site collections across the SSP, or added later to the user information list for a site collection. The properties in user information lists in a site collection are based on replicated properties of user profiles, but are not connected to user profiles. Properties added to the information list are not stored in the user profile. These properties are not imported, so you do not have to worry about planning property mappings.

|  |
| --- |
| Worksheet action |
| Use the [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) to record this information. |

## Plan connections to Profile Services

Profile Services is used to connect user-based properties of data sources, such as line-of-business applications and directory services (primarily Active Directory and LDAP), with user profiles and properties that enable many of the features of Office SharePoint Server 2007.

Profile Services is available from the SSP administration pages. From the Import Connections link on the User Profiles and Properties administration page, you can connect directly to Active Directory or LDAP to import user profiles from those sources into Office SharePoint Server 2007. Services administrators select the properties from directory services to import to user profiles.

You can also add business data properties that contain information about users to existing user profiles by connecting to the Business Data Catalog, selecting a relevant entity from a registered business data application, and either mapping that entity to an existing profile property or adding it as a new property. These properties augment the existing profiles imported from directory services. You cannot create or import entirely new user profiles from the Business Data Catalog.

You can import the properties from all of these sources into user profiles by connecting to the relevant service or database and mapping the unique identifier for each property in the shared service to the unique identifier of the corresponding property in the business application. These connections can be made regardless of the authentication method used by the business application.

The service maintains the connections with the relevant business applications and updates the properties of user profiles during regularly scheduled imports from all relevant data sources. Data is not exported, however, so the user profile database cannot overwrite the source databases.

Planning for user profiles consists of starting with the default properties of user profiles in Office SharePoint Server 2007, identifying the connections to directory services that you need to supplement those properties with the information about users you already have, and considering additional business data that enables you to connect users to line of business applications. The key planning principle is consistency across data sources for all users in your organization.

|  |
| --- |
| Worksheet action |
| Use the [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) to record your planning decisions. Include a list of connection sources for user profiles, including Active Directory, LDAP, and business applications, such as SAP or Siebel that track users. Include the location, authentication type, accounts, and any other information needed to connect Profile Services to each source. |

Profile Services enables you to collect information about users in your organization across directory services and business applications so that consistent and timely information is always available. Information about users is synchronized across the deployment to all site collections that use the same SSP. This information can also be used by personalization features to increase the value of collaboration and relationships in your organization.

## Plan user profile properties

User profiles and properties are available to administrators from the User Profiles and My Sites section of the Shared Services Administration page. User profiles can be viewed by everyone else from the public profile page of each user's My Site.

Every site that uses the same SSP receives the same basic set of properties from the user profile store and displays them in the site's user information list. SSP administrators can add additional properties to the user information list across all site collections that use the same SSP. Administrators of each site collection cannot add properties to user profiles, but they can add properties to the user information list for certain users, depending on their particular business needs. When you plan for user profiles, you should consider several factors:

 What are your existing and planned directory services? These services will form the foundation for user profiles. Decide which properties you will use for your core user profiles, based on those that are relevant across your organization (or across the SSP in an organization that has multiple sets of shared services). Properties that can be used when finding users, creating audiences to use when targeting content, and establishing relationships between colleagues and workgroups are essential. Start by reviewing the list of properties in directory services, followed by the default properties provided by Office SharePoint Server 2007, and modify that list according to these considerations.

|  |
| --- |
| Worksheet action |
| Use the [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) to record the planned properties. |

 Which line-of-business applications do you use that have information about users? Which properties can be mapped to the properties of directory services?

|  |
| --- |
| Worksheet action |
| Use the [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) to record these mappings, and note which mappings should have priority if there is a conflict. Be sure to add the line-of-business applications to your list of business applications that must be registered in the Business Data Catalog, and integrate them into business intelligence planning. |

 Based on your business intelligence planning, what other, non-user related properties of business applications might be useful for users in your organization? You can use these properties in personalized Web Parts to target business data based on audiences.

|  |
| --- |
| Worksheet action |
| Use the [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) to record this information. |

 How many records of users are you planning to import from all sources, and how often do you want to schedule imports? The frequency of scheduled imports will depend on the number of records, how heavily you are using personalization features, and when you can schedule imports to have the least impact on performance and availability. Let your IT administrators know this information so they can include it in their deployment planning.

 Which site-level user profile properties do you anticipate? In some organizations, this might be dictated centrally. At other organizations, this decision might be left to the discretion of each site collection administrator.

note_ddNote:

The My Site public profile replaces the Microsoft Windows SharePoint Services 3.0 user profile when Office SharePoint Server 2007 is installed. If your initial deployment of Office SharePoint Server 2007 is installed over a Windows SharePoint Services 3.0 installation, be aware that your user profile information will be replaced, and plan accordingly.

### Default user profile properties

 Office SharePoint Server 2007 provides a set of default properties. You will want to review these properties and the policies that apply to them before deciding which changes to make, which properties to keep or remove, and which additional properties to create. For more details about default user profile properties and policies, see [Additional user profile properties](#DSDOC_subsection1267523c2_703f_455e_bbb5) later in this article.

### Additional user profile properties

The default user profile properties and the properties imported from connections to directory services and business applications can be supplemented with additional properties tracking key information that is not available from other sources.

You should plan to add properties at the SSP or site collection level depending on the business needs you identified in earlier planning. Key business needs can often be addressed by creating new properties that associate users with important business processes. For each major concept in your information architecture, consider whether there is a custom property that could be added to user profiles to link users in your organization to information about that concept. These properties can then be used by search to find users, or by personalization features to target content to users. Properties do not have to be visible in public profiles or My Sites, and properties can be useful for search or personalization without being displayed in public profiles or My Sites.

To limit the scope of your planning, prioritize the most important opportunities to improve user profiles. Focus on adding properties that enable key business needs or scenarios for each site collection. If the property relates to a less central business process for the site collection, or if the property seems relevant but does not address specific scenarios, wait until a specific need is identified during regular operations instead of planning to add the property during initial deployment. It is possible you might not need to add many new properties at all, but it is worth considering in case there are any obvious needs.

#### Configure property choice lists

Property choice lists enable Profile Services administrators to suggest acceptable values or limit the values for any property by listing the suggested or approved choices, which then appear to users in a list of values for the property. Property choice lists can either leave the choices up to the user, or define a list of choices that can be added manually or imported from (or exported to) a comma-delimited file. The latter type of property choice list, a defined property choice list, is a powerful way to suggest useful values for a custom property. You can also decide to prevent the inclusion of irrelevant values by limiting the choices to the defined list.

You can also use property choice lists to enable users to select multiple values for the same property. Many kinds of information about users involve more than one value. For example, you can use a property choice list to enable employees to list their professional certifications and other official qualifications, all of which appear as values for the property.

As an example of using a defined list to make information easier to find and promote collaboration, consider an organization that adds a custom property for areas of expertise. The SSP administrator identifies 10 top areas of expertise that are most relevant for users across the site collections that use the SSP. These areas are recorded as values in a defined property choice list for the Area of Expertise property. The same properties are mapped to managed properties by the search administrator, and the site collection administrators for each site collection can then identify Best Bets associated with keywords for each area of expertise. Now when users search for common keywords, experts for each relevant area will appear at the top of search results.

|  |
| --- |
| Worksheet action |
| Use the [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) to record whether the property uses a defined list, the property choice list values, and whether the list is open or closed. This enables you to more easily configure properties during initial deployment. |

For more information about how user profile properties are used by search, see Plan search.

## Plan people and relationships

The relationships among different users who use the sites in your organization are displayed in the public profile page for each user, and also in each user's personal site home page. SSP administrators can also see information about these relationships from the user profiles stored in Profile Services. This relationship information includes:

 Site membership (a global view of all memberships for each user).

 Distribution list membership.

 Security group membership (including by default only e-mail–enabled groups).

 Colleagues (who use both the My Colleagues Web Part and the In Common With Web Part).

When you plan the structure of your site collections, one key part you will plan is the membership for each site. Users are added as members by adding them or a group including them to the Member group for each site. Sites should be provided for all key business processes and divisions, and include the proper users.

Membership in distribution lists and security groups will exist for all but the newest organizations. The planning period for Office SharePoint Server 2007 is a good time to review user and group permissions to ensure that users have the correct permission levels to do their jobs. Planners for personalization features will want to talk to security planners to incorporate any changes into their own planning.

This is also a good time to review distribution lists and reorganize them to reflect information architecture planning. Redundant distribution lists can be discontinued, and new distribution lists can be created to meet additional needs.

Colleagues automatically include all people within each user's immediate workgroup — which includes one's manager, peers, and direct reports—so no specific planning is needed. In organizations that have key relationships that cross workgroups, managers or other users might want to add people to My Colleagues lists for certain workgroups. SSP and site collection administrators should encourage managers to make these changes after initial deployment, or allow managers earlier access to the initial deployment so they can verify the organizational hierarchy and make the changes to directory services.

Planning for users and relationships starts with planning for membership in sites, distribution lists, and SharePoint groups based on security considerations, your organizational hierarchy, and the roles of individuals and teams of users in your organization.

Consider how users currently collaborate, based on common managers or common tasks across workgroups, and then consider ways in which you might improve that collaboration by using new distribution lists or groups, or by adding users as colleagues. Consider other functionality that relies on membership in these groups. For example, membership can be used to target content to specific audiences. You can then decide how much of this information is shared and how it is shared by planning for policies.

|  |
| --- |
| Worksheet action |
| Use the [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) to record all planning decisions. |

## Plan policies

When planning for personalization of your portal sites, you must carefully consider the availability of information about users in your organization. Not all information is appropriate for everyone to see. Some information should only be available to users and administrators to preserve privacy. Other information can and should be shared freely with other users to encourage collaboration. The decision about what information to share is an important one that depends on the particular needs of each organization.

Office SharePoint Server 2007 provides a set of configurable policies so that Profile Services administrators can make the right information available to meet the needs of their organization. Policies might vary between SSPs, so it is a good idea for the planning team to review collaboration needs across the organization to develop a plan for implementing the right mix of policies.

Every personalization feature and property exposed in user profiles and personal sites has a recommended default policy that can be customized based on the needs of each organization. Each policy is made up of two parts:

 Policy setting   Some personalization features provides information that is critical for key business processes in an organization. Other information might be inappropriate for sharing across an organization. Some information will be useful for some users to share, but not other users, so that different policies are needed for different users. The planning team can decide to change the policies by feature or property to meet the business needs of their organization. The specific options are:

 Enabled   The feature is visible to users other than the SSP administrator, depending on the default access setting.

 Required   This property must contain information, and the information is shared based on default access. Forms containing these features or properties cannot be submitted until the required information is provided. For example, the Manager property is often mandatory so that it can be used to provide information for the My Workgroup feature and audiences based on an organization's reporting hierarchy.

 Optional   The property is created and its values might or might not be provided automatically. Each user decides whether or not to provide values for the property or leave the property empty. For example, the telephone number of a user is often left blank, and each user can decide whether or not to provide a telephone number visible to other users. The My Colleagues feature is optional, but rather than being blank the list of colleagues that includes everyone in the current workgroup is visible by default to users who have access. Users can decide to opt out by removing colleagues from the list, or expand the list by adding additional colleagues.

 Disabled   The property or feature is not visible to anyone but the SSP administrator. It does not show up in personalized sites or Web Parts, and cannot be shared.

 User Override   Properties that have the User Override option selected allow users to change the default access policies for user profile properties. With this option selected, each user can decide who can see the values they entered for the property. If this option is not selected, only administrators can change default access settings.

 Replicable   Properties and features that have the Replicable option selected can be replicated to other SharePoint sites, but only if the default access is set to Everyone and the User Override option is not selected.

 Default privacy setting   The privacy setting determines who can see information for a particular personalization feature. Available settings include:

 Everyone   Every user who has viewer permissions to the site can see the relevant information.

 My Colleagues   Every user in this user's My Colleagues list can see the information for this user.

 My Workgroup   Every colleague in the user's workgroup can see the information.

 My Manager   Only the user and the user's immediate manager can see the information.

 Only Me   Only the user and the site administrator can see the information.

### Plan policies for people features

Some organizations will allow individual SSP administrators to configure policies, and other organizations will want to implement a consistent policy across the organization. By setting expectations for policies during initial planning, you can avoid later confusion, surprises, and misunderstandings. Whatever your decision, you should make the policies clear to users in your organization when they begin using Office SharePoint Server 2007, so they can expect that certain information about them and their work will be available to others.

Policies can vary depending on the purpose of the sites in your SSP. Consider your information architecture planning and site hierarchy when deciding which policies to use. For example, a site based around collaboration is likely to have a less restrictive set of policies than a site designed as a document repository.

Also consider who is using your sites. Customer-facing sites will have entirely different policy considerations compared to collaboration sites, and a central portal site for a large organization might have less need to share information than a departmental site. Many of these issues will be handled as part of security planning, but privacy policies and security considerations are sufficiently related that it is a good idea to consider them together.

Policies that have fewer restrictions mean that users will be viewing public profiles more frequently, which affects how often you must update user profiles and compile audiences. In organizations that have a large number of users, this could affect performance and capacity planning.

|  |
| --- |
| Worksheet action |
| Use the [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) to record policy decisions for every feature and property. |

Site and SSP administrators should share policy decisions with IT professionals in the organization. Some issues that could conceivably affect IT planning include:

 The expected frequency of updating user profile information.

 The expected frequency of compiling audiences.

 The effect on performance and capacity of servers running Profile Services.

 The effect on security planning.

For more information about the default policies and available policy settings, see Policies for Profile Services.

### Plan policies for the properties of user profiles

Properties — such as account name, preferred name, work telephone number, department, title, and work e-mail address — are mandatory by default because in most organizations those are key methods of enabling collaboration and developing organizational relationships. Many of them are also used by Office SharePoint Server 2007 in enabling other features, such as colleagues and audiences.

By default, users cannot override these properties because it is important to Profile Services administrators that access to information stay consistent and predictable.

By default, most properties are visible to everyone, but sensitive information, such as non-work telephone numbers, are limited to users who have been selected as colleagues. A couple of other properties are of private interest only.

Different organizations might have different needs. For example, a company that has many employees in the field might find that mobile telephone information is important for everyone to see. Other organizations might keep all non-work telephone numbers completely private. Organizations focused around small-team collaboration might want to limit more properties to a core group of colleagues.

When planning the policy setting for a property, consider the following factors:

 Consider making a property required if:

 The property is used by key user features.

 The property is associated with key business data for applications in the Business Data Catalog.

 The property is used in creating audiences.

 Administrators for Profile Services expect consistent and meaningful values for the property.

 Consider disabling a property if:

 The property will rarely be used.

 The property will distract from more important properties. Note, however, that you can change the display settings for properties to hide them from users viewing public profiles, the Edit Details page, or the My Colleagues Web Part.

 Consider selecting optional if you decide to provide default values for properties, but still want users to be able to remove the information, or if you want to allow each user to provide the relevant value for the property.

When planning default access policy, consider the following factors:

 If you want to use the property in search so that users can be found by searches for the property, set the default access policy to Everyone. Properties that have more restrictive access will not be used by search.

 If the property is useful across workgroups and other divisions in your organization and does not contain sensitive information, consider making it visible to everyone.

 If the property is mostly useful for collaboration within an immediate workgroup or within a particular group of individually selected colleagues, consider making it visible only to colleagues.

 If the property is of a private or sensitive nature, consider making it visible only to the immediate manager, or in some cases, only the individual user. What is considered private information can vary from organization to organization.

When deciding whether to allow users to override the policies for properties, consider the following factors:

 Configure key user profile properties that need consistent values and clear administrator control so that users cannot override them. Override should be enabled only when the access to a property is not central to the needs of an organization.

 Users should be able to override the access policy for a property if the sensitivity of the information can vary between different users, and the administrator cannot predict a single policy for all users. For example, an employee's hire date might be considered private to one employee and a point of pride to another.

 Users should be able to override properties that might be relevant to different groups of users over time, by changing the default access policy.

 For more information about the default policies and available policy settings, see Policies for Profile Services.

### Policy replication

Another factor to consider is what information will be replicated from the SSP to user information lists on SharePoint sites. You can limit replication of information by making policies more restrictive, or by limiting the information that is replicated. Only properties can be replicated. Properties that have the Replicable option selected are replicated to other SharePoint sites, but only if the default access is set to Everyone and the User Override option is not selected.

Every site that uses the SSP will use the replicable properties in user information lists. Properties set to Everyone that are not replicable can be seen in the public profile, but those properties do not appear in user information lists. If a property is not replicated, the values for the property in the user information lists for SharePoint sites remain, but changes are no longer replicated and must be made by the site collection administrator.

|  |
| --- |
| Worksheet action |
| Use the [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) to record which properties you want in the user information lists. |

## Plan for finding people

Office SharePoint Server 2007 enables users to find other users based on their expertise and role in the organization. By default, the following methods of finding people are enabled:

 People search scope   A search scope is provided that limits search results to the public profiles in the user profile store for the SSP. Regardless of the search terms used, only users who match those terms appear in search results.

 People tab in the Search Center site   The People tab in the Search Center site provides options for finding users. You can find users by name or related subject, or by users-related properties, such as title and department.

 Advanced search   Users can be found by advanced searches that search by user profile property values. Every user profile that matches the value of the selected profile appears in search results.

 From values for user profile properties   You can find users without explicitly searching by clicking values for users to find other users who have the same value for the property. These properties can be displayed in user profiles, in user information lists, in SharePoint lists, or in general search results.

 Refined searches   You can refine search results for a people search to include only results for users who have a specific value in their user profiles.

 Group by social distance   By default, all searches for users are grouped by social distance. That is, users who work most closely with the user viewing search results are grouped first, followed by users more distantly.

Regardless of the search method used, the people search results contain links to the public profiles of each user, and links to contact them by e-mail or messaging programs.

When planning for users, you might want to consider supplementing the default people search scope and Search Center tab with customized search scopes and tabs for more specific groups of users.

SSP administrators will want to consult the information architecture and site hierarchy to identify key business concepts that might relate to specific groups of users that might be sought out by users across sites. Then, they can work with the SSP administrator for search to develop search scopes and people search tabs for those specific groups. They can also use their knowledge of the user profiles they manage to identify other useful groups of users and create additional specific search scopes and search tabs for those groups.

Site collection administrators can create site-level search scopes for users who are members of their site collection.

|  |
| --- |
| Worksheet action |
| Use the [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) to record planned search scopes and search tabs. |

People search planning also feeds back into user profile planning. Initial planning might reveal individuals or groups of users that you would like to make easier to find, but the right properties might not exist to allow those users to be found easily.

|  |
| --- |
| Worksheet action |
| Use the [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) to record these new properties to be implemented during deployment. |

## Plan additional personalization functionality

Profile Services is used to provide personalized information to My Sites and other pages by using audiences and targeted Web Parts.

For more information about planning audiences, see [Plan for audiences](#DSDOC_18f26340_695a_40fd_bb4d_1a05f7b5cc).

For more information about My Sites, see [Plan My Sites](#DSDOC_4edf74cf_8808_4277_ba10_b1f925d7c4).

For more information about targeted Web Parts in general, see [Plan for personalized Web Parts](#DSDOC_c976bea3_148c_4be6_96b7_6400c12692).

## Worksheets

Use the following worksheets to plan for people and user profiles:

 [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409)

 [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409)

# Plan for audiences

In this article:

 [About audiences](#DSDOC_section118f26340_695a_40fd_bb4d_1a)

 [Plan key audiences](#DSDOC_section218f26340_695a_40fd_bb4d_1a)

 [Worksheet](#DSDOC_section318f26340_695a_40fd_bb4d_1a)

You use audiences to group the users in your organization so that you can personalize information to ensure that it is as relevant as possible. From the Manage Audiences page for the Audiences Shared Service in Microsoft Office SharePoint Server 2007, you can create and manage up to 10,000 audiences and use them to target content in all of the site collections that use that shared service.

When planning audiences during initial deployment, you want to identify a small set of key audiences based on your evaluation of content needs, your information architecture planning, the structure of your site collections, and the users associated with each site collection.

## About audiences

Before planning audiences, you should understand how audiences are defined. Audiences are defined by Shared Services Provider (SSP) administrators in the Application Management page for the core services of the server farm providing the Audiences Shared Service. There are three types of audiences:

 SharePoint groups   You define SharePoint groups by associating each group with a set of permission levels for each site collection, and then adding members to groups based on their user accounts. Administrators create new SharePoint groups during initial configuration and deployment. Audiences based on SharePoint groups target content to users that are members of the selected groups. SharePoint groups used for audiences can be specific or general, but should be built from sets of users specific to the needs of the business processes and audiences relevant for each site collection.

 Global audiences   Global audiences are audiences based on the properties of user profiles, which are managed by SSP administrators. Global audiences target content to users based on properties in their user profiles.

 Distribution lists and security groups   Distribution lists can be created by different users in an organization, depending on the policies of each organization. Audiences based on distribution lists target content to users who are members of the included distribution lists.

The properties of distribution lists and security groups used for audiences must be imported from Windows security, and mail servers and directory services, such as Microsoft Exchange Server, Active Directory directory service, and Lightweight Directory Access Protocol (LDAP). These properties, including distribution lists, are imported when user profiles are imported. For more information about user profiles, see [Plan for people and user profiles](#DSDOC_267523c2_703f_455e_bbb5_d75f1e2f66).

The properties in user profiles and their underlying sources change frequently. To ensure that audiences remain current, SSP administrators must compile audiences. They schedule compilations regularly to update audiences, and might also compile audiences at other times if necessary. Compilation settings and scheduling for audiences in Office SharePoint Server 2007 use the Microsoft Windows SharePoint Services Extensible Job Service.

## Plan key audiences

Because audiences are built on other administration features, good planning for audiences is a multi-stage process that includes planning for all of these features. The basic steps to plan are:

1. Plan for Windows security.

2. Plan for user profiles.

3. Plan for distribution lists and SharePoint groups.

4. Plan for sites and site collections.

5. Plan for audiences based on groups, distribution lists, and properties in user profiles.

Complete the first four steps before you begin planning for audiences. When you start planning for audiences in an initial deployment, you will record all distribution lists, SharePoint groups, and the central purpose for each site and site collection. Then, you consider how best to group all of that information to create a relatively small number of audiences that reflect the important groups within your organization based on all of these criteria.

We recommend that you consider creating additional SharePoint groups that are planned with audiences in mind. Each site collection will generally have a focused set of business processes associated with specific groups of users, and custom SharePoint groups can be used to define each audience as precisely as possible in combination with existing SharePoint groups, Windows security, user profile properties, and distribution lists. By the end of the audience planning process, you should have a list of audiences that meet the needs of the groups of users who are using each site collection.

|  |  |
| --- | --- |
| Audience rule | Description |
| User profile properties | These include a logical operator that is used to evaluate the property. |
| Reporting structures | These are recorded in the user profile and are visible by default in My Site Web Parts. |
| Memberships | These are in a source group, such as a distribution list or a Windows security group. Memberships are also displayed by default in My Site. |

You can also create audiences directly from distribution lists or SharePoint groups, without including them as audience rules.

You typically will have a natural starting point when you create audiences. For example, your existing working teams, cross-group projects, key business processes, and site structure include groups of users that can be easily translated to audiences by using audience roles based on user profile properties, reporting structure, or membership.

Audience planning can also identify potential improvements in planning for distribution lists, user profile properties, SharePoint groups, and reporting structure. If you want to target some users as a group and there are not existing SharePoint groups, distribution lists, or user profile properties, it is a good idea to plan for adding those groups, lists, or properties.

|  |
| --- |
| Worksheet action |
| Use the [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) to record planned audiences as you identify them. Record all planned content targeted to each audience. Record any underlying distribution lists, groups, and properties of user profiles that must be added before you create audiences. |

### Plan content targeting to audiences

Creating audiences is only half of the story. You make use of audiences to target content, to highlight relevant information for the right users, and to reduce the presentation of irrelevant information to the wrong users.

You target content in the following ways:

 By list item or Web Part.

 By using Trusted My Sites host locations.

 By using the My Site navigation bar to target personalization sites.

 As part of the discovering servers feature.

 By filtering Web Parts by audience.

#### Target by list item or Web Part

Any Web Part can be targeted to a specific set of audiences by adding those audiences to the Target Audiences text box in the Advanced section of the Web Parts tool pane.

Audiences can target content to users in many ways by using different Web Parts. One of the best ways to target content in site collection pages is by using the Content Query Web Part.

The Content Query Web Part is provided by default for certain SharePoint template pages, such as portal site areas and team sites, and can target content in the following ways:

 Group results by options or audience, and is often used to target both by Web Part and by list item.

 Display list items from multiple hierarchical levels, and includes better rendition of audience information.

 Target specific list items to specific audiences by using the Content Query Web Part. Then, even when those list items appear in Web Parts or pages, only the individual list item is targeted and not the entire page or Web Part.

You can also target content in My Sites to audiences by using several different Web Parts. For more information about those Web Parts, see [Plan for personalized Web Parts](#DSDOC_c976bea3_148c_4be6_96b7_6400c12692).

#### Target by using Trusted My Site host locations

In some scenarios, such as a global deployment with geographically distributed shared services, some users can have access to one or more My Site host locations. In these scenarios, SSP administrators for each SSP manage a list of Trusted My Site host locations across all SSPs, and then target each location to the audiences of users who need to view those locations.

Trusted My Site host locations are processed in priority order within the list so that users see the personalized information that is most relevant for the My Site that they are viewing, and personalization information is available even if individual SSPs are unavailable. During the initial deployment, this should be fairly straightforward. In most deployments, there is only one SSP and no need to configure this feature.

|  |
| --- |
| Worksheet action |
| Use the [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) to plan for and record Trusted My Site host locations based on the number of SSPs in your deployment and the need for users to see personalized information across SSPs. |

For more information, see [Plan My Sites](#DSDOC_4edf74cf_8808_4277_ba10_b1f925d7c4).

#### Target by using the My Site navigation bar

My Site links to personalization sites in the My Site navigation bar can be targeted to specific audiences. Links are added to the My Site navigation bar by SSP administrators. In many cases, a personalization site might be relevant for one group in your organization but not everyone. The SSP administrator can target links so that they appear only for users for whom the personalized content in the site is relevant. For more information, see [Plan My Sites](#DSDOC_4edf74cf_8808_4277_ba10_b1f925d7c4).

#### Target links published to Office client applications

Just as personalization sites can appear on the My Site navigation bar based on targeting of the personalization sites on the personalization links list, it is possible to target the links on the Links Published to Office Applications page. This list, available from the User Profiles and My Sites section of the Shared Services Administration page, is used to include links to Office Server sites from Office client applications. Examples of links that show up in client applications include:

 Sites, including team sites, portal sites, and project workspaces.

 Data connection libraries.

 Document libraries or document repositories.

For example, if a personal site directory is added to this list, that location is provided as a choice whenever someone shares a document from an Office client application. This enables users to use the same personal site from multiple client computers. Similarly, data collection libraries added to the list show up in the Microsoft Excel client, and document libraries show up whenever saving documents from any Office client application. By default, links to Office client applications appear for all users in the SSP. Those links become much more powerful when they are targeted to users who most need them, so that users only see the personal sites, data connection libraries, and document libraries relevant to their own work.

When planning the initial deployment of Office SharePoint Server 2007, consider each of these kinds of links. Plan to add links to cover sites, data connection libraries, and document libraries for all the site collections by using the SSP.

|  |
| --- |
| Worksheet action |
| Use the [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) to record each of the links and the relevant audience for each link. |

#### Filter by audience

A group of Web Parts known as filters can be connected to other Web Parts so that they only display results based on certain properties. The exact properties available vary from filter to filter, but one of the available options is to filter by audience. Filters are usually connected to business data Web Parts, so this allows you to target business data based on audience. Unlike simple Web Part personalization, the audience property passed by the filter to the business data Web Part can be used in relatively complex business analysis or calculations when displaying results.

Filters are commonly used in dashboards and report-enabled sites, such as the Report Center site, but they can be used on many kinds of sites, including personalization sites. For more information about filters, see [Plan dashboards and filters](#DSDOC_5fe87ec1_431e_4b7f_ae33_1e2edd8613).

## Worksheet

Use the following worksheet to plan for audiences:

 [People, profiles, and policies worksheet](http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73268&clcid=0x409)

# Plan for personalized Web Parts

In this article:

 [About personalized Web Parts](#DSDOC_section1c976bea3_148c_4be6_96b7_64)

 [Plan for public profile Web Parts](#DSDOC_section2c976bea3_148c_4be6_96b7_64)

 [Plan for personal site Web Parts](#DSDOC_section3c976bea3_148c_4be6_96b7_64)

 [Plan for personalization site Web Parts](#DSDOC_section4c976bea3_148c_4be6_96b7_64)

 [Plan additional Web Parts for My Sites](#DSDOC_section5c976bea3_148c_4be6_96b7_64)

 [Plan for personalized Web Parts on other sites](#DSDOC_section6c976bea3_148c_4be6_96b7_64)

 [Worksheet](#DSDOC_section7c976bea3_148c_4be6_96b7_64)

When planning personalization and site structure across the Shared Services Provider (SSP) and within each site collection, it is helpful to understand how Web Parts are used to personalize sites.

The three templates used by My Sites each have a set of default Web Parts and a gallery of additional Web Parts that can be added to each site. It is also possible to use many of these same personalized Web Parts on other pages. You can also develop custom Web Parts that extend the personalization features that are available in Microsoft Office SharePoint Server 2007.

## About personalized Web Parts

SharePoint sites are composed of Web Parts. Personalized Web Parts are those Web Parts that filter or display information based on the user profile and related properties of the user viewing the site, or a particular user in the organization. The typical template for site collections contains a My Site link that can be used by every user who uses the site collection to view, share, and collaborate by using personalized information.

Web Parts can be added by administrators and site designers, or anyone else who has the correct permissions. When these users select Edit Page on the Site Actions menu, the current page opens in design mode. Designers can add Web Parts by clicking Add a Web Part tool in the zone where they want to add the Web Part, and then selecting a Web Part from the gallery that appears.

Although it is not necessary to plan a personalized Web Part for every site in the organization, it is a good idea to plan for the Web Parts that you want to include in the My Site templates, and for any personalized Web Parts that you want to add to key sites in each site collection, such as the Report Center site.

|  |
| --- |
| Worksheet action |
| Use the [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) to record the personalized Web Parts for each site. If there are settings that need to be detailed for any Web Part, record that information as well, so that it can be used as a reference during initial deployment. |

## Plan for public profile Web Parts

Although many of the administration settings for public profiles are managed by SSP administrators, the Web Parts for public profiles are managed by the administrator of the site collection that hosts My Sites.

### Default Web Parts for public profiles

The default Web Parts for the public profile page template are:

 In the top zone: A Web control that includes the user's name, title, and department.

 In the left zone:

 User Properties Web control   This custom Web control is used only in the public profile. It provides information about each user, including a description if one has been provided. Details based on user-provided profile properties that link to related searches on the People tab of the Search Center site include contact information, availability based on meetings scheduled in Microsoft Outlook, and organization hierarchy.

 Documents Web Part   This Web Part is available only in the public profile, but is similar to the SharePoint Sites Web Part in personal sites. All of the shared documents for the user are grouped in tabs by site, including My Site and every site or subsite in any site collection where that user is a member. Within the My Site tab, there is a link that opens a page of search results that contains every document authored by the user. Within each tab is a list with a link to every document and document location for that particular site, and a link to the site's home page.

 Links Web Part   This Web Part is a list of links shared by the user. Two actions that are visible to site administrators and users viewing their own public profiles are shown in the following table.

|  |  |
| --- | --- |
| Action | Description |
| Add Link | Add a link to the list in this Web Part and the drop-down list on the top menu bar, organized into groups. |
| Manage Links | Edit settings for this link. |

 In the right zone:

 In Common with [user] Web Part   This Web Part is used only in the public profile. It contains the nearest manager, colleagues, and memberships held in common between one user and other users viewing the public profile, based on the visibility policy. If a user is viewing his or her own public profile, it explains what other users see.

 Memberships Web Part   Memberships are displayed to users based on the visibility policy. Memberships include sites, SharePoint groups, audiences, and distribution lists. Administrators and users viewing their own public profile (depending on policy) have a Manage Memberships action in this Web Part.

 Colleagues Web Part   Colleagues are displayed to users based on the visibility policy. Administrators and users viewing their own public profile (depending on policy) have the following actions: Manage Colleagues, Add Colleagues.

All of these Web Parts are customized for My Site. These Web Parts are not available in galleries unless they are exported from galleries available in other pages. A different version of the Colleagues Web Part is available for other pages in galleries as the Colleague Tracker Web Part.

### Additional Web Parts for public profiles

Site collection administrators can add or remove Web Parts from the public profile. The design mode of the public profile page includes Add a Web Part Web Parts in each zone on the page. These parts do not appear in the site, but are used to add other parts to each zone. For more information about adding Web Parts to public profiles, see [Plan additional Web Parts for My Sites](#DSDOC_section5c976bea3_148c_4be6_96b7_64) later in this article.

## Plan for personal site Web Parts

Personal sites are managed by each user, but site collection administrators can make changes to the personal site template to add or remove Web Parts and promote different personalization, business intelligence, and collaboration features of Office SharePoint Server 2007.

### Default Web Parts for personal sites

The default Web Parts for the personal site template are:

 In the top zone: A Web Part that includes the user's name, title, and department.

 In the left zone:

 Getting Started with My Site Web Part   This part, based on the Content Editor Web Part, contains links to important tasks to get users started using My Site, and can be removed by the user when it is no longer needed. Actions linked here include editing the public profile and adding colleagues.

 SharePoint Sites Web Part   This Web Part is only available in the personal site, but is similar to the Documents Web Part in public profiles. All of the documents and tasks for the user are grouped in tabs by site, including My Site and every site or subsite in any site collection where that user is a member. Within the My Site tab is a link that opens a page of search results containing every document authored by the user. Within each tab is a list with a link to every document and task, its location, as well as a link to the site's home page.

 In the right zone:

 My Calendar Web Part   This contains tasks and meetings for the user.

 Colleagues Web Part   Colleagues are displayed, along with the following actions: Show all colleagues, Modify alert settings.

 Memberships Web Part   Memberships are displayed, along with a Manage Memberships action.

All of these Web Parts except the My Calendar Web Parts are customized for My Site, and do not appear in any Web Part galleries. The Memberships Web Part is only available for other sites if it is exported. A version of the Colleagues Web Part is available for other pages in galleries as the Colleague Tracker Web Part, and a different version of the SharePoint Sites Web Part is also available. The My Calendar Web Part is also available in galleries for other sites.

### Additional Web Parts for personal sites

Each user can add or remove Web Parts from the home page of the personal site. The personal sites Web Part galleries include all of the Web Parts available in the gallery for public profiles except for the Document Library Web Part, and several additional Web Parts for personalizing e-mail, lists, and business data presentation. For more information about adding Web Parts to the personal site, see [Plan additional Web Parts for My Sites](#DSDOC_section5c976bea3_148c_4be6_96b7_64) later in this article.

## Plan for personalization site Web Parts

A personalization site is a site created by using a template that filters and targets the information displayed on the page based on the identity of the current user viewing the site. Personalization sites can use many of the Web Parts provided in Office SharePoint Server 2007, along with any other Web Parts you might create or import from galleries of Web Parts created by others. Some Web Parts are used more often, or provide functionality that is specific to the personalization experience.

### Default Web Parts for personalization sites

The default Web Parts for the personalization site template are:

 In the top zone:

 Current User Filter Web Part   This Web Part enables the author to pass the current user's login name to connected Web Parts.

 Profile Property Filter Web Part   This Web Part enables the author to pass the current user's preferred name to connected Web Parts.

Both Web Parts are provided by default and are visible to personalization site authors.

No other Web Parts are provided by default. Each personalization page uses different Web Parts that are connected to the existing filters so that the information on the page is personalized.

### Additional Web Parts for personalization sites

The owner and administrator of each personalization site can add Web Parts to the page. Personalization sites can use all of the Web Parts available in the gallery for personal sites except for the Shared Documents, Shared Pictures, and My Pictures Web Parts.

Personalization pages are built upon the Current User Filter Web Part and the Profile Property Filter Web Part. The main Web Parts added to personalization sites will be parts that are connected to the filters so that whatever content they display is filtered based on either the user name or the preferred name of the current user.

Connected Web Parts are often business data Web Parts, key performance indicator (KPI) Web Parts, and lists and libraries Web Parts. The decision about which parts to include depends on the business needs of your organization, the purpose of the site collection containing the personalization site, and the information most needed by the members of the personalization site.

Personalization sites for initial deployment will be more effective if they are focused narrowly towards a single purpose. When you plan for each site collection, some will contain personalization sites. Each personalization site should be focused around a shared set of business processes and information that reflects a central purpose of the site collection.

For example, a human resources site that exists to provide information about employee benefits, time reporting, and company policies will have a personalization site that provides Web Parts that personalize that information. A call center personalization site might present Web Parts linked to the customer service database, personalized so that users can see their own open issues, customer service statistics, and so on. A site collection used for authoring Web site content might contain lists and libraries of content for each of a writer's current projects, along with core personalization parts, such as e-mail and calendar Web Parts.

You can categorize personalized content in the following three ways, and most personalization sites will focus on one type.

 Content personalization   Content is managed by users on another team and published to a site that has a personalized view for each member.

 Data personalization   There is an underlying business application associated with a key business process, allowing each user to see a personalized view of the data at any time.

 Personalized views of group project content   Users within the same group or team work together to produce content, and they have a common personalization site to display the work and relevant content for each user.

For complex site collections, personalization might include all of these categories, but it is a good idea to start with a simplified set of personalization sites and extend the sites over time as needs evolve.

Beyond the initial filter Web Parts on personalization pages, you might want to add additional filter Web Parts to further filter data and content on personalization sites. For more information about these filters, see [Plan additional Web Parts for My Sites](#DSDOC_section5c976bea3_148c_4be6_96b7_64) later in this article. The same parts are available as are available in public profiles and dashboard sites.

The administrator of each site collection that has a personalization site should make a note of the content they want to personalize for that site based on the purpose of the site collection, and then identify the Web Parts and filters they will need to deploy each site.

## Plan additional Web Parts for My Sites

The additional Web Parts available to add to the pages and templates for My Sites fall into several groups:

 Suggested Web Parts

 List and libraries Web Parts

 Business data Web Parts

 KPI Web Parts

 Filter Web Parts

Each of these groups of Web Parts raises different questions during public profile planning.

Because personal sites are designed and administered by each user, there are not as many considerations for planning them as there are for personalization sites and public profiles. However, there are some factors you should consider to plan for added functionality in personal sites according to the needs of your organization.

### Plan for suggested Web Parts on My Sites

Some Web Parts are specifically suggested for specific zones in the personal site and personalization sites when users add Web Parts to a page in design mode. Personalization is built into most of these Web Parts, which are intended to be used in pages to provide personalized information that users need to accomplish their tasks. They involve e-mail, workspaces, and commonly used lists, libraries, and pages. Other Web Parts can be personalized by using filters or audiences, but suggested Web Parts are inherently personalized.

Note that the public profile does not include any of these suggested Web Parts, because it is not intended to be a place where users learn information about themselves and their work, but a place for other people to learn information about them.

The suggested Web Parts for personal sites are:

 Colleague Tracker Web Part (This is the same as the default Colleagues Web Part.)

 Content Editor Web Part (For example, the Getting Started with My Site Web Part.)

 Page Viewer Web Part

 Image Web Part

 My Pictures Web Part

 My Links Web Part

 My Workspace Sites Web Part

 Outlook Web Access Web Parts, including:

 My Calendar (This is one of the default Web Parts for personal sites.)

 My Inbox

 My Mail Folder

 My Tasks

The suggested Web Parts for personalization sites include all of these Web Parts except the Content Editor Web Part, the Page Viewer Web Part, the Image Web Part, and the My Pictures Web Part. Each of these Web Parts (except for My Pictures) is available in the gallery but not suggested.

To encourage the use of Outlook Web Access Web Parts in personal sites, you can add more of those parts or add mail server information before deployment so the parts will be fully functional from the start without any additional steps required for each user. These Web Parts can also be useful in personalization sites based around collaboration or business data. The distinction is that in personal sites, these parts are central to its purpose as the personalized page for each user, while personalization sites use these parts in a more secondary role to supplement other parts.

You can add the Content Editor Web Part to the personal site template to provide text and links that suggest ways for users to develop their personal sites by adding new Web Parts or by using the existing Web Parts. This is already done by default in the Getting Started Web Part, but you can customize this and even add Content Editor Web Parts focused on different ways to improve personal sites. You can link to personalization sites, business-critical lists, and other resources that can be used in personal sites that users might otherwise not find as easily. If information is particularly critical, you can use the Page Viewer Web Part to display the page within a Web Part of each personal site.

Personalization sites are less likely to use Content Editor Web Parts or Page Viewer Web Parts because they are designed as single pages that provide personalized views for every member, and content in those parts cannot be filtered by the current user. However, it can still be useful for some personalization sites to use Content Editor Web Parts to provide important information for users. Similarly, if the purpose of the site is collaboration, a Page Viewer Web Part for a page central to that collaboration can be helpful.

The My Workspace Sites Web Part displays a list of all workspaces and sites within the personal site or personalization site. In the case of personalization sites, if the purpose of the personalization site involves collaboration or viewing other sites related to the personalized view, you can create those sites and include links here so that users can quickly and easily move from personalization information to related content and tasks. The My Links Web Part can be used to provide links to other relevant content other than subsites of the personalization site. Although users can add their own links to this Web Part, administrators might decide to add and target important links during initial deployment.

As with any Web Part, the core personalization parts can be targeted to audiences, so you can use one personalization site that has some parts targeted to different groups of users. This is useful when the personalization site has the same broad purpose, but different groups of users have different related links, or only some of them need to see workspace sites.

### Plan for lists and libraries Web Parts on My Sites

Lists and libraries Web Parts are used by all three My Site templates to include links for relevant lists and libraries. Each template has a different set of available list and libraries Web Parts.

The one Web Part of this kind for the public profile is the Document Library Web Part. This Web Part can be used to associate a library with the public profile. That document library appears on every public profile for every user, and is visible to all users who view the page. The documents in this library are typically documents of general interest for users who view public profiles, such as a frequently asked questions list.

The lists and libraries Web Parts for personal sites are:

 Cache Profiles Web Part

 Reports List Web Part

 Reusable Content Web Part

 Shared Documents Web Part

 Shared Pictures Web Part

 Site Collection Documents Web Part

 Site Collection Images Web Part

 Style Library Web Part

Users can also add Web Parts to their personal sites based on lists created in the personal site. Those are the only lists and libraries Web Parts available by default in the galleries for personalization sites. You can add additional lists and libraries Web Parts to the personalization site galleries by exporting them from sites and galleries where they are available. Some Web Parts are associated with certain features of Office SharePoint Server 2007 and are only available when the related feature is enabled. For example, the business data Web Parts appear when the Office Server Enterprise feature is activated.

You can add parts for important lists to the default template of the personal site. For example, you can add key documents and pictures to Shared Documents and Shared Pictures Web Parts, which encourages users to add more documents and pictures to those shared lists over time. You can also add Web Parts for KPI lists that are already linked to real business processes that provide meaningful status indicators as part of the initial personal site experience, and add some lists as default personal site content so they can be added by users as Web Parts later on.

These parts are even more useful in personalization sites to add lists for important content that is relevant to the purpose of the site. A list Web Part can be added that is linked to the Current User Filter Web Part so that it displays performance information that is personalized for each user who uses the site.

### Plan for business data Web Parts on My Sites

The business data Web Parts available in the gallery for all three templates of My Site are:

 Business Data Actions Web Part

 Business Data Related List Web Part

 Business Data Item Web Part

 Business Data List Web Part

 Business Data Item Filter Web Part

 IView Web Part

 WSRP Consumer Web Part

The first four business data Web Parts are used to display information based on the properties of applications registered in the Business Data Catalog. The Business Data Item Filter Web Part filters the other Web Parts within the page based on values found in the Business Data Catalog. The IView and WSRP Web Parts support the presentation of data from SAP and WSRP subsites, respectively.

Additional business data Web Parts available for the personal site and personalization sites, but not public profiles, include:

 Excel Web Access Web Part (listed in the Default gallery category)

 SQL Server 2005 Analysis Services Web Part

The Excel Web Access Web Part is used to provide information from a specific worksheet directly within the Web Part by using Excel Calculation Services. The SQL Server 2005 Analysis Services Web Part is available for personal sites and personalization sites for rendering data directly from SQL Server 2005 Analysis Services.

Business data Web Parts provide a way to present information from data sources, such as business applications registered in the Business Data Catalog, to provide key information about users in sites. In the context of public profiles, you might want to provide business data relevant to the user profile that is being viewed, and the person who is viewing the user profile. Depending on the part used, this can include lists of business data, key properties of business data, and important business actions. For personalization sites, you can add business data Web Parts for business applications that are central to the purpose of the site, and connect those parts to the Current User Filter Web Part so they provide information personalized for each user. The Business Data Associations Web Part, Business Data Details Web Part, and Business Data List Web Parts each provide distinct views of business data.

You use the Business Data Actions Web Part to include links to perform custom business actions that the administrator of the Business Data Catalog has planned and created based on the common tasks associated with core business applications. Business actions provide a particularly useful possibility for public profiles. For example, you can create a custom action that returns business data for the user profile that is being viewed. Employees viewing public profiles in a call center site collection might be able to click View Customer Service Records for this Person. Anyone could click someone's name anywhere in the site collection, and then click this action, and be provided with a page linked to the customer service database that would display a list of customer service records for that user.

This is also useful for personalization sites. In the same call center site collection example, a personalization site could use Business Data Actions Web Parts to provide actions to resolve customer service records, open existing records, or transfer cases to other service departments, all without having to start a separate application or find another page.

You can also add business data Web Parts to the personal site template to encourage individual users to use those Web Parts. By providing links to personalization sites that also use that Web Part, you can demonstrate the possibilities for viewing business data Web Parts so that users are more likely to add the Web Parts in their personal sites.

When planning My Sites, you can easily go overboard by adding too many actions and other business data. As always during initial planning, only include the most important business data for each site.

For more information about business data Web Parts, see [Plan business data Web Parts](#DSDOC_165f1afe_11e5_4c45_8f93_bf16e18338).

For more information about business data actions, see [Plan business data actions](#DSDOC_60b8a5be_c54e_488c_90b0_80f4aeba40).

### Plan for dashboard Web Parts on My Sites

Because KPI Web Parts are commonly used in dashboards, they are also called dashboard Web Parts in My Site Web Part galleries. Dashboards, also known as multi-report summary pages, contain one or more business intelligence Web Parts, such as business data Web Parts, Excel Web Access Web Parts, or KPIs that can be filtered at the page level by various properties to get a unified view of data and content from several sources.

The dashboard Web Parts are:

 KPI Details Web Part

 KPI List Web Part

These Web Parts are available in the Web Part galleries for all three My Site templates.

KPI Web Parts can be useful for presenting personalized performance information for key business goals. For public profiles and personalization sites, these might be status indicators that apply to individuals and not entire groups or organizations. For example, you could create a KPI (by using either a KPI List Web Part along with other KPIs, or as a KPI Details Web Part) that is based on an Excel workbook of sales reports for all employees. When you add that Web Part to a personalization site, the current user filter will only calculate the KPI for the current user. The same KPI on another page without the same filter would calculate the KPI for all users whose sales are documented in the source Excel workbook.

If the KPI is of interest only to some users, such as users within the same workgroup, you can target the Web Part to an audience defined to include only the users in the workgroup. For example, if the sales KPI is based on a spreadsheet from the New York sales office, you can target the KPI Web Part to only show results for users working in that office, and use another targeted KPI Web Part for users in another office.

You can use the KPI List Web Part to display several status indicators within one Web Part, such as number of sales, the dollar value of sales, improvement over the last quarter, and customer satisfaction. The KPI Details Web Part only shows a single KPI, such as number of sales.

You can also add a KPI, possibly targeted by team, that shows results at the team level and is not connected to the current user filter. This information might still be useful in a personalization site because it provides information that relates to other Web Parts that are personalized. This is a common scenario for KPI Web Parts on personalized sites because KPIs tend to indicate performance information calculated across groups rather than for individuals.

As with any site planning, before you add a KPI Web Part you should consider the purpose of the site collection that contains the public profile or personalization site. If the site collection is a team site for a sales team, sales data KPIs make sense. If it is a site collection intended for collaboration across a larger organization, the KPI will have to match the breadth of that collaboration or be targeted if it is included at all. If it is a site for human resources information, which is not used by any group in the organization to meet its goals but instead simply provides policies and business applications, you probably will not use a KPI Web Part.

After deciding whether to use KPIs, make decisions about who should see what data, and use audiences and Current User Filter Web Parts to tailor KPIs to your organization.

Consider whether particular KPIs are more appropriate in public profiles or within personalization sites. Users are more likely to look for information about a particular business process in the Report Center site or a personalization site designed for that purpose, rather than in their own or someone else's public profile page. Only include KPIs in public profiles to reinforce the most important indicators for your organization, or when the information is something that is central to the role of each user who views the public profile.

Remember to plan for the data sources that provide information for KPIs. For more information, see [Plan key performance indicators](#DSDOC_d8f9b41e_e324_490d_bf85_1370c8b63b).

### Plan for filter Web Parts on My Sites

Filter Web Parts are available for all three My Site templates. The default filter Web Parts available are:

 Authored List Filter Web Part

 Business Data Catalog Filter Web Part

 Current User Filter Web Part

 Filter Actions Web Part

 Page Field Filter Web Part

 Query String (URL) Filter Web Part

 SharePoint List Filter Web Part

 SQL Server 2005 Analysis Services Filter Web Part

 Text Filter Web Part

### Plan for miscellaneous and custom Web Parts on My Sites

Personal sites can select the following miscellaneous Web Parts:

 Contact Details Web Part

 Form Web Part

 XML Web Part

Personalization sites can use those Web Parts, and can also use the following additional Web Parts:

 From the Default group in the Web Part gallery:

 Advanced Search Box Web Part

 Category Results Web Part

 Category Web Part

 People Search Core Results Web Part

 Search Box Web Part

 Search Paging Web Part

 Search Statistics Web Part

 Search Summary Web Part

 Search Core Results Web Part

 Search High Confidence Web Part

 Site and Documents Web Part

 Tasks and Tools Web Part

 This Week in Pictures Web Part

 Top Sites Web Part Web Part

 From the Miscellaneous group in the Web Part gallery:

 Content Query Web Part

 Summary Link Web Part

 Table of Contents Web Part

The Form Web Part is used to connect a simple form to other Web Parts on the page. Along with the XML Web Part form, you can add significant interactivity to a personalization page.

Most of the other miscellaneous Web Parts enable you to add search functionality right into the personalization site. When you plan for search, consider how you want personalization sites to work with the content sources and search scopes you have created for the site collection and SSP as a whole.

In addition to the Web Parts that are available in galleries for the My Site templates, you can create custom Web Parts. For more information about designing custom Web Parts, see the [Microsoft Office SharePoint Server 2007 Software Development Kit](http://go.microsoft.com/fwlink/?LinkID=71218&clcid=0x409) (SDK) (http://go.microsoft.com/fwlink/?LinkID=71218&clcid=0x409).

## Plan for personalized Web Parts on other sites

You can personalize Web Parts on other pages in several ways, including:

 Using the Current User Filter Web Part on a dashboard or any other site to filter data from other Web Parts based on the identity of the current user.

 Using the Business Data Catalog Filter Web Part to filter business data Web Parts based on properties of business data types in applications registered in the Business Data Catalog, such as people in SAP.

 Using the IView Web Part specifically with SAP to present personalized data from IView in SAP.

 Adding one or more audiences to the Target Audiences text box in the Advanced section of the Web Part tool pane.

## Worksheet

Use the following worksheet to plan for personalized Web Parts:

 [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409)

# Plan My Sites

In this article:

 [About My Sites](#DSDOC_section14edf74cf_8808_4277_ba10_b1)

 [Plan for personalized sites](#DSDOC_section24edf74cf_8808_4277_ba10_b1)

 [Worksheet](#DSDOC_section34edf74cf_8808_4277_ba10_b1)

To effectively plan My Sites, you must decide the following:

 Whether or not to activate the My Site feature.

 Which users you want to have My Sites.

 Where to store and manage personal sites within and across Shared Services Providers (SSPs).

 Which templates will be used in My Sites and which Web Parts will be used to extend their functionality.

 Which policies will be applied for viewing user profile information in the public profile.

 Which personalization sites to create on other site collections.

## About My Sites

In Microsoft Office SharePoint Server 2007, My Sites are special SharePoint sites that are personalized for each user. My Sites are enabled by default, and every user in an organization has a unique My Site.

A My Site is composed of three types of My Site pages, each with its own template:

 Public profile page   Anyone in the organization can see a public profile page, which is hosted in the My Site template.

 Personal site   This is for storage of each user's content and for easy collaboration with colleagues. Each personal site has a private home page that only that user can see.

 Personalization site   This is owned by site collection administrators or users designated as site administrators by the site collection administrator, and contains information personalized and targeted to the user. Each My Site provides a personalized navigation bar that connects personalization sites with other parts of the My Site.

My Sites also include personalized views of links, documents, and other Office SharePoint Server 2007 features.

Each user can view the My Site by clicking on the My Site link in the portal site. The My Links menu includes links to all sites of which someone is a member, and links to pages where users can add to and manage the links.

Users can navigate between their personal site home pages, the public profile, and personalization sites by clicking the tabs in the My Site top link bar.

The common features of all personalization sites include:

 Branding   This is inherited from the main site, and replaces the site banner logo with the My Site logo.

 Top and left navigation sections   The left pane contains a picture of the user and the Quick Launch, and the top link bar is specialized for My Sites.

 Four Web Part zones   The four zones include top, bottom, middle left and middle right.

The administrator of each part of My Site has a Site Actions menu that has the following actions available:

 Create   The administrator can add a library, list, or Web page on the site collection that contains My Sites. This library typically contains content, such as pictures for users, lists for business data Web Parts, and other documents and files needed for public profiles and My Site.

 Edit Page   The administrator can edit the Web Parts for the page.

 Site Settings   The administrator can change the settings for the page.

When planning My Sites, ensure that there is a common look that sets them aside from other pages in the site, while still being consistent with the overall appearance of your site. The templates used for My Sites can be customized just as any other template or site. Before you modify the templates for My Sites, it is a good idea to understand the default appearance and functionality of the templates, and the individual Web Parts used by default or available for each site.

For more information about templates and Web Parts in My Sites, see [Plan for personalized Web Parts](#DSDOC_c976bea3_148c_4be6_96b7_6400c12692).

### About the public profile page

The public profile page, also known as the My Site Public Page, is the public view of each user's user profile and My Site. The public profile is accessed by clicking any link to a user within a portal site or site collection, including links in search results. Users can link to edit their own public profiles on the My Profile link in their My Sites.

The layout of public profiles is designed by the site collection administrator for the site that hosts My Sites, and possibly a designer. Though the same user profile is used in every site collection in a single SSP, the look of the public profile can vary from SSP to SSP. Some consistency of the public profile is a good idea, but different sites created for different purposes have good reasons to vary some of their content and appearance. The default layout includes:

 Quick Launch   Links to shared lists, such as Shared Documents and Shared Pictures, and My Site subsites, such as workspaces. These links enable users who visit someone's public profile to quickly view shared content.

 As seen by drop-down list   Seen by users who view their own profile, and has options to see how the public profile looks for different groups of users. The drop-down list is a good way to check that selected policies are working properly.

 Web Parts   These are in each of the four zones.

For details about the Web Parts available for the public profile, see [Plan for personalized Web Parts](#DSDOC_c976bea3_148c_4be6_96b7_6400c12692).

From their own public profile pages, users can return to the personal site by clicking My Home on the My Site top link bar. Users who view public profiles for other users will not see a My Site top link bar because they are not viewing pages in their own My Sites.

### About personal sites

The personal site is each user's My Site home page. The personal site is private by default, so the home page of each personal site can only be viewed by the site owner. The personal site is the page that appears when users click the My Site link for the site, and can also be accessed by clicking My Home on the My Site top link bar by users who want to view their own public profiles. It is also the page that appears when users click links to their own name.

Because the home page of each personal site is private, there are no policy considerations during planning. Each user that has a personal site is administrator of the site and can create and edit other pages, change the default layout or customize the page to personal taste, and change site settings. The default layout for personal sites includes:

 Quick Launch links to:

 View All Site Content page.

 Public profile page and sections within the public profile.

 Shared documents and pictures visible to other users on the public page.

 Lists, discussions, surveys, and sites added by the user and visible to other users on the public page.

 Web Parts in each of the four zones of the home page, and contain private content viewed only by the user of the personal site.

 Recycle Bin for the personal site, which is visible only by the user of the personal site.

All of the Quick Launch links except the Recycle Bin are visible to other users on the public page.

Because each user selects the Web Parts to use for the home page of the personal site, there are fewer planning considerations for Web Parts.

For more information about Web Part planning for personal sites, see [Plan for personalized Web Parts](#DSDOC_c976bea3_148c_4be6_96b7_6400c12692).

The other pages, lists, libraries, and workspaces created in the personal site can be shared and viewed by other users, so in that sense the personal site is not entirely private. The planning considerations for subsites and other shared content are no different from those of any other site, except that decisions are up to each user during normal operations and not an organized planning process before initial deployment.

Users can use the links on the My Site top link bar to switch between the personal site, the public profile, and relevant personalization sites that have been linked by the SSP administrator or that they have personally pinned to the top link bar.

### About personalization sites

Personalization sites target information personalized for every member of the site by using personalized Web Parts and user filter Web Parts. Each personalization site is created by a site collection administrator or another user that has site creation permissions.

Links to personalization sites can be added to the My Site top link bar by SSP administrators, and appear for every member of each site, or targeted to specific audiences. Links to personalization sites can also appear in the top navigation pane and the left pane of the All Site Content page of the main site. Personalization sites are registered by the SSP, so that personalization sites from all site collections that use the same shared service all appear in My Site, depending on the targeted audience of the personalization site link.

Individual users can add links to other personalization sites that have not been registered by an administrator, but those sites only appear on that user's My Site top link bar.

Personalization sites can be branded by using either the main site logo or the My Site logo. The default layout for personalization sites includes:

 Picture of the user above the Quick Launch.

 Quick Launch links, including links to the View All Site Content page and the Recycle Bin for the personalization site.

 Filter Web Parts in the top zone.

 A Content Editor Web Part in the middle left zone that explains the purpose and use of personalization sites.

 A Site Actions menu. The top link bar for Site Settings contains an option to pin the personalization site to the My Site top link bar.

Each site uses filter Web Parts that connect the Web Parts on the site to each user who view the page, but there are no default Web Parts and each personalization site uses a different mix of Web Parts.

For more information about personalization site Web Parts, see [Plan for personalized Web Parts](#DSDOC_c976bea3_148c_4be6_96b7_6400c12692).

Each personalization site can also include subsites, such as workspaces, lists, and libraries that are relevant to the personalization site.

Users can use the links on the My Site top link bar of personalization sites to go to the personal site or the public profile of My Site, and to go to any other linked personalization sites. They can also use the breadcrumb navigation to view other parts of the main site.

## Plan for personalized sites

Different organizations have different personalization needs. When planning My Sites, you can consider several factors:

 My Site feature   Enabled by default in Office SharePoint Server 2007, but some organizations might want to disable it.

 Personal sites in the SSP   Where are personal sites stored and managed, and how My Sites will work across multiple SSPs.

 Policies   Which policies will you apply to information shown on each user's public profile.

 Personalization sites   Which personalization sites are needed, and who will create and own each site.

|  |
| --- |
| Worksheet action |
| Use the [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) to record decisions regarding the sites and site collections for your organization. Also, remember to note who is likely to own managing the public profiles for each site collection. The personalization sites that you plan should be included on a per-site basis by site collection administrators, who will probably have more detailed worksheets planning the organization of the site collections they own. The site collection administrator will want to note plans for ownership of personalization sites that are created during initial deployment. |

### Activate the My Site feature

The My Site feature is activated by default at the Web application level. Some organizations might decide to deactivate the feature for the farm or for individual sites. When deciding whether to use My Site, the following factors are important:

 Site purpose

 Web application performance

The most important factor to consider when deciding whether to use the My Site feature is the purpose of your sites. Sites that are designed to enable users to work and share information easily will almost certainly benefit from My Sites. Each user in the organization will be able to easily find users and information related to them.

On the other hand, sites that are not built upon collaboration might not benefit from personal sites. An example is a large document repository that does not contain team sites or workspaces, does not target content by audience, and is not a place where users go to find or share organizational information about themselves or their colleagues.

Because My Site is activated at the Web application level, it is usually a good idea to retain the feature if any of the sites on the Web application will benefit from using it. One exception to this is a Web application that is optimizing for other functionality of Office SharePoint Server 2007. Although the My Site feature is not particularly resource-intensive, Web applications that have a large number of users, a high volume of content, and relatively little need for personalization or collaboration might benefit from deactivating the My Site feature. Administrators planning for personalization should talk to IT administrators in the organization about performance and capacity considerations if this is a concern.

As soon as the My Site feature is activated, any user profiles from an existing installation of Microsoft Windows SharePoint Services 3.0 are replaced by the public profiles that are part of My Site. A My Site link is added to the top menu bar for all sites in the site collection, along with the My Links menu.

You activate or deactivate the My Site feature from the Manage Web application features link in the SharePoint Web Application Management section of the Application Management tab in Central Administration. You can also limit the ability to create My Sites by removing the right from the authenticated users group for the SSP, or deleting that group from the Personalization Services Permissions page.

You can turn off My Sites at the site collection or site level by deactivating the Office SharePoint Server Standard feature in Site Settings, but you will also lose the search functionality for the site. This can be a good option for sites, such as large document repositories. In that case, the documents on the site can still be crawled so that they appear in searches from other sites in the server farm, without having to support My Sites features that are not relevant for the site but are available on other sites in the farm that have kept the features active.

#### Plan for My Sites in the SSP

SSP administrators for personalization consider the interaction between personalization sites across all site collections in all farms that use the SSP, and how personalization sites are made available within My Sites. They also make decisions about the presentation of the My Site as a whole. Their considerations include:

 Personalization links

 Trusted My Site host locations

 Personal sites settings

These settings are managed from the User Profiles, Audiences, and Personal Sites section of the SSP.

##### Personalization links

Any user who has permission to create sites within a site collection can select the personalization site template, but not all of these sites will be relevant for all users in the site collection, much less all users within the same SSP. Personalization sites that are relevant for users across the SSP can be added as links to the My Site top link bar. Every user who uses My Site will see links to all personalization sites that were linked by the SSP administrator, regardless of site collection, except for personalization site links that are targeted to specific audiences.

Personalization sites planned for initial deployment are important enough to add to the My Site link for the users who use the corresponding site collection, but not all users in the SSP will consider the same personalization sites to be relevant. My Site links to personalization sites can be targeted to specific audiences so they are only seen by relevant users.

For information that applies to everyone in an organization, such as human resources information, a My Site link to the personalization site might make sense for everyone. For a personalization site that shows personalized content to the sales team, it makes sense to target the My Site link so that it appears only for members of that team, or for members of the sales site collection.

|  |
| --- |
| Worksheet action |
| Use the [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) to record decisions regarding which personalization sites will be linked in My Site navigation. Also record decisions about targeting to audiences. |

For more information about audience planning, see [Plan for audiences](#DSDOC_18f26340_695a_40fd_bb4d_1a05f7b5cc).

##### Trusted My Site host locations

From the Shared Services Administration page, you can add additional trusted personal sites locations. This enables SSP administrators to select My Site locations from multiple site locations. This is needed in any scenario that has more than one SSP, such as a global deployment that has geographically distributed sets of shared services, where each SSP contains a distinct set of users. By listing the trusted personal site locations for all other SSPs, you can ensure that My Sites are created in the correct location for each user. This also enables you to replicate user profiles across SSPs.

##### Personal sites settings

By default, My Sites are stored on the server that contains shared services. Public profiles are created and stored on the Web application that contains the Shared Services Administration pages for the SSP, and personal sites are stored on the default Web application for the server. However, you can change the Web application so that My Sites can be stored on the default Web application, the Web application for the SSP, or any other Web application.

Personalization sites are created on individual site collections that can be on any farm that uses the same SSP. The settings for those sites are controlled by the administrators of those respective sites, by using the same Site Settings pages that are available for any site.

Settings for personal sites are managed by the SSP administrator, who can manage settings that are unique for those sites. Personal sites settings appear on the Manage Personal Sites page, which is available from the My Site settings link on the Shared Services Administration page. Manageable settings include the following:

 Personal site services   By default, personal sites are stored on the (same as My Site host) Web application for the server that runs the shared services, typically that uses port 80. The public profiles are also stored on the Web application for the SSP by using a different port. You can decide to set a different provider for personal site services so that personal sites are stored on a different Web application. This can be a different application on the same server or another server. The Web application must already exist. Existing sites are not migrated and must be moved manually. For large organizations, it might make sense to store personal sites on a separate server. When planning personal sites, SSP administrators should talk to IT administrators about the number of users and expected use of personal sites so that the appropriate choice can be implemented during initial deployment. If your deployment process involves using a test server before deploying to a production server, realize that restoring a backup image of the first server to the second server will not update the location of personal site services. You will have to update this property to use the personal site services on the second server.

 Personal site location   This is the Web directory where personal sites are stored and accessed. It is a good idea for this to be memorable, and it should not duplicate directories already used for other purposes. Otherwise, you do not have to plan for this setting.

 Site naming format   There are three options for the format, used to resolve possible conflicts between user names in multiple domains. If your users are in a single domain, you can format by using a simple user name. If your users are in multiple domains, it makes sense to use both domain and user name in the format. The option to resolve conflicts by formatting the second instance of the same user name by including the different domain name should be reserved for after initial deployment, such as when you are adding users from additional domains to a deployment that previously used accounts from a single domain.

 Language options   In a multilingual deployment, you can allow users to choose the language of their personal site.

 Default reader site group   You can select which users are members of the SharePoint Reader group for personal sites. By default, this Reader group is the same as the site collection that contains personal sites, but you can limit access based on specific policies of your organization.

### Plan My Site policies

When considering how to implement My Sites, you must consider how much control you want to give individual users over the visibility and presentation of their personal information, and which policies you want to set for them based on the needs and policy decisions of your organization.

For more information about policy planning, such as what information to provide for all public profiles, and what information to change based on per-site needs, see [Plan for people and user profiles](#DSDOC_267523c2_703f_455e_bbb5_d75f1e2f66).

### Plan for personalization sites

When planning for personalization sites, consider the following factors:

 How personalization sites will fit into the broader information architecture and site structure of your organization.

 Which site collections will benefit from personalization sites.

 Who will own each personalization site.

 Which Web Parts you will use to target content to users of the personalization site.

#### Incorporate personalization sites into site collections

Site collection administrators, SSP administrators, and business planners should consider the information architecture planning to eliminate duplication and identify the most important personalization sites to implement during initial deployment.

It is not necessary to plan for all possible personalization sites. Most sites will be created as needed during ongoing operations. The sites identified during planning for initial deployment should be those that identify content needs or are relevant to key business processes, and can also benefit from personalization.

Good candidates for high-priority personalization sites are those that present a personalized view of key business applications. For example, a human resources site might have a personalization site with Web Parts that link to time reporting, benefits, and other similar business applications. A call center site might present information specific to each customer service representative on its personalization site. A sales reporting site tracking activity in Microsoft Office Excel 2007 might have a personalization site that filters columns based on each user's role on the sales team.

For each of those sites, any number of personalization sites is possible, but only a small number will be central to the purpose of each site. In many cases, one personalization site can capture the key personalized information for the central purposes of the site. If a potential personalization site does not correspond to the central purpose of the site, it can wait until after initial deployment.

Site collection administrators are responsible for planning personalization sites in their site collections and incorporating them into the overall structure of their sites. They identify the personalization sites to plan and implement during initial deployment, based on the central purposes of the site collection.

By default, personalization sites are added to the top bar navigation links for the site collection. Site collection administrators decide whether to keep those navigation links. If a personalization site is important enough to include during initial deployment, it is probably important enough to include at the top level of navigation. However, each organization will organize site navigation differently, and in some cases personalization sites might not be appropriate for the top level.

|  |
| --- |
| Worksheet action |
| Use the [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) to record decisions regarding the organization of personalization sites. |

#### Plan owners of personalization sites

Personalization sites are managed by their owners at the site collection level, and not within the SSP.

#### Plan Web Parts for personalization sites

Personalization sites can use any of the Web Parts provided by Office SharePoint Server 2007, along with any other Web Parts you might create or import from galleries of Web Parts created by others. Some Web Parts are used more often, or provide functionality that is specific to the personalization experience.

For more information about planning personalization Web parts, see [Plan for personalized Web Parts](#DSDOC_c976bea3_148c_4be6_96b7_6400c12692).

## Worksheet

Use the following worksheet to plan My Sites:

 [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409)

# IV Plan workflows

In this chapter:

 [Chapter overview: Plan workflows](#DSDOC_adc8aefd_8c4e_4824_8676_c61c10d180)

 [What are workflows?](#DSDOC_b23efef5_27bb_4eec_8cf3_a5ecb8df53)

 [Plan workflows: Next steps](#DSDOC_62a5b633_67b0_4b1c_a4cf_bb443bf9cc)

# Chapter overview: Plan workflows

A workflow is a feature of Microsoft Office SharePoint Server 2007 that moves documents or list items through a specific sequence of actions or tasks related to a business process. Workflows can be used to manage common business processes such as document review or approval.

The articles in this chapter include:

 [What are workflows?](#DSDOC_b23efef5_27bb_4eec_8cf3_a5ecb8df53) introduces the types of business processes that workflows can facilitate and describes the workflows included in Office SharePoint Server 2007.

 [Plan workflows: Next steps](#DSDOC_62a5b633_67b0_4b1c_a4cf_bb443bf9cc) contains links to topics that will help you in your workflow planning.

# What are workflows?

In this article:

 [About business processes](#DSDOC_section1b23efef5_27bb_4eec_8cf3_a5)

 [Workflows in Office SharePoint Server 2007](#DSDOC_section2b23efef5_27bb_4eec_8cf3_a5)

## About business processes

Much of the work in any enterprise is done by using business processes that depend on the flow of information or documents. These business processes require the active participation of information workers to complete tasks that contribute to their workgroup's decisions or deliverables. In Microsoft Office SharePoint Server 2007, these types of business processes are implemented and managed by using workflows.

Examples of business processes that could be facilitated by workflows include:

 Contract approval   Guiding a proposed contract among members of an organization who must approve or reject it.

 Expense reporting   Managing the submission of an expense report and associated receipts, reviewing the report, approving it, and reimbursing the submitter.

 Technical support   Guiding the progress of a technical support incident as it is opened by a customer, investigated by a support engineer, routed to technical experts, resolved, and added to a knowledge base.

 Interviewing   Managing the process of interviewing a job candidate. This includes scheduling and tracking interview appointments, collecting interview feedback as it accumulates, making that feedback available to subsequent interviewers, and facilitating the hire/no-hire decision.

 Content publishing   Managing the approval of the publication of content on an enterprise's Internet presence site.

One of the problems faced by many IT departments when implementing business processes requiring information workers' participation is that those processes do not integrate with the way people actually work. For a business process to be effective, it must be integrated with the familiar, everyday tools and applications used in the workplace so that it becomes part of the daily routine of information workers. In the electronic workplace, this includes integration with e-mail, calendars, task lists, collaboration Web sites, and client applications such as Microsoft Office Outlook 2007 and Word 2007. This is the approach implemented in workflows based on Office SharePoint Server 2007.

## Workflows in Office SharePoint Server 2007

Office SharePoint Server 2007 includes the following standard workflows that address primary business needs:

 Collect Feedback   Sends a document for review. The author chooses the reviewers, sends instructions, and checks on the workflow's progress. Reviewers receive e-mail notification and are assigned a task with a link to the document to review. Participants can optionally delegate their tasks or decline altogether.

 Approval   Sends a document for approval. Approval is often a prerequisite to another document management task, such as publishing a document to a Web site or submitting a business proposal to a client. As with the Collect Feedback workflow, authors choose approvers, send instructions, and track workflow status. By default, Approval is a serial workflow — the order in which approvers view the document is specified by the author. (By contrast, Collect Feedback is a parallel workflow — reviewers can provide feedback in any order.)

 Disposition Approval   Allows participants to approve the disposition of expired documents.

 Collect Signatures   Routes a document to a set of participants who must sign that document.

 Translation   Manages the translation of a document into one or more languages. This workflow creates placeholder documents and tracks translation tasks for each language version of the source document. If the source document changes, the workflow assigns tasks to update the translated versions.

 Issue Tracking   Routes an issue to team members for resolution.

 East Asian Document Approval   Routes a document for approval by using digital signature stamps and a group-oriented consensus process. This workflow is available only in East Asian product versions and language packs.

In Office SharePoint Server 2007, site designers can associate workflows with libraries, lists, or content types to make them available to run on documents or list items. A workflow's progress is recorded in a workflow history list, and workflow tasks are assigned to participants by using a tasks list.

So that they become part of the daily routine of information workers, workflows are tightly integrated into Office SharePoint Server 2007 and 2007 Microsoft Office system, enabling information workers to easily participate in them. The following tasks can be performed from the Web-based Office SharePoint Server 2007 interface or from 2007 Office release client programs:

 Viewing the workflows available to run on a document or list item.

 Initiating a workflow.

 Viewing and starting a workflow task.

 Completing a workflow task and filling out the task completion form.

Workflows in Office SharePoint Server 2007 are built on the Windows Workflow Foundation component of Microsoft Windows, and software developers can create custom workflows by using the Windows Workflow Foundation Designer in Microsoft Visual Studio 2005. After a workflow built on the Windows Workflow Foundation component of Microsoft Windows is installed and enabled by an administrator, users can associate it with one or more libraries, lists, or content types.

Users can also create custom workflows by using Microsoft Office SharePoint Designer 2007. Each workflow created by using Office SharePoint Designer 2007 can be associated with a single library or list. Using Microsoft Visual Studio 2005, you can create custom workflow actions that can be made available in Office SharePoint Designer 2007. Office SharePoint Designer 2007 includes a visual workflow design environment and a set of workflow actions that users can add to workflows without having to write source code, including:

 Setting list metadata

 Creating, copying, deleting, or changing list items (including documents)

 Checking items in or out

 Pausing, starting, or stopping the workflow

 Sending e-mail messages

 Setting the moderation status of an item

 Setting an item's metadata

 Assigning tasks

## [[7]](#footnote-8)#See Also

[Plan workflows: Next steps](#DSDOC_62a5b633_67b0_4b1c_a4cf_bb443bf9cc)

# Plan workflows: Next steps

This article contains links to topics that will help you in your workflow planning.

## [[8]](#footnote-9)#Planning workflows: Next steps

To continue planning workflows in the context of document management, forms, or publishing, see one of the following topics:

 [Plan workflows for document management](#DSDOC_34bc3a16_91f6_4c62_ae09_821cb94155)

 [Plan workflow for form templates](#DSDOC_76b6409f_d38b_438c_af0a_d8d0a6da95)

 [Plan content approval and scheduling](#DSDOC_b43e9421_66b8_4cfc_ba06_f772ae7420)

## See Also

[What are workflows?](#DSDOC_b23efef5_27bb_4eec_8cf3_a5ecb8df53)

# V Plan for forms

In this chapter:

 [Chapter overview: Plan InfoPath Forms Services](#DSDOC_4ec9c00a_8cb6_407c_9f63_c725ea7c57)

 [Plan what form templates are needed [Office SharePoint Server]](#DSDOC_f669dd10_a737_49ba_b02e_c8b805f30c)

 [Plan custom form templates (Office SharePoint Server)](#DSDOC_3ce912a1_64fe_4a52_8b06_10e7e01381)

 [Plan form template design infrastructure requirements (Office SharePoint Server)](#DSDOC_b6824b9d_596f_4440_9582_c0f98a1bf3)

 [Plan server-side data connections needed for form templates [Office SharePoint Server]](#DSDOC_44e91039_e88f_4088_a97e_1d090a23a1)

 [Plan deployment of form templates [Office SharePoint Server]](#DSDOC_5f80ea0e_ed1e_49f3_80ea_3c7c4441ac)

 [Plan deployment of administrator-approved form templates [Office SharePoint Server]](#DSDOC_7de89276_e882_4abc_9699_6f70dee463)

 [Determine the impact of anonymously accessible form templates](#DSDOC_0ee46518_8f98_46ee_ae9a_ec2f8b46a8)

 [Plan for naming form templates [Office SharePoint Server]](#DSDOC_2a841374_b8ad_4dc8_85fe_03c137284a)

 [Plan for upgrading form templates [Office SharePoint Server]](#DSDOC_2785361f_decf_4308_a217_00a32949ae)

 [Plan for retiring form templates [Office SharePoint Server]](#DSDOC_dc9e1e37_0a74_4613_9cbd_cba727c5ef)

 [Plan version control for form templates [Office SharePoint Server]](#DSDOC_8d734e5b_e0a4_497b_9524_ff9153f15b)

 [Plan for mobile device access to form templates [Office SharePoint Server]](#DSDOC_5af84900_6501_47c9_8c25_0e8c8944fb)

 [Plan workflow for form templates](#DSDOC_76b6409f_d38b_438c_af0a_d8d0a6da95)

# Chapter overview: Plan InfoPath Forms Services

In this article:

 [InfoPath Forms Services planning articles](#DSDOC_section14ec9c00a_8cb6_407c_9f63_c7)

 [Scenario planning](#DSDOC_section24ec9c00a_8cb6_407c_9f63_c7)

Using InfoPath Forms Services, you can publish form templates that can be opened either in Microsoft Office InfoPath 2007 or rendered in a Web browser.

note_ddNote:

InfoPath Forms Services is a component of Microsoft Office SharePoint Server 2007 and should not be confused with Microsoft Office Forms Server 2007, a separate product.

This technology requires specific server configuration, server resource and network bandwidth allocation, consideration of security and user management, and careful planning related to the deployment, accessibility, and management of form templates. You do not have to install InfoPath Forms Services separately, as it is installed with Microsoft Windows SharePoint Services. In order to make the most effective use of InfoPath Forms Services, you need to do some planning. The planning tasks have been organized into articles to make it easier for you to find the planning information you need for each step.

note_ddNote:

"Forms" and "form templates" are separate entities. A form is an instance of a form template, invoked when the form is opened from a document library or when a Web page containing a form is opened. A form template is an .xsn file that resides on a server and contains the code that generates a form.

For example business scenarios for InfoPath Forms Services, see [Scenario planning](#DSDOC_section24ec9c00a_8cb6_407c_9f63_c7) in this article.

## InfoPath Forms Services planning articles

### Before you begin designing form templates

[Plan what form templates are needed [Office SharePoint Server]](#DSDOC_f669dd10_a737_49ba_b02e_c8b805f30c)This article helps you to plan what form templates you need to create. It also helps you understand which of your current forms can be imported and which must be recreated manually, and the factors that should be taken into account.

[Plan for naming form templates [Office SharePoint Server]](#DSDOC_2a841374_b8ad_4dc8_85fe_03c137284a)   This article helps you to establish a naming convention for form templates.

### Planning form template design

[Plan form template design infrastructure requirements (Office SharePoint Server)](#DSDOC_b6824b9d_596f_4440_9582_c0f98a1bf3)Before you begin deploying form templates in an InfoPath Forms Services production environment, read this article to help you consider the server, security, and network requirements to support your deployment.

[Plan custom form templates (Office SharePoint Server)](#DSDOC_3ce912a1_64fe_4a52_8b06_10e7e01381)   Read this article to help you develop custom form templates to address specific forms needs.

[Plan server-side data connections needed for form templates [Office SharePoint Server]](#DSDOC_44e91039_e88f_4088_a97e_1d090a23a1)   This article describes how server-side data connections function when a form template is deployed, and it assists you with planning for the data connections you need.

### Planning form template deployment

[Plan deployment of form templates [Office SharePoint Server]](#DSDOC_5f80ea0e_ed1e_49f3_80ea_3c7c4441ac)   This article helps you to understand the deployment process for the two categories of browser-compatible form templates: user form templates and administrator-approved form templates.

[Plan deployment of administrator-approved form templates [Office SharePoint Server]](#DSDOC_7de89276_e882_4abc_9699_6f70dee463)   Read this article to help you plan for the deployment of form templates that contain business logic such as a compiled, managed code DLL (form code); require full trust; or use a data connection that is managed by an administrator.

### Planning server supportability and maintenance

[Plan for upgrading form templates [Office SharePoint Server]](#DSDOC_2785361f_decf_4308_a217_00a32949ae)   Read this article to help you plan for upgrading administrator-deployed form templates.

[Plan for retiring form templates [Office SharePoint Server]](#DSDOC_dc9e1e37_0a74_4613_9cbd_cba727c5ef)   Read this article to help you plan for retiring form templates when they become obsolete.

[Plan version control for form templates [Office SharePoint Server]](#DSDOC_8d734e5b_e0a4_497b_9524_ff9153f15b)   Read this article to help you plan for enabling version control, which causes document libraries to create a new version of the form template every time the template is edited and saved, preserving previous versions as defined by the administrator.

[Plan for mobile device access to form templates [Office SharePoint Server]](#DSDOC_5af84900_6501_47c9_8c25_0e8c8944fb)   Read this article to help you plan for providing access to browser-enabled forms from mobile devices such as handheld PDAs that support HTML, CHTML, or XHTML.

InfoPath Forms Services Best Practices   Read this article for best practices for InfoPath Forms Services.

## Scenario planning

You need to carefully plan before you implement InfoPath Forms Services in your organization. You need to consider that InfoPath Forms Services can:

 Integrate with other applications in Office SharePoint Server 2007.

 Integrate with other systems such as e-mail.

 Retrieve data from or push data to databases.

Several factors can make this process complex and challenging. Your organization should decide what purpose forms will serve in the enterprise. Forms can be critical business artifacts in many organizations.

Many organizations use scenario planning to make strategic decisions about how forms are used. The basic method is for a team to generate a scenario that incorporates known facts about the future. For example, the scenario can include the following:

 System capacity

 Network topology

 Number of users

 Location of users

 Server configuration

 Legacy system integration

 Form complexity

 Session length

This section contains some sample scenarios for the use of InfoPath Forms Services.

### Scenario 1: Expense-Report Submission

A. Datum Corporation, a national computer equipment and IT services provider, sells computers, networking hardware, and IT service contracts. A. Datum Corporation has 10,000 employees in North America. Many A. Datum Corporation teams — including marketing, sales, and support consultants — incur and report work-related expenses. These teams represent about one third of the A. Datum workforce.

#### Situation

A. Datum Corporation has adopted mySAP ERP for its business data and operations. It wants to add InfoPath Forms Services to its environment to take advantage of data connections to its back-end systems. By deploying InfoPath Forms Services, A. Datum intends to benefit in the following ways:

 Streamline the process of expense-report submission, review, approval, and reimbursement.

 Increase data accuracy through data validation and business logic built into the form.

 Enable expense reports to be completed online or offline.

 Enforce corporate expense policy rules at the time of expense-report submission.

 Provide immediate access to expense-report status and expense data.

In addition, A. Datum wants to leverage the advantages realized through Office SharePoint Server 2007 such as document management, team collaboration, and workflow features available with SharePoint sites. The corporation plans to connect the SharePoint sites to its SAP portal so that it can search and index the content along with its other business information.

#### Solution: Forms for internal use

The IT department in A. Datum Corporation is responsible for deploying and maintaining InfoPath Forms Services and connecting it to SAP. It is concerned with keeping its business-critical information available and secure. It is responsible for ensuring that the end-user experience is smooth and that response times are within acceptable limits. Time studies indicate that users take about 30 minutes to complete an expense report. To accommodate the new expense-reporting forms, the IT department is preparing to do the following:

 Provide intranet access for employees accessing the forms within the corporate network.

 Provide dial-up access to a remote access server for employees outside the corporate firewall.

 Provide the Microsoft Office InfoPath 2007 client for those employees who require offline capability.

 Deploy this solution on a medium server farm.

### Scenario 2: Insurance claims processing

A large organization introduces Office SharePoint Server 2007 into its environment to enable customers, insurance agents, and related businesses to use online forms for processing insurance claims. The organization has been using InfoPath 2003 internally but wants to make its forms browser-enabled.

#### Situation

Humongous Insurance is a large multinational company that sells insurance products for boat, automobile, and home owners. These products are sold to both consumers and corporate clients. Humongous Insurance has a large, mobile workforce of over 10,000 people that includes salespeople, claims adjusters, attorneys, IT staff, HR staff, and finance staff. Humongous Insurance is based in the United States, but has offices in Canada and several Latin American countries.

#### Solution 1: Forms for internal use

The insured customer contacts his Humongous Insurance agent by telephone to file a claim. The agent connects to the corporate claims Web site and completes the claim form for the customer. The agent forwards the claim by e-mail to the adjuster, who conducts an inspection. The adjuster approves repairs and costs. The adjuster completes the form that was sent in e-mail and returns it to the agent. The agent reviews the form for accuracy and then forwards it to the accounting department for payment processing. A representative from the accounting department approves a check and archives the claim form. The form is stored as an XML document in the Humongous Insurance claims database. The repairs are done and the customer is refunded the covered amount. Relevant account information is updated accordingly.

#### Solution 2: Customer-facing forms

Alternatively, a Humongous Insurance customer can file a claim over the Internet. The customer need not wait for regular business hours to file a claim. The customer can go to the Humongous Insurance Web site, establish her account, log on, and file the claim. In this case, the customer completes the form that is typically completed by the agent. After the customer submits the form, it is sent to the adjuster by e-mail and a copy of the e-mail is sent to the agent. The adjuster returns the form to the agent if additional information is needed. From this point, the claim form is handled in the same way as a claim initiated by a telephone call.

### Scenario 3: Online government permits

A local government agency uses Office SharePoint Server 2007 and InfoPath Forms Services to provide permit application and approval to contractors over the Internet.

#### Situation

An electrical contractor successfully bids a job for electrical service updates to a home, and seeks a permit issued by the local government agency to complete this work. The electrical contractor goes to the Web site for the City Power and Light Department of Building Inspections to apply for a permit by using an online service. The contractor has previously registered to use this service. His company information, as well as a prior permit request, is already stored.

#### Solution 1: Customer-facing forms

Data entered into the permit application Web form is submitted to an XML database located on the network of the Department of Building Inspections. After the application data is submitted, a new permit request is automatically populated to a SharePoint workspace as a link to a multi-part InfoPath form. When the form is opened, the requesting contractor’s company data and permit application data are populated into fields in the first view of the form. This view is identical to the form that the contractor completed.

#### Solution 2: Forms processing workflow

As part of the process, City Power and Light Department of Building Inspections must formally acknowledge receipt of the application. The receiving agent checks the information for completeness and digitally signs the application form to confirm receipt. A precise image of the application form acknowledging receipt by the department is sent by e-mail to the contractor. InfoPath uses data adapters to access data relevant to qualifying a decision. InfoPath pulls this information from other internal agency data sources into the form in other views. The agency employee reviews this other data, adjudicates the request based upon this merged information, and approves or denies the permit request. If the request is approved, an electrical permit, populated with the requestor’s contact data and relevant information, is rendered in HTML. The permit is posted to the contractor’s home page on the Department of Building Inspections Permit SharePoint site, where the contractor can view and print the permit for posting on the job site.

# Plan what form templates are needed [Office SharePoint Server]

In this article:

 [Create an inventory of current forms](#DSDOC_section1f669dd10_a737_49ba_b02e_c8)

 [Survey the advantages of online forms](#DSDOC_section2f669dd10_a737_49ba_b02e_c8)

 [Assess the need for new form templates](#DSDOC_section3f669dd10_a737_49ba_b02e_c8)

 [Determine form template complexity](#DSDOC_section4f669dd10_a737_49ba_b02e_c8)

 [Worksheet](#DSDOC_section5f669dd10_a737_49ba_b02e_c8)

It is important that you follow some planning steps when you are considering what form templates you will need. Most organizations already have forms in use, and while some of these forms can be imported, you will almost certainly want to create new form templates. This article helps you plan what form templates you need to create. It also helps you understand which of your current forms can be imported and which must be recreated manually, and the factors that should be taken into account.

At the end of this article, you should use the [Inventory of existing forms](http://go.microsoft.com/fwlink/?LinkId=73266) worksheet (http://go.microsoft.com/fwlink/?LinkId=73266) to list your current form inventory. In the article named [Plan what form templates are needed [Office SharePoint Server]](#DSDOC_f669dd10_a737_49ba_b02e_c8b805f30c), you will use the "Plan deployment of administrator-approved form templates" worksheet to record the form templates you will initially create, and the existing forms you will import.

## Create an inventory of current forms

Before you deploy InfoPath Forms Services, it is important to identify what forms are currently used in your organization. Forms exist in many different formats, including:

 Microsoft Word

 Paper

 Fax

 E-mail

 Web

 Microsoft Office InfoPath 2003

 Other software

Determine whether your existing forms are useful and effective. Some parts of forms or entire forms might not fulfill the purpose for which they were originally designed. Some forms might duplicate other forms. Identify the forms that you want to keep. Of the forms that you want to keep, determine which ones can be developed and deployed to InfoPath Forms Services. Determine if forms should be combined. Identify which forms can be eliminated, either by retiring them or by combining them with another form.

## Survey the advantages of online forms

There are a number of reasons that an organization would decide to move forms from their legacy format to an online version. The key advantages for doing this with InfoPath Forms Services are:

1. Microsoft Office InfoPath 2007 provides a design-once model for both form templates that are viewed and edited in the Office InfoPath 2007 program, and browser-compatible form templates that are viewed and edited in a browser. All declarative rules in the form work identically when a form is filled out by using Office InfoPath 2007 or a Web browser. Similarly, all business logic written in a .NET Framework language to the new managed object model will run identically in both environments. This allows developers to design rich, complex forms once without having to worry about creating different versions.

2. The Office InfoPath 2007 design mode allows form template designers to define simple validation rules, calculations, and conditional formatting declaratively, without having to write any code. All of these declarative rules run as is on InfoPath Forms Services without making any server-specific or browser-specific changes.

3. A simple deployment model and features for form template management are available. InfoPath Forms Services provides a one-step deployment model through the InfoPath Designer and also integrates with the Microsoft Windows SharePoint Services 3.0 and Microsoft Office SharePoint Server 2007 infrastructure to provide administration and manageability tools.

4. No download or custom installation is required on the client in order to fill out a form.

5. InfoPath Forms Services can understand XML schemas inherently and can provide a rich, flexible, dynamic, and familiar user model for working with nested, repeating, and optional sections. InfoPath Forms Services also has advanced capabilities for defining validation rules and applying them at run time to catch data integrity problems at the source. All of these capabilities are available when filling out InfoPath forms, whether in a Web browser or in Office InfoPath 2007.

6. Forms are commonly used as a front end for a more complex business process where the collected data needs to flow through predefined workflow and server processes. Form fields might be mapped to rows and fields in a database. InfoPath Forms Services provides excellent connectivity to Web services with built-in functionality that can let you consume data from or submit data to a Web service without writing a single line of code.

7. Office InfoPath 2007 is built on the XML standard. InfoPath form templates are based on an underlying XML schema that defines the shape of the data captured by the form. The form is an XML file complying with this schema. Data can easily be retrieved from and submitted to external data sources. This is also true for forms running in a Web browser. Because of this standard data format, form template designers can directly manipulate the data captured through Office InfoPath 2007.

8. InfoPath Forms Services supports a complete managed object model for forms that can take a dependency on the Microsoft .NET Framework. Business logic written in C# or Visual Basic that takes advantage of this object model runs directly without recompilation on InfoPath Forms Services.

9. Microsoft Windows SharePoint Services 3.0 architecture allows administrators to take advantage of CPU and memory upgrades to both scale up and scale out the performance of InfoPath Forms Services to meet demands.

10. InfoPath Forms Services is natively compatible with the dominant browsers on all platforms.

## Assess the need for new form templates

While creating the planning scenario and forms inventory, you might identify gaps where a new form template can fill a need. You might find that InfoPath Forms Services technology offers new opportunities that were not previously practical or possible with current forms. For example, paper forms do not integrate with e-mail. A new form template that integrates with e-mail, if it is appropriate to your scenario, might be valuable. The worksheet in this article includes a section for assessing your need for new form templates.

## Determine form template complexity

You have a wide range of options when designing a form template in Office InfoPath 2007. A form template can be simple and short-lived. For example, a workgroup might create a form to determine who will attend a meeting next week. A form template can also be very complex. For example, the form template might:

 Use form code.

 Contain multiple data connections.

 Require deployment by the administrator of the server farm. Understanding the complexity of your form template can help you determine the impact on system resources.

Questions you need to answer when you plan for InfoPath Forms Services include the following:

 Will the form template be exposed to anonymous users?

 Will this be an administrator-approved form template? That is, is this a form template that can only by deployed by an administrator because it requires full trust, contains form code, or uses an administrator-managed data connection?

 Will this form template use data connections to submit or retrieve data from external sources? For more information about data connections, see [Plan server-side data connections needed for form templates [Office SharePoint Server]](#DSDOC_44e91039_e88f_4088_a97e_1d090a23a1).

 How many people are expected to use this form template over its life span?

 What will the average number of concurrent users be for the form template?

 What is the expected number of concurrent users during peak usage?

 What is the expected session length for the form template?

 Will users access the form template offline?

 Will the form template require a digital signature?

 Will workflow be applied to this form template, or is the form template intended to be used in a workflow?

## Worksheet

Use the [Inventory of e](http://go.microsoft.com/fwlink/?LinkId=73266) (http://go.microsoft.com/fwlink/?LinkId=73266) to list your current form inventory.

## [[9]](#footnote-10)#See Also

[Plan deployment of administrator-approved form templates [Office SharePoint Server]](#DSDOC_7de89276_e882_4abc_9699_6f70dee463)

# Plan custom form templates (Office SharePoint Server)

You can develop custom form templates to address specific forms needs. Microsoft Office InfoPath 2007 provides several form templates that can be customized for your organization's needs and systems, but most organizations find that they need to design custom form templates to suit their specific needs.

For example, an insurance company may need to design a form template to gather accident claims information, with certain form fields being populated by existing database entries related to the customer. Because such a form template would contain specialized logic and data connections, it would need to be designed from the ground up.

InfoPath form templates can also be created by importing forms from Microsoft Office Word 2007 and Microsoft Office Excel 2007 documents. For more information, see [Convert a Word document to an InfoPath form template](http://go.microsoft.com/fwlink/?LinkId=74648) (http://go.microsoft.com/fwlink/?LinkId=74648) and [Convert an Excel workbook to an InfoPath form template](http://go.microsoft.com/fwlink/?LinkId=74649) (http://go.microsoft.com/fwlink/?LinkId=74649) on Office Online.

Custom form templates that contain form code, require full trust, or use a data connection managed by a server administrator must be approved and deployed by an administrator. Such form templates are called "administrator-approved form templates." For more information, see [Plan deployment of administrator-approved form templates [Office SharePoint Server]](#DSDOC_7de89276_e882_4abc_9699_6f70dee463). If a form template does not contain form code, require full trust, or use a data connection managed by an administrator, you can configure InfoPath Forms Services to permit users to deploy such form templates, called "user form templates," without administrator approval.

## See Also

[Plan what form templates are needed [Office SharePoint Server]](#DSDOC_f669dd10_a737_49ba_b02e_c8b805f30c)

[Plan deployment of form templates [Office SharePoint Server]](#DSDOC_5f80ea0e_ed1e_49f3_80ea_3c7c4441ac)

[Plan deployment of administrator-approved form templates [Office SharePoint Server]](#DSDOC_7de89276_e882_4abc_9699_6f70dee463)

# Plan form template design infrastructure requirements (Office SharePoint Server)

In this article:

 [Server requirements](#DSDOC_section1b6824b9d_596f_4440_9582_c0)

 [Network requirements](#DSDOC_section2b6824b9d_596f_4440_9582_c0)

 [Security requirements](#DSDOC_section3b6824b9d_596f_4440_9582_c0)

Before you begin deploying form templates in an InfoPath Forms Services production environment, it is important that you carefully consider the server, security, and network requirements to support your deployment. InfoPath Forms Services can support many thousands of form templates of varying degrees of complexity, and it provides support for user-deployed form templates. As with any enterprise system, it is crucial to design your infrastructure to support the intended level of usage and to establish a clear strategy for scaling the system to meet increased capacity requirements.

note_ddNote:

Once you have established the expected usage and size of your deployment, you should always deploy to a staging system before you deploy to a production environment. This allows you to establish performance and capacity baselines and to ensure that your design functions as expected.

The factors you need to consider include:

 Expected number of users

 Expected number of form templates

 Expected life cycle of form templates (the length of time that a form template will be used before being retired or upgraded)

 Complexity of form templates (for example, how many form templates will use data connections or complex code, or instantiate a workflow)

 Security considerations

You should read the following Microsoft Office SharePoint Server 2007 planning articles before you begin planning your InfoPath Forms Services infrastructure:

 [Chapter overview: Plan for performance and capacity (Office SharePoint Server)](#DSDOC_8dd52916_f77d_4444_b593_1f7d6f330e)

 [Chapter overview: Design server farms and topologies [Office SharePoint Server]](#DSDOC_b474b3dd_b1e3_4d3e_a83c_bc4a6ec4e0)

 [Chapter overview: Design logical architecture](#DSDOC_1a8e707a_a9b9_4cc1_9daa_08d450692d)

 [Chapter overview: Plan for performance and capacity (Office SharePoint Server)](#DSDOC_8dd52916_f77d_4444_b593_1f7d6f330e)

 [Chapter overview: Plan for and design security (Office SharePoint Server)](#DSDOC_3df68222_235b_45de_82fa_b89166c5c6)

## Server requirements

Because InfoPath Forms Services is only one component of Office SharePoint Server 2007, you need to ensure that your overall Office SharePoint Server 2007 planning process takes into account the particular requirements of InfoPath Forms Services. You may need to increase server capacity to accommodate InfoPath Forms Services users and form templates, particularly if you plan to deploy anonymous form templates to the Internet or plan to deploy complex form templates that require considerable memory and processor time.

For more information on infrastructure and capacity planning for Office SharePoint Server 2007, see the Office SharePoint Server 2007 planning articles [Chapter overview: Design server farms and topologies [Office SharePoint Server]](#DSDOC_b474b3dd_b1e3_4d3e_a83c_bc4a6ec4e0) and [Chapter overview: Plan for performance and capacity (Office SharePoint Server)](#DSDOC_8dd52916_f77d_4444_b593_1f7d6f330e).

## Network requirements

In general, you should follow common networking best practices for enterprise systems, such as:

 Use a firewall between tiers, and between front-end Web servers and the Internet.

 Use a high-speed network backbone for intra-server communications.

 Monitor the network environment for peak bandwidth usage and denial-of-service attacks.

 Perform regular network security audits.

For more information on network requirements, see the Office SharePoint Server 2007 planning article [Chapter overview: Design server farms and topologies [Office SharePoint Server]](#DSDOC_b474b3dd_b1e3_4d3e_a83c_bc4a6ec4e0).

## Security requirements

InfoPath Forms Services security takes advantage of the Office SharePoint Server 2007 security framework, but InfoPath Forms Services has its own security considerations apart from Office SharePoint Server 2007 security, which include the following:

 Administrator-approved form templates may have privileges on corporate systems, including cross-domain access rights, and may contain code that runs under an administrator account. For this reason, it is important that all administrator-approved form templates be carefully reviewed prior to deployment by an administrator who is familiar with InfoPath Forms Services security.

 An administrator may grant certain farm-level privileges, such as allowing user form templates to use data connections that access data across domains. These settings should be carefully considered before changing the defaults, as they may have a broad impact on security across the entire farm.

 If you have enabled the Web service proxy, it should run under a unique application pool account. You should disable the Web service proxy if it is not used.

For more information on security requirements, see the Office SharePoint Server 2007 planning article [Chapter overview: Plan for and design security (Office SharePoint Server)](#DSDOC_3df68222_235b_45de_82fa_b89166c5c6).

## See Also

[Determine the impact of anonymously accessible form templates](#DSDOC_0ee46518_8f98_46ee_ae9a_ec2f8b46a8)

# Plan server-side data connections needed for form templates [Office SharePoint Server]

In this article:

 [Scenarios for the use of data connections](#DSDOC_section144e91039_e88f_4088_a97e_1d)

 [Database data connection](#DSDOC_section244e91039_e88f_4088_a97e_1d)

 [HTTP post data connection](#DSDOC_section344e91039_e88f_4088_a97e_1d)

 [SharePoint library submit data connection](#DSDOC_section444e91039_e88f_4088_a97e_1d)

 [SharePoint list data connection](#DSDOC_section544e91039_e88f_4088_a97e_1d)

 [Web service data connection](#DSDOC_section644e91039_e88f_4088_a97e_1d)

 [XML file data connection](#DSDOC_section744e91039_e88f_4088_a97e_1d)

A data connection is a dynamic link between a form template and a data source that stores or provides data for the form template. A form template must have one primary data connection, called the main data connection, and it can optionally have one or more secondary data connections. The main data connection defines the main data source of the form template, which is the XML schema that determines how data is stored. The one main data connection allowed on a form template is created automatically when you create the template. You can create as many secondary data connections as you like when you design a form template.

The Microsoft Office InfoPath 2007 designer supports a number of different data connections, which can be used both in the Office InfoPath 2007 program and in InfoPath Forms Services. Office InfoPath 2007 form template designers can develop a form template once and publish it both for the rich client and for the browser using InfoPath Forms Services. If data connections are used within a browser-enabled form template, the form template calls data connections that are resident in InfoPath Forms Services. This topic describes how server-side data connections function when a form template is deployed.

To plan what data connections you will need, gather the following information:

 What forms currently exist in your organization

 What application or systems you want to send the data to

## Scenarios for the use of data connections

The following are scenarios that show how data connections can be used in conjunction with InfoPath Forms Services.

### Scenario 1: Intranet: Authenticated user submitting data through e-mail

April logs onto her computer on the corporate intranet. She browses to her group's SharePoint site and opens an expense report form template from a document library. Because she does not have Office InfoPath 2007 installed, the form is instantiated in her browser. She fills out the form and clicks "Submit." The form is submitted by e-mail to her Accounts Payable department. The mail is delivered to A/P's e-mail box and the "Sender" field shows that the form was sent by "Office Forms Server." Because April is authenticated on the LAN by NTLM, the message's Subject line begins with "Submitted by April Meyer:" Meanwhile, April simply receives confirmation that her form has been submitted.

### Scenario 2: Extranet: Basic authentication submitting data through e-mail

The next time April has an expense report to submit, she is traveling to a conference. Using the free wireless Internet at her hotel, she logs into her company's extranet. She is prompted to enter her user name and password. Once she is authenticated, she accesses her expense report form in her browser. When she submits the form, she receives confirmation that the form was submitted. Behind the scenes, mail is sent to A/P as described in the first scenario. Because April is authenticated on the LAN using Basic authentication, the message once again has her name on the Subject line.

### Scenario 3: Intranet: HTTP post to application server

Tim works for the IT department at Linfield College. He sets up a BizTalk orchestration to handle admissions applications. He chooses to have the application forms, which are in XML format, submitted using BizTalk's ISAPI adapter. Melissa, who works at the Admissions desk at Linfield, enters the data from the applications that have been submitted by means of postal mail into the application form using InfoPath. When she submits the form, an HTTP post occurs, sending the data to the BizTalk queue.

InfoPath Forms Services uses the E-mail data connection to submit e-mail messages in MIME format on behalf of the user, using mail functionality provided with Microsoft Windows SharePoint Services 3.0. An e-mail message is sent using the credentials of the account under which the forms server is running. All configuration of this mail service is done by the server administrator. For information about configuring e-mail on Windows SharePoint Services 3.0, see the Windows SharePoint Services Administrator's Guide.

## Database data connection

The Database data connection looks up information in a database to populate form fields. You can use this connection to look up data in Microsoft SQL Server, or in any ODBC-compliant database. The Database data connection is query-only and cannot be used to submit data to a database. If you want to use a form to submit data, you should use the Web service data connection.

The Database data connection can authenticate requests to the database in different ways, depending on the security level of the form template that is being used to render the form. Administrator-approved form templates can be designed to have full trust, which means that any business logic or code that runs in the form is authenticated as the InfoPath Forms Services service account unless another authentication method is specified in the form template. Forms that are not running in full trust can only access a database that exists in the same domain as the server running InfoPath Forms Services, and database queries are authenticated either as the user or the account specified in the configuration database. In this case, if authentication fails, a prompt appears in which the user can specify a user name and password to connect to the database.

## HTTP post data connection

The HTTP post data connection enables an InfoPath form to post data to an application server using an HTTP post function. The HTTP post originates from the InfoPath Forms Services server.

If the HTTP post data connection is used in a form template running in full trust, then cross-domain HTTP posts can be made. If the form template does not have full trust, HTTP posts can only be made to servers in the same domain as the InfoPath Forms Services server. Before performing an HTTP post, InfoPath Forms Services calls an API method, passing the host name of the computer specified in the connection file to determine whether a connection can be made to that server within the current security context.

## SharePoint library submit data connection

The SharePoint library submit data connection enables forms to be published directly to a SharePoint document library. The connection uses the current user identity to access the SharePoint site.

Before submitting a form to a document library, InfoPath Forms Services calls an API method, passing the host name of the computer on which the data source resides to determine whether the form can connect to that server within the current security context.

## SharePoint list data connection

The SharePoint list data connection is a query-only connection used to populate InfoPath form fields from an existing SharePoint list.

When this data connection is used, the server calls an API method, passing the host name of the server to determine whether the form can connect to that server within the current security context.

## Web service data connection

The Web service data connection can submit data to a Web service and use the return data to update fields in the originating form. This connection collects form data as query parameters, wraps the data in a SOAP envelope, and submits it to a Web service. The connection then obtains the returned SOAP message containing return data or, in the case of failure, error-message data. A Web service connection can be created as a query connection or as a submit connection.

## XML file data connection

The XML file data connection connects to an XML file specified when the form template is designed, and it uses the data from the XML file to populate form fields. Form template designers can also choose to include the XML file in the form template itself, which reduces resource-management issues associated with connecting to an external resource.

# Plan deployment of form templates [Office SharePoint Server]

In this article:

 [Browser-compatible form templates](#DSDOC_section15f80ea0e_ed1e_49f3_80ea_3c)

 [Scenario: Insurance claims processing](#DSDOC_section25f80ea0e_ed1e_49f3_80ea_3c)

Microsoft Office SharePoint Server 2007 enables you to deploy rich forms on a server running InfoPath Forms Services that can be opened in Microsoft Office InfoPath 2007, Microsoft Office Outlook 2007, or in a Web browser. Browser-compatible form templates (.xsn files) created in the design mode of the InfoPath client can be published to a document library as browser-enabled form templates that run on InfoPath Forms Services.

You can also upload form templates to a document library that are not browser-compatible. These form templates can only be opened in Office InfoPath 2007.

|  |
| --- |
| Worksheet action |
| Use the [Inventory of existing forms](http://go.microsoft.com/fwlink/?LinkId=73266) worksheet (http://go.microsoft.com/fwlink/?LinkId=73266) to list your current form inventory. |

## Browser-compatible form templates

There are two categories of browser-compatible form templates: user form templates and administrator-approved form templates. Form templates that do not contain managed code, require full trust, or use a data connection managed by an administrator may be deployed by any user with the Add and customize pages permission. This permission is granted by default to the Design permission level and above on the site collection, but may be granted to any group or user by a site collection administrator.

note_ddNote:

For more information on customizing permissions for groups and users, see the Office SharePoint Server 2007 article, [Define custom permission levels [Office SharePoint Server]](#DSDOC_c5dd8b7e_202d_4d33_8535_5c03f88ea1). Form templates that contain managed code (business logic that incorporates extended functionality such as database queries or integration with third-party application servers), require full trust, or use a data connection managed by an administrator can only be deployed by an administrator.

important_ddImportant:

In addition to planning for the deployment of form templates, you should also plan a review and testing strategy for deployment of administrator-approved form templates. Because administrator-approved form templates contain code that could run under an administrative user account, it is important that they be subjected to thorough review and testing before they are deployed to a production environment. For more information, see [Plan deployment of administrator-approved form templates [Office SharePoint Server]](#DSDOC_7de89276_e882_4abc_9699_6f70dee463).

## Scenario: Insurance claims processing

This section describes a scenario for the deployment of browser-compatible form templates.

Humongous Insurance, a large insurance organization, introduces Office SharePoint Server 2007 into their environment to enable customers, insurance agents, and related businesses to use online forms for processing insurance claims. The organization has been using InfoPath 2003 internally but is now using InfoPath Forms Services to make forms available to their customers online.

Ted, the lead form template designer for Humongous Insurance, has just completed the design of a form template that allows customers to manage their policy online. Since the form contains business logic and data connections that are managed by the Office SharePoint Server 2007 administration group, he cannot publish the form directly to InfoPath Forms Services. Ted publishes the form template to a network location specified by the administrator, where it can be checked for compliance with design standards for form templates. He then notifies the administrator that the form template is ready for review.

Jorje, the InfoPath Forms Services administrator in charge of validation of form templates, sees the new form template in the network folder. The policy for new form templates at Humongous Insurance is to first validate the template by reviewing the code for compliance with security regulations and design standards, and then to upload the form template to a staging environment for further testing. Jorje reviews the code by opening the form template in the InfoPath program. Then he checks to make sure that the form template code calls the correct data connection, the form template is signed with a digital certificate, and trust settings are configured correctly. When he is satisfied that the form template is compliant with design standards, Jorje uploads the template to the staging environment, which closely matches the production Office SharePoint Server 2007 architecture.

Once the form template has been uploaded to the staging environment, Jorje logs in as a test user and opens the Web page where the form resides. Following his template review checklist, he fills out the form by using every available field and submits it, following this process several times and changing specific data, check box selections, and menu command selections each time. He also verifies that form data is being correctly submitted to the database and that business logic is functioning properly. Once the testing process is complete, Jorje signs off on the review checklist and uploads the form template to the production environment.

## [[10]](#footnote-11)#See Also

[Plan what form templates are needed [Office SharePoint Server]](#DSDOC_f669dd10_a737_49ba_b02e_c8b805f30c)

[Plan deployment of administrator-approved form templates [Office SharePoint Server]](#DSDOC_7de89276_e882_4abc_9699_6f70dee463)

# Plan deployment of administrator-approved form templates [Office SharePoint Server]

InfoPath Forms Services provides functionality that enables both administrators and users to deploy browser-compatible form templates. Browser-compatible form templates (.xsn files) created in the design mode of Microsoft Office InfoPath 2007 can be opened in a Web browser from servers running InfoPath Forms Services. InfoPath form templates (.xsn files) created in Office InfoPath 2007 design mode can be converted into browser-enabled form templates that run on Microsoft Office SharePoint Server 2007. An administrator must deploy form templates that contain business logic such as a compiled, managed code DLL (form code); require full trust; or use a data connection that is managed by an administrator.

If your organization will deploy form templates that require administrator approval, you must consider several factors in your planning:

 Map out a review and testing strategy for the deployment of administrator-approved form templates. It is important that form templates that could potentially have a performance impact on the server or that contain business logic are thoroughly reviewed and tested prior to deployment to production systems. We recommend that as part of your planning process, you develop a design standard for form templates that defines best practices, guidelines, and mandatory requirements to be followed by designers of form templates. We recommend that you develop a review checklist for form templates that makes it easy for administrators to verify that new form templates comply with the standards you have established. Also note that any good testing process includes testing in a staging environment to verify that the form template works as expected and to measure the performance impact under load.

 You should make sure that administrators are available to approve forms in a timely fashion. This will help to reduce bottlenecks in the publishing cycle. Administrators who review and approve form templates should be familiar with the form template design process and have a good understanding of the networking environments to which the form template will be available once it has been deployed.

 You should carefully consider the approval workflow. If your organization will use form templates that perform sensitive operations, such as submitting data to databases or Web services, then you should ensure that your approval process allows for adequate technical review.

 You should have an accurate understanding of the difference between administrator-approved form templates and user form templates, and which form templates require deployment by an administrator.

 You should make sure your server configuration strategy enables the features you need to support the deployment of administrator-approved form templates.

 You should ensure that you understand how network and application security affect your organization's forms. For example, if a form will access databases in a different domain than the Office SharePoint Server 2007 server on which the form template resides, such a form template requires full domain trust. Therefore, it must be carefully reviewed by an administrator prior to deployment to confirm that the form template's code does not compromise your organization's security policies. Likewise, you should confirm that form template authentication and authorization have been properly configured.

 Determine whether new form templates that require administrator approval need to be created on a regular basis, and if so, ensure that the necessary procedures, personnel, and applications are in place to support the approval process.

|  |
| --- |
| Worksheet action |
| Use the [Plan deployment of administrator-approved form templates](http://go.microsoft.com/fwlink/?LinkId=73267) (http://go.microsoft.com/fwlink/?LinkId=73267) worksheet to record the administrator-approved form templates you plan to deploy. |

## See Also

[Plan what form templates are needed [Office SharePoint Server]](#DSDOC_f669dd10_a737_49ba_b02e_c8b805f30c)

[Plan deployment of form templates [Office SharePoint Server]](#DSDOC_5f80ea0e_ed1e_49f3_80ea_3c7c4441ac)

# Determine the impact of anonymously accessible form templates

In this article:

 [Identify the need for anonymously accessible form templates](#DSDOC_section10ee46518_8f98_46ee_ae9a_ec)

 [Security and usage considerations for anonymously accessible form templates](#DSDOC_section20ee46518_8f98_46ee_ae9a_ec)

 [Bandwidth and capacity considerations for anonymously accessible form templates](#DSDOC_section30ee46518_8f98_46ee_ae9a_ec)

If your organization plans to deploy form templates that can be accessed by unauthenticated users, you need to consider a variety of factors in your planning. Without adequate planning, form templates that can be submitted without user authentication can present problems with security, improper usage, bandwidth, and database capacity. Before making form templates anonymously accessible either on a private network or on the Internet, carefully read this article and make sure that your strategy takes these considerations into account.

## Identify the need for anonymously accessible form templates

Anonymously accessible form templates provide your end users simple and unobstructed access. Two likely scenarios for anonymously accessible form templates are over the Internet and within the corporate network.

### Internet scenario

Anonymously accessible form templates are a reasonable choice on the Internet when there are no security concerns about the functionality or data associated with the form template. Providing anonymously accessible form templates on the Internet can reduce administrative effort because user authentication does not need to be managed or maintained.

### Corporate scenario

The reasons for using anonymously accessible form templates within a corporation are similar to those for the Internet. The difference is that users are within a closed network, an Intranet, or are authenticating through a Virtual Private Network, a Remote Access Server, an extranet, Terminal Services or a password-protected Web site. Unlike the Internet scenario, users would typically be known on the network. Providing anonymously accessible form templates can enhance user experience in situations where unfettered and anonymous access is desirable. For example, a corporate survey of employees might produce more candid and useful responses if they are anonymous.

Another advantage to using anonymously accessible form templates is that performance can be improved when you implement anonymous scenarios. Performance advantages are realized because postbacks to request access control list (ACL) verifications are eliminated.

## Security and usage considerations for anonymously accessible form templates

Before making a form template anonymously accessible, you must consider the possible consequences to security and the implications of attempts to improperly use the form template.

 You should ensure that form templates cannot be accessed by scripts or other automated or non-human processes. One way to achieve this is to force users submitting a form template to enter an identification code such as a short alphanumeric string displayed in an image, which cannot be "read" by a script or automated process.

 Form templates that contain sensitive information such as authentication information, server or database names, or proprietary code should not be exposed to anonymous users.

 Form templates that contain code or functionality that can invoke processes on a server should be carefully evaluated and tested to ensure that security cannot be compromised by making the form template accessible to anonymous users.

 In order to prevent users from submitting multiple copies of a form, you might consider including code that tracks the IP address of each user who submits a form and prevents duplicate submissions from the same IP address.

## Bandwidth and capacity considerations for anonymously accessible form templates

Once you make a form template anonymously accessible to the Internet, you no longer have control over how many times that form is submitted. Therefore, before publishing an anonymously accessible form template to the Internet, carefully consider your expectations regarding the following factors:

 How many users will submit the form within a given time period

 How much data must be transferred and stored

 How much server processor time, memory and throughput will be utilized each time the form is submitted

You can then estimate how much bandwidth, server processor time and database capacity is required in order to support the form template. Using the IIS administration tool, you can throttle bandwidth and the number of concurrent connections for a Web site if you want to control usage.

## [[11]](#footnote-12)#See Also

[Plan what form templates are needed [Office SharePoint Server]](#DSDOC_f669dd10_a737_49ba_b02e_c8b805f30c)

# Plan for naming form templates [Office SharePoint Server]

You should establish a naming convention for form templates that avoids confusion about their origin and usage. Of course, you can name form templates any way you like, but it's useful in the long run to follow a logical naming convention. General best practices include:

 Make sure that form template designers are aware of the naming conventions you establish, and that they understand how to check for duplicate template names before saving a new template. Conversely, as the administrator, you can change template names to conform to naming conventions before uploading them to the system.

 Establish a naming convention that reflects relevant information about the templates.

 Avoid using dates in form template names, as date information may be confusing if a form template is upgraded at a later time.

 Make sure that you distribute form template naming conventions to InfoPath designers and administrators.

 Keep in mind that form templates may be reused throughout your enterprise, and that developers may use file names to organize form templates.

## See Also

[Plan version control for form templates [Office SharePoint Server]](#DSDOC_8d734e5b_e0a4_497b_9524_ff9153f15b)

[Plan custom form templates (Office SharePoint Server)](#DSDOC_3ce912a1_64fe_4a52_8b06_10e7e01381)

# Plan for upgrading form templates [Office SharePoint Server]

You can upgrade administrator-deployed form templates in InfoPath Forms Services when you upload a new version of an existing form template. The upgrade process allows you to configure how the transition between the existing version and the upgraded version will take place.

There are three ways to upgrade a form template. Before you upgrade a form template, evaluate the circumstances and choose the most appropriate type of upgrade.

 Hard upgrade   If you want to remove the existing form template when the upgrade takes place, you can use a hard upgrade. Existing form-filling sessions are terminated and all user data is lost. The user must begin a new form-filling session with the upgraded form template to continue. This upgrade method should only be used when a serious problem with the form template has been identified and you need to remove it from the system immediately.

 Quiesce and upgrade   If you need to ensure that a form template will no longer be available for use after a given time and you want to allow existing form-filling sessions to complete, you can quiesce the existing form template and then upgrade to the new version. This upgrade method is useful when a form template contains content or code that will become obsolete or outdated at a given time.

 Gradual upgrade   If you want to allow the existing form template to remain available for an indefinite period, you can upload the new version as a new form template and remove the old version when it is no longer in use. This is the method that should be employed for most normal upgrades.

note_ddNote:

Before you upgrade a form template, make sure that you have adequately reviewed the new template and checked for problems that may affect security and proper operation of the form.

# Plan for retiring form templates [Office SharePoint Server]

InfoPath Forms Services administrators can retire form templates when they become obsolete. For example, you may want to retire a survey form template when the survey has been completed.

When a form template is no longer in use, you should generally retire the form template rather than deleting it. This preserves a record of form templates that have been used in your enterprise, and enables them to be reused later.

In the interest of keeping document libraries current and uncluttered, make sure that form templates that are no longer used are retired, and that you have a policy in place for auditing and upgrading existing form templates.

When you deploy a form template, consider the following:

 Will this form template eventually need to be retired, or will it need to be upgraded?

 How will you track the life cycle of form templates to be retired?

If you plan to retire a form template that is still in use, you should plan to use one of the following methods:

 Perform a gradual upgrade. In a gradual upgrade, you deploy the latest version of a form template alongside the current version and redirect users to the latest version. Once the older version of the form template is no longer being accessed, you can retire it safely.

 Quiesce the form template before upgrading. This prevents current sessions from being terminated, which can result in the loss of data and an abrupt interruption of user form-filling experiences.

For more information on how to quiesce form templates, see the "Quiesce form templates" section in Manage form templates.

## See Also

[Plan for upgrading form templates [Office SharePoint Server]](#DSDOC_2785361f_decf_4308_a217_00a32949ae)

# Plan version control for form templates [Office SharePoint Server]

In this article:

 [Document Retention](#DSDOC_section18d734e5b_e0a4_497b_9524_ff)

 [Capacity Planning](#DSDOC_section28d734e5b_e0a4_497b_9524_ff)

You can configure InfoPath Forms Services to enable version control for form templates at the document-library level. Enabling version control causes the library to create a new version of the form template every time the template is edited and saved, preserving previous versions as defined by the administrator. If form templates will be regularly edited in a given document library, you should configure the library for version control. This prevents existing form templates from being overwritten when edits are made, and it provides a mechanism for rolling back to a prior version.

Note that version control does not apply to form template upgrades. When you upgrade a form template by uploading a new version of an existing form template, the prior version of the form template is no longer available, and there is no mechanism provided for rolling back from an upgrade.

note_ddNote:

You can only configure version control for a given document library. You cannot configure "global" version control for sites, site collections, or farms.

## Document Retention

If version control is enabled for a document library, the library owner has the option of allowing unlimited previous versions to be retained. The library owner can also elect to only allow a certain number of versions to be retained, but there is no provision for automated deletion of documents past a certain age, also known as tombstoning. This means that documents could potentially be retained for years unless they are manually deleted. You may want to consider the following factors:

 Your organization's policy may require that documents past a certain age be destroyed. You should plan how to conform to such policies, and how to monitor the age of documents on the farm.

 If new versions of documents are uploaded without version control, there is a risk that obsolete documents may be accessed by users. You should ensure that document libraries are configured to prevent obsolete documents from remaining available on the system.

## Capacity Planning

The farm administrator does not have any direct control over whether document library owners enable version control for their libraries. Therefore, you should consider the following when planning farm capacity:

 You should plan to use reporting to run regular reports on the size of document libraries in the farm.

 You should ensure that sufficient database capacity exists to provide overhead for a potentially large number of documents.

## [[12]](#footnote-13)#See Also

[Plan deployment of form templates [Office SharePoint Server]](#DSDOC_5f80ea0e_ed1e_49f3_80ea_3c7c4441ac)

# Plan for mobile device access to form templates [Office SharePoint Server]

InfoPath Forms Services provides access to browser-enabled forms from mobile devices such as handheld PDAs that support HTML, CHTML, or XHTML. Because each mobile device renders Web pages differently, the behavior of forms will vary depending on the device used.

note_ddNote:

InfoPath Forms Services does not support Wireless Access Protocol (WAP) browsers.

Because of the lack of standardization across mobile devices, the user experience may be significantly different depending on what type of device is being used. Different mobile devices will automatically break up the user interface into different views, in a device-specific way. Possible examples may include:

 Automatic pagination

 Automatic switching between list and detail views for lists

 Automatic switching to a separate edit view for each editable field

Furthermore, because mobile devices may or may not support script execution, and due to low memory and bandwidth capabilities for many of those devices, InfoPath Forms Services cannot use a client-side architecture (CSA) for mobile devices as it does for standard Web browsers. Instead, InfoPath Forms Services uses ASP.NET mobile controls. This means that a mobile device browser will not:

 Provide client-side actions using script. All such actions will post back to the server.

 Use out-of-band postback as is used by a standard Web browser. Instead, the mobile device browser will always perform a full-page postback.

Mobile device browsers will therefore need to post back much more frequently than a desktop browser accessing InfoPath Forms Services. You should carefully plan how to support your mobile infrastructure in order to maximize performance.

When an HTTP request is received by InfoPath Forms Services, the server detects whether the request is coming from a mobile device and redirects the request to the appropriate page. ASP.NET mobile controls also can detect the device making a connection and auto-change the protocol used for the connection. For more information about ASP.NET mobile controls, see [Mobile Controls](http://go.microsoft.com/fwlink/?LinkID=72731) (http://go.microsoft.com/fwlink/?LinkID=72731) on the Microsoft Web site.

When planning for mobile device access, you need to consider the following:

 How many mobile devices do you expect to be accessing your documents and form templates?

 How will these devices be connected to the network (Wireless access points throughout the organization, across the Internet)?

 Will there be a standard for the type of mobile device accessing the server? If so, it would be easier for form template designers to exercise control over the way mobile forms will be displayed.

## See Also

[Plan deployment of form templates [Office SharePoint Server]](#DSDOC_5f80ea0e_ed1e_49f3_80ea_3c7c4441ac)

# Plan workflow for form templates

Workflows implement business processes on documents, Web pages, forms, and list items in Microsoft Office SharePoint Server 2007. They can be associated with libraries, lists, or content types. For more information on workflows, see [Chapter overview: Plan workflows](#DSDOC_adc8aefd_8c4e_4824_8676_c61c10d180).

There are three contexts for workflow planning in relation to forms:

 [Custom workflow form templates](#DSDOC_section176b6409f_d38b_438c_af0a_d8) — The form template is included in a custom workflow package to gather information as a part of the workflow.

 [Workflows for form template approval](#DSDOC_section276b6409f_d38b_438c_af0a_d8) — The workflow is used to approve a form template, as it would be to approve any other type of page or document in a library.

 [Workflows launched from a form](#DSDOC_section376b6409f_d38b_438c_af0a_d8) — The workflow is bound to the Submit or Save button on the form template. When the user clicks the button in a form-filling session, the workflow is launched.

## Custom workflow form templates

You can upload a custom workflow package to Office SharePoint Server 2007 that includes workflows and form templates. When a workflow uses a form template as an interface to gather data during the workflow process, these form templates are integrated into the application experience by means of an InfoPath Forms Services Web Part.

These server-side workflow form templates are specific to the workflow and cannot be activated to a site collection or added to a document library. These form templates are stored in the farm forms library and must be uploaded by an administrator. Office SharePoint Server 2007 includes several form templates that are specifically for use in default workflows. These form templates cannot be used outside of these workflows.

## Workflows for form template approval

You can use a workflow to review or approve a form template in the same way you can use workflows to route any document or page for review. For more information, see [Plan workflows for document management](#DSDOC_34bc3a16_91f6_4c62_ae09_821cb94155).

## Workflows launched from a form

InfoPath Forms Services can be used to launch workflows using the submit button in a form. For example, you can use browser-enabled form templates in a workflow that routes documents from person to person to complete document management tasks, such as reviewing documents, approving their publication, or managing their disposition.

Additionally, administrator-approved form templates can be designed to initiate a workflow. For example, when a form template used for collecting customer information is submitted, it could start a workflow to notify the appropriate personnel and require action within a given time frame.

If you will deploy form templates that trigger workflows, keep the following things in mind:

 Workflows need to be enabled for the site collections to which the form template will be deployed. If workflows are not enabled for a site collection, a workflow-enabled form template will generate errors on the server when it is submitted.

 You should ensure that the workflow exists and is enabled in the production environment. A form template designer will typically be designing a form template against a development environment that may have workflows and other custom features that have not been deployed to the production system.

 Ensure that the workflow is configured to work the same way in the production environment as it does in the development environment.

For more information about launching a workflow from a form, see How To: Add SharePoint Workflow Support to an InfoPath Form.

## [[13]](#footnote-14)#See Also

[Chapter overview: Plan workflows](#DSDOC_adc8aefd_8c4e_4824_8676_c61c10d180)

# VI Plan for business intelligence

In this chapter:

 [Chapter overview: Plan for business intelligence](#DSDOC_84db8a3d_9ba4_482d_9ee6_000ac324e5)

 [Determine business data and business intelligence needs](#DSDOC_c1725ade_b558_47d9_9749_6ce68b8df0)

 [Determine scope of business intelligence analysis](#DSDOC_361ece77_817f_482d_9631_1d9fe71d9e)

 [Plan data connection management](#DSDOC_b390b289_f7ac_457d_bbaa_f958b13730)

 [Plan key performance indicators](#DSDOC_d8f9b41e_e324_490d_bf85_1370c8b63b)

 [Plan reports](#DSDOC_fbe7fe46_8d60_4de2_a699_7921c13dbd)

 [Plan dashboards and filters](#DSDOC_5fe87ec1_431e_4b7f_ae33_1e2edd8613)

 [Plan Excel Services security](#DSDOC_a49883a7_de84_4a66_8fa0_7c7d125f23)

 [Determine resource requirements to support Excel Services](#DSDOC_fb6928ce_49f8_492a_abff_5bd00ed588)

 [Plan rendering Excel KPI data](#DSDOC_ff3ee313_7293_4611_b9ab_175d539878)

 [Plan Excel reports against OLAP cubes](#DSDOC_bbaa06e5_a953_4637_9114_bda62aba0e)

 [Plan access to Excel spreadsheets](#DSDOC_93f576a4_e549_4675_b083_7fe4f145ac)

 [Plan for business data connections with the Business Data Catalog](#DSDOC_c803c1fa_cb0f_4a26_b439_de7ff4195e)

 [Plan for business data profiles](#DSDOC_560cb26b_f530_464e_ab9f_f506df8d8d)

 [Plan business data lists](#DSDOC_10008f02_d602_4749_b89a_15f7406aea)

 [Plan business data Web Parts](#DSDOC_165f1afe_11e5_4c45_8f93_bf16e18338)

 [Plan business data actions](#DSDOC_60b8a5be_c54e_488c_90b0_80f4aeba40)

 [Plan for business data search](#DSDOC_2b7121fc_a1f2_469d_ac1c_7b12283897)

# Chapter overview: Plan for business intelligence

Business intelligence enables you to store data that represents your organization's key business processes, to organize that data in a useful manner, and to present that data as meaningful information. Knowledge workers can then act on that information to increase productivity and to provide feedback that improves underlying business processes.

Business intelligence planning is a key part of any deployment of Microsoft Office SharePoint Server. You start by identifying the business needs of your organization. Then, you identify the features of Office SharePoint Server that can help you collect, present, and act on data in your organization.

Plan for business intelligence and business data by using the following steps:

1. Plan for business intelligence needs   Consider the business processes and business data applications commonly used by your organization, plan the scenarios in which you work with business data, and determine the scope of the business intelligence analysis that your organization is considering. Use the following articles to help plan for business intelligence needs:

 [Determine business data and business intelligence needs](#DSDOC_c1725ade_b558_47d9_9749_6ce68b8df0) provides a discussion of using business intelligence and business data presentation to increase the effectiveness of data analysis and business processes for the common business scenarios of your organization.

 [Determine scope of business intelligence analysis](#DSDOC_361ece77_817f_482d_9631_1d9fe71d9e) provides a discussion of the appropriate depth of planning for analysis and use of business data.

2. Plan for business intelligence   Plan data sources for the core business intelligence functionality of Microsoft Office SharePoint Server 2007, and then plan the analysis tools used in SharePoint sites based on those data sources. Use the following articles to help plan for business intelligence:

 [Plan data connection management](#DSDOC_b390b289_f7ac_457d_bbaa_f958b13730) provides a discussion of connecting to data in Microsoft SQL Server 2005 Analysis Services cubes and other databases.

 [Plan key performance indicators](#DSDOC_d8f9b41e_e324_490d_bf85_1370c8b63b) provides a discussion of calculating easy-to-use scorecards from ranges of data in data connection libraries, Excel Calculation Services worksheets, business data lists, and SharePoint lists.

 [Plan reports](#DSDOC_fbe7fe46_8d60_4de2_a699_7921c13dbd) provides a discussion of presenting key performance indicators (KPIs) and business data Web Parts in Report Center pages and other sites to improve analysis of business data and key business processes.

 [Plan dashboards and filters](#DSDOC_5fe87ec1_431e_4b7f_ae33_1e2edd8613) provides a discussion of displaying multiple related reports and KPIs, and connecting the Web Parts for business data so that you can filter data based on key business properties for all reports on the dashboard page.

3. Plan for Excel Calculation Services   Plan to use Excel Calculation Services to analyze business data and increase business intelligence. Use the following articles to plan for Excel Calculation Services:

 [Plan Excel Services security](#DSDOC_a49883a7_de84_4a66_8fa0_7c7d125f23) provides a discussion of security considerations to use with Excel Calculation Services.

 [Determine resource requirements to support Excel Services](#DSDOC_fb6928ce_49f8_492a_abff_5bd00ed588) provides a discussion of the factors that can affect the performance and availability of Excel Calculation Services.

 [Plan rendering Excel KPI data](#DSDOC_ff3ee313_7293_4611_b9ab_175d539878) provides a discussion of how data in spreadsheets can be rendered in KPI List Web Parts or aggregated into a dashboard.

 [Plan Excel reports against OLAP cubes](#DSDOC_bbaa06e5_a953_4637_9114_bda62aba0e) provides a discussion of online analytical processing (OLAP) functions and formulas that can be used to create customizable reports.

 [Plan access to Excel spreadsheets](#DSDOC_93f576a4_e549_4675_b083_7fe4f145ac) provides a discussion of spreadsheet management and controlling access to workbooks.

4. Plan for business data presentation   Plan to use data from line-of-business applications to analyze and act on data in your SharePoint sites. Use the following articles to plan for business data presentation:

 [Plan for business data connections with the Business Data Catalog](#DSDOC_c803c1fa_cb0f_4a26_b439_de7ff4195e) provides a discussion of registering applications in the Business Data Catalog.

 [Plan for business data profiles](#DSDOC_560cb26b_f530_464e_ab9f_f506df8d8d) provides a discussion of which business data types and properties to include when registering applications in the Business Data Catalog.

 [Plan business data lists](#DSDOC_10008f02_d602_4749_b89a_15f7406aea) provides a discussion of adding columns to SharePoint lists that contain data from applications registered in the Business Data Catalog.

 [Plan business data Web Parts](#DSDOC_165f1afe_11e5_4c45_8f93_bf16e18338) provides a discussion of creating Web Parts based on the data in business data lists, the many types of business data Web Parts, and the sites that can benefit from using these Web Parts.

 [Plan business data actions](#DSDOC_60b8a5be_c54e_488c_90b0_80f4aeba40) provides a discussion of creating actions based on properties of business data, and displaying those actions in Web Parts that can be connected to other business data Web Parts and filter Web Parts.

5. Plan for business data search   Plan to include data from business applications in search queries from your SharePoint sites. Use the following article to plan for business data search:

 [Plan for business data search](#DSDOC_2b7121fc_a1f2_469d_ac1c_7b12283897) provides a discussion of adding business data content sources, mapping crawled business data properties to managed properties used by search queries, and modifying the search experience so that business data is easier to find and business data search results are more relevant.

# Determine business data and business intelligence needs

In this article:

 [About business intelligence](#DSDOC_section1c1725ade_b558_47d9_9749_6c)

 [Plan Office SharePoint Server 2007 features for business intelligence](#DSDOC_section2c1725ade_b558_47d9_9749_6c)

 [Plan business data scenarios](#DSDOC_section3c1725ade_b558_47d9_9749_6c)

 [Determine business intelligence needs for your organization](#DSDOC_section4c1725ade_b558_47d9_9749_6c)

 [Worksheets](#DSDOC_section5c1725ade_b558_47d9_9749_6c)

Microsoft Office SharePoint Server 2007 includes business intelligence capabilities that can help you preserve data integrity throughout your organization while enabling powerful search, data integration, data analysis, data rendering, and data sharing scenarios.

The business intelligence functionality in Office SharePoint Server 2007 enables centralized management and control of shared resources that can include reports, forms, documents, spreadsheets, and data connections.

As part of planning for your initial deployment of Office SharePoint Server 2007, you should understand business intelligence and how it relates to the processes and conditions of your organization. This will enable you to identify specific business intelligence needs in your organization, and to use those needs to identify which features of Office SharePoint Server 2007 to implement to improve your business processes over time.

## About business intelligence

Business intelligence, sometimes known as business performance management, is a set of technologies used to increase the understanding of business processes and their associated data. Good use of business intelligence helps you organize data about your organization so that it is useful, actionable, and capable of transforming your underlining business processes. These goals are achieved through the following processes:

 Gather data   The first step in building business intelligence is to create and store data that accurately represents what is happening in your organization. Databases are only useful when the data they are tracking is representative of business processes and business conditions. It can be difficult to determine what is missing from data sources, so that additional data can be gathered to improve business processes.

 Turn data into useful information   Data is typically represented as sets of fields that have corresponding values. By itself, data is neutral and not inherently useful. When you use tools and business processes to make data useful, you create information. One key way to create information is to create a view into data that contains a subset of data that is useful for one or more groups of users in your organization.

 Use information to impart knowledge   Knowledge is created when you provide actionable information to the people who can use that information. Having a list of data that might be interesting to a particular group of people is better than having raw data, but it does not actually enable you to do anything. By personalizing information, targeting audiences and groups, and providing a way for people to analyze and interact with data, you create actionable information that is the basis for knowledge in your organization.

 Turn knowledge into action   As you build a base of knowledge in your organization, knowledge workers act more efficiently in pursuing key business goals and managers can identify opportunities for improvement and make decisions based on that knowledge to improve business processes.

Business intelligence provides an effective set of solutions that correspond to each of these steps in an integrated process that enables you to continually improve business processes. Starting with data, you create information that can help you achieve an understanding of the processes. Then, you act on that information to build a base of knowledge and update information, while also changing business processes. These changes produce new data and information that you can use to deepen your knowledge and continue to change your business processes in the future.

Business intelligence includes several strategies and techniques that are designed to improve business processes:

 Data integration   This includes data storage and warehousing, data mining, and data consolidation. Data integration involves collecting information from various structured and unstructured sources, and consolidating it into a single data source that can be used to create meaningful information by using the business intelligence tools of an organization. Information presentation enables users to query data sources and find usable information that can be analyzed against business goals, while ensuring security and data integrity in a collaborative workspace.

 Information presentation   This includes information discovery, visibility, analysis, and collaboration.

 Reporting   This includes the use of scorecards and other tools used to compare information across multiple business processes. Reporting tools, such as scorecards, enable knowledge workers to evaluate information and act on it, thereby creating a base of knowledge for your organization.

Each of these strategies corresponds to an essential step of business performance. Using all of these techniques together creates positive feedback loops of increasing knowledge that can be used to improve your organization and its business processes and associated data over time.

## Plan Office SharePoint Server 2007 features for business intelligence

Office SharePoint Server 2007 provides many tools that enable you to display information and build knowledge in your organization. You can use the personalization and targeting features of Office SharePoint Server 2007 to increase the usability of your data and enable knowledge workers in your organization to act on the information built on that data. You can aggregate content across many sources and find it more easily by using search features. Office SharePoint Server 2007 supplements these features with an important set of features for business intelligence.

These features include:

 Data integration features, such as data connection libraries, the Business Data Catalog, business data profiles, and business data lists.

 Information presentation and reporting features, such as reports, key performance indicators (KPIs), and dashboards.

### Plan data integration features of Office SharePoint Server 2007

Data warehousing and data mining are techniques for gathering useful information from your existing data sources. Business intelligence solutions frequently use online analytical processing (OLAP) tools to provide meaningful data and expose underlying patterns that might not be otherwise apparent. Office SharePoint Server 2007 uses Microsoft SQL Server 2005 Analysis Services. OLAP and SQL Server 2005 Analysis Services are preferred for large data sources that have relatively stable and unchanged data. That data is then used to create information in processes that change more quickly.

Office SharePoint Server 2007 can also use data from other business applications, known as line-of-business applications. Although not part of the core business intelligence functionality, the data from these applications can be displayed and analyzed in similar ways as the data in data connection libraries, providing an integrated view of all business data in the organization. Line-of-business applications manage data about people and business operations and are widely used within large organizations and enterprises. Examples of line-of-business applications include:

 SAP Business Information Warehouse or mySAP ERP

 Siebel eBusiness Applications

 Attunity Legacy Data Access Solutions

 Microsoft BizTalk Server

These applications are registered in the Business Data Catalog. Data from the Business Data Catalog is used by Office SharePoint Server 2007 to create additional kinds of information for the knowledge workers in your organization. That information can be easily integrated with the other features of Office SharePoint Server 2007 site collections.

Data consolidation is the process of grouping data in meaningful ways so that it is useful. The key data consolidation features of Office SharePoint Server 2007 are data connection libraries, business data profiles, and business data lists.

A data connection library is a library of connections to data sources that can be analyzed by using SQL Server 2005 Analysis Services. This allows the data to be analyzed and displayed by using the business intelligence features of Office SharePoint Server 2007. Data connection libraries include links to data sources, such as SQL Server 2005 Analysis Services cubes, that are relevant for a particular site or site collection.

Business data profiles are lists of properties associated with business data types from line-of-business applications registered in the Business Data Catalog. Each business data profile is a meaningful consolidation of relevant data for key business processes to create usable information for users in your organization. For example, you can have a business data profile for customers that tracks telephone numbers, addresses, e-mail addresses, and locations for each customer.

Business data lists are SharePoint lists that gather one or more columns directly from the data of one or more business applications. Each list has a collection of items with several columns that represent properties for each item. Lists can contain information similar to the information in business data profiles. You can also create lists for KPIs, another important business intelligence feature.

### Plan information presentation and reporting features of Office SharePoint Server 2007

After data is consolidated in a meaningful form, additional business intelligence tools enable knowledge workers to query and analyze the resulting information and act on it as quickly and effectively as possible.

You can query business data by using the business data features of Office SharePoint Server 2007 search. You register applications in the Business Data Catalog, and then you crawl content sources for those applications. The subset of data selected by administrators for the Business Data Catalog is then available for administrators for search to map to managed properties that affect the results of search queries.

Users in your organization can search for business data and find meaningful and useful results. For example, the administrator of the Business Data Catalog registers a sales application and selects business data types for customers, product lines, and sales associates, and also selects the properties for the business data profiles associated with those business data types. The Shared Services Provider (SSP) administrator who is responsible for search then creates a content source for the application. After crawling the content source, the SSP administrator for search maps selected crawled properties to managed properties used by the system during search queries. Users who search for a customer based on the customer name, location, or address are more likely to find the customer if the customer name, location, and address are managed properties. These managed properties can also be used to create search scopes.

You can analyze business data by presenting it within sites in your site collection. Business data stored as information in lists or business data profiles in the Business Data Catalog can be used in several technologies designed to enable analysis of information so that knowledge workers can act on information and create knowledge.

For example, you can create KPIs, which calculate a value from a range of data, and compare that data against a target to indicate the performance of key business processes. By analyzing a list of related KPIs, you can see how different business processes interact.

You can also create reports that take KPIs or business data lists by using properties in the Business Data Catalog and display that information with related SharePoint information, such as documents or workspaces.

Dashboards display several business data Web Parts for different data sources and business processes in one place. The Web Parts on dashboards are connected to filters so that the dashboard owner can limit the scope of the data presented across all Web Parts. Users can apply one or more filters to analyze the data in a way that is more relevant to each person. Within dashboards, users in your organization can also use Excel Calculation Services and Excel Web Access Web Parts to look at data sources and filter them based on one or more columns in each workbook.

Each of these analysis tools creates more actionable information. To complete the business intelligence cycle, there are several methods provided by Office SharePoint Server 2007 for acting on information immediately after analyzing data. If you are using Microsoft Office Excel 2007 and have the appropriate permissions, you can start an Office Excel 2007 client to directly edit the underlying workbook. You can add business data actions that appear in search results, the business data profile, reports, and dashboards that directly relate to the information in each of these presentation options. You can edit business data profiles as new information about your business is collected. Knowledge workers in your organization can act on information as they see it, immediately providing feedback that improves productivity. They can also detect underlying patterns to business processes, which can be used to improve your processes, data collection, and information presentation.

## Plan business data scenarios

Business intelligence features are deployed as part of larger business data scenarios. These scenarios can be defined in several ways, including:

 By the purpose of the organization and site collection that is using business data.

 By specific business processes within a larger scenario for your organization.

 By information technology infrastructure, deployment, and security concerns.

### Plan purpose-based scenarios

Examples of scenarios based on the purpose of an organization and site collection include:

 Call center   Find open customer service requests (CSRs) in the CSR database from the Search Center site, update CSRs by using InfoPath Forms Services forms tied to business actions, and view performance of front-line technicians by using KPIs.

 Employee records and personalization   Target data to employees in portal sites based on their Siebel or SAP properties, and allow employees to update their information by using Web-enabled forms.

 Customer facing   Use Web-enabled InfoPath Forms Services forms to provide a way for customers to personalize account information, update insurance claims information, or submit government forms.

These types of scenarios are useful to consider when you are planning the business intelligence needs of your site structure.

Business intelligence needs can be much more diverse than these few examples, and every organization is unique. For your organization, it is a good idea to state the broad scenario that is relevant before you begin specific planning to deploy a solution for that scenario. For each site collection in your organization, identify those that are using business applications, and identify which applications are central to the purpose of each site collection. Think of the features you will use in broad terms.

### Plan process-based scenarios

Examples of scenarios based on more focused business processes within a larger business data and business intelligence framework include:

 Prediction analysis   Show additional items that might be of interest to people buying a displayed item. For example, display additional products created by the same person or organization.

 Cross selling   Offer discounted services and products in conjunction with a purchase. For example, offer an item for free with the purchase of two similar items.

 Data mining   Find and use hidden data. Build behavioral models based on tracking. For example, find card-key access by time of day, by date, by building, or by event to determine traffic patterns.

 Sales forecasting   Review current account status or customer characteristics and make adjustments based on live data.

 Purchase order approval   Check current budget status and other data before approving a workflow-generated purchase order.

You can identify similar scenarios to represent different sets of business processes within your organization. Then, you can plan for the specific features you need to address each set of business processes.

You should also consider the planning for infrastructure, security, and other information technology considerations. The business scenarios and business process planning within each scenario that you identify are affected by the environment in which you deploy, and similar overall scenarios that have different deployment scenarios will be planned differently.

These types of scenarios are useful to consider when you are focusing on business intelligence planning and want to determine the appropriate scope of your business intelligence solution.

### Plan IT-based scenarios

Examples of scenarios based on deployment and security considerations include:

 Human resources site collection   One source, one consumer. The application administrator uses business data features to construct a site collection that displays human resources data from a data warehouse. The data on the site collection is sensitive, and is displayed only on that site collection.

 Expense reports across sites and site collections   One source, many consumers. Team site owners want to display a list of pending expense reports for their teams. Individuals want a My Expense Reports Web Part on their personal site home pages. Expense data changes frequently, so the data is collected from SAP by registering the application in the Business Data Catalog and then by using that data in multiple sites.

 Product issues databases   Many sources, many consumers. Team site owners want to include live data from a product issues database application on their team sites. There are many databases for different products and teams.

 Product issues data is provided to an external partner   A business partner uses an extranet that has access to a subset of relevant product issues.

These types of scenarios are useful to consider when you are planning the architecture and deployment of your business intelligence solution.

Whatever your deployment considerations, the people on your planning teams should consider each business scenario and feature in the context of the supporting infrastructure of your organization.

## Determine business intelligence needs for your organization

One or more of the scenarios described above, or similar scenarios, can exist within any organization that is deploying Office SharePoint Server 2007. When you plan for business data and business intelligence, consider the scenarios that apply to your organization, and then select the features of Office SharePoint Server 2007 to use that correspond to those scenarios.

Scenarios will revolve around distinct business processes, each of which is built on one or more data sources. These sources are used by features that present that data as information to knowledge workers, who then act on that information. Your business intelligence needs for each business process will correspond to the essential steps of business intelligence: The essential steps of business intelligence are:

1. Connect to business data sources and collect data.

2. Present business data as information.

3. Query and analyze data.

4. Act on data.

The corresponding feature planning steps are:

1. Plan line-of-business applications and the Business Data Catalog and SQL Server databases.

2. Plan business data profiles and business data lists.

3. Plan business data search, KPIs, and reports.

4. Plan dashboards, the Report Center site, and business data actions.

If you consider these points when planning the initial deployment of business intelligence features of Office SharePoint Server 2007, you are much more likely to create a business intelligence solution that accomplishes your goals.

|  |
| --- |
| Worksheet action |
| Use the [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) to record your decisions. For more information, see the worksheet actions described in the planning topics for particular business data and business intelligence features. |

## Worksheets

Use the following worksheets to determine business data and business intelligence needs:

 [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409)

 [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409)

# Determine scope of business intelligence analysis

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [About business intelligence scope planning](#DSDOC_section1361ece77_817f_482d_9631_1d)

 [Business intelligence principles](#DSDOC_section2361ece77_817f_482d_9631_1d)

 [Business intelligence examples](#DSDOC_section3361ece77_817f_482d_9631_1d)

## About business intelligence scope planning

Business intelligence is the process of gathering, storing, analyzing, and accessing business data across an organization. Microsoft SQL Server 2005 provides a storage and management foundation for business data, and a set of reporting and analysis tools. Microsoft Office SharePoint Server 2007 provides controlled access to — and analysis of — business data, and the ability to leverage data to make better business decisions. Office SharePoint Server 2007 supports workflow, document management, search, data integration, data analysis, and data rendering. It enables you to maintain data integrity and centrally manage shared resources that can include reports, forms, documents, spreadsheets, and data connections.

The Microsoft BI stack is an end-to-end solution built on Microsoft SQL Server 2005, Office SharePoint Server 2007, 2007 Microsoft Office system client applications, and performance management products provided by the Office Business Applications group.

SQL Server 2005 is the data storage and analysis foundation of the Microsoft BI stack. SQL Server 2005 provides relational database management system (RDBMS) data storage, and a set of management tools including:

 SQL Server 2005 Analysis Services

 SQL Server 2005 Integration Services

 SQL Server 2005 Reporting Services

 SQL Server 2005 Business Intelligence Development Studio

## Business intelligence principles

The principles of business intelligence in Office SharePoint Server 2007 include:

 Data gathering   Integrating data from various structured and unstructured sources.

 Data storage   Providing a secure, centrally managed data repository.

 Data analysis   Creating hierarchical views to enhance data discovery and rendering data that can be understood in business terms.

 Data access   Improving data quality and ensuring data integrity by providing secure access to shared data resources in a collaborative workspace.

 Data cleansing   Ensuring that data from the source makes sense, is not duplicated, and does not contain null values.

 Extract, Transform, and Load (ETL)   Extracting data from source databases, transforming data into the structures used in targeted databases, and loading data into targeted databases.

## Business intelligence examples

Some examples of business intelligence solutions include:

 Predictive analysis   Determining the probable outcome of an event or the likelihood of a database state using information that is extrapolated from a known data set.

 Data mining   Sorting through data to identify patterns and establish cause-and-effect relationships.

 Sales forecasting   Reviewing current account status or customer characteristics and making adjustments based on live data.

 Purchase order approval   Checking current budget status and other data before approving a workflow-generated purchase order.

 Closed-loop analysis   Continuously tracking and improving the quality and performance of products and processes based on feedback. Closed-loop analysis enables you to align the day-to-day operations of an organization with a long-term business strategy. You can use closed-loop analysis to make data more discoverable and actionable.

# Plan data connection management

In this article:

 [About data connection management in Office SharePoint Server 2007](#DSDOC_section1b390b289_f7ac_457d_bbaa_f9)

 [Plan access to external data](#DSDOC_section2b390b289_f7ac_457d_bbaa_f9)

 [Plan access to data connection libraries](#DSDOC_section3b390b289_f7ac_457d_bbaa_f9)

## About data connection management in Office SharePoint Server 2007

Because connections to data sources are volatile, IT managers need an efficient way to maintain and update connections from Microsoft Office Excel 2007 spreadsheets to data sources. The physical stores that contain data sources can be moved and the names of physical stores can be changed. When a spreadsheet contains direct links to data sources, link integrity is dependent on the validity of the logical address of the linked source. If the logical address of a data source changes, or if the address of the data store that contains the data source changes, the link to the data source is broken.

Excel spreadsheets can contain data from multiple external data sources. Tracking and maintaining connections to multiple data sources within a single spreadsheet can be difficult and time consuming. IT managers often have to track and maintain multiple data sources in hundreds or thousands of spreadsheets. With Microsoft Office SharePoint Server 2007, you can prevent broken links to data sources by defining data connections and storing them in data connection libraries that can be centrally managed, updated, maintained, and listed in a SharePoint site.

## Plan access to external data

To plan a strategy for data connection management, you need to determine what kind of external data Excel spreadsheets will be accessing in your deployment scenario. Excel spreadsheets can access Microsoft SQL Server data and online analytical processing (OLAP) data. You can determine how data connections in workbooks that are opened in Excel Calculation Services are handled by the server. You can configure Excel Calculation Services to:

 Block all data connections.

 Allow data connections from trusted data connection libraries only.

 Allow embedded data connections and data connections from trusted data connection libraries.

Data connections can be saved as Office data connection (.odc) files, which are stored separately from spreadsheet files. Workbook authors who have write permissions to Office SharePoint Server 2007 can create data connection files from Office Excel 2007 by using the Data Connection Wizard. The wizard enables workbook authors to create .odc files and save them to a data connection library. Workbook authors who have access permissions to the data connection library can then use the .odc files to create data connection links in their workbooks.

## Plan access to data connection libraries

Excel Services provides an efficient way to manage the connections from Excel spreadsheets to external data sources by preventing the use of embedded data connections in spreadsheets. Instead of using an embedded link to connect directly to an external data source, the spreadsheet gets the latest connection definition from a data connection library and uses that definition to connect to the data source.

Data connection libraries contain .odc files and metadata about the connections. Data connection libraries enable spreadsheets to locate external data sources and maintain connections to data sources that have been renamed or moved to different servers. If an external data source is moved to a new server, the .odc file in the data connection library can be updated by using the location of the new server, and the connection from the spreadsheet is automatically updated.

You can restrict save access to data connection libraries and allow only trusted authors to save connection files. Restricted data connection libraries enable you to ensure that all connection files in a data connection library are authorized. By configuring Excel Calculation Services to use only data connection library connections, instead of direct connections to external data sources, you can ensure that spreadsheets connect only to authorized databases. By default, data connection libraries are created as part of the Report Center template. However, data connection libraries can be created anywhere in Office SharePoint Server 2007 and accessed from a centrally managed Office SharePoint Server 2007 portal site.

# Plan key performance indicators

In this article:

 [About KPIs](#DSDOC_section1d8f9b41e_e324_490d_bf85_13)

 [Plan data sources for KPIs](#DSDOC_section2d8f9b41e_e324_490d_bf85_13)

 [Plan KPIs in reports](#DSDOC_section3d8f9b41e_e324_490d_bf85_13)

 [Plan KPIs in dashboards](#DSDOC_section4d8f9b41e_e324_490d_bf85_13)

 [Plan KPIs in My Site](#DSDOC_section5d8f9b41e_e324_490d_bf85_13)

 [Worksheets](#DSDOC_section6d8f9b41e_e324_490d_bf85_13)

Key performance indicators (KPIs) are simple graphical scorecards that can be used to evaluate business data against business goals.

As part of planning your initial deployment of Microsoft Office SharePoint Server 2007, you should understand the data sources used in KPIs, how to configure those data sources and evaluate the status of indicators, and how to display KPIs in sites used by your organization. You can use these plans during initial deployment.

## About KPIs

KPIs are a central way of presenting business intelligence for an organization. Also known as status indicators or scorecards, KPIs evaluate business data against business goals and display current status by using easy-to-understand graphical indicators.

For example, a KPI can use traffic light icons to indicate that customer satisfaction is exceeding, meeting, or failing to meet goals. If customer satisfaction exceeds a preset goal, calculated by counting the percentage of positive satisfaction ratings across your organization, the customer satisfaction KPI is displayed with a green traffic light icon. If customer satisfaction is failing to meet minimum goals, the customer satisfaction KPI is displayed with a red traffic light icon. Otherwise, it is displayed with a yellow traffic light icon.

KPIs increase the speed and efficiency of evaluating progress against key business goals. Without KPIs, employees and business managers would have to painstakingly extract performance data and evaluate that data against goals, and then spend the time to present that data in a separate report for business decision makers. It is difficult to get timely status without a way to quickly and automatically evaluate live data. With KPIs, users who want to find out current performance can look quickly at a report in their business site, or even see relevant indicators in their personal sites.

KPIs connect to business data from various sources, and then use Web Parts that display that information in a list of KPIs or in a detailed view for a single KPI. Those Web Parts can be added to reports in the Report Center site, or displayed in other lists and sites.

Each KPI gets a single value from a data source, either from a single property or by calculating averages across the selected data, and then compares that value against a preselected value. Because values are calculated across a range of data rather than displaying data in list form, KPIs tend to be more useful when measuring performance across groups or projects. However, by calculating a range of data for a specific person, such as a list of sales for a single employee, a KPI can evaluate individual performance.

To use KPIs, you must first create a KPI list. KPI lists are created from a template that enables you to add KPIs based on any of the data sources described in the following table.

|  |  |
| --- | --- |
| Data source | Description |
| SharePoint lists | The data comes from a SharePoint list that might include business data from the Business Data Catalog or Microsoft SQL Server 2005. |
| Microsoft Office Excel 2007 workbooks | The data comes from an Excel workbook. |
| SQL Server 2005 Analysis Services | The data comes from database stores known as cubes, for connections in a data connection library. |
| Manually entered information | The data comes from a static list, rather than based on underlying data sources. This is used less frequently, for test purposes prior to deployment or on occasions when regular data sources are unavailable but you still want to provide performance indicators. |

After creating a KPI list, you create a Web Part that is bound to that KPI list. The KPI data is displayed in one of the following Web Parts:

 KPI List Web Part

 KPI Details Web Part

The KPI List Web Part shows a list of KPIs that correspond to the bound KPI list. The KPI Details Web Part shows detailed properties for a single KPI.

After you create a KPI Web Part, you can deploy that Web Part in several ways:

 In a KPI list page report in the Report Center site or a secondary Report Center site, or in a reports library on another site.

 In a multi-report summary page, or dashboard.

 In a personalization site.

The KPI list page is a type of report built around a KPI List Web Part, and related summary, and possibly other Web Parts depending on the purpose of the report. When you create a KPI list page report, a KPI List Web Part is included by default. Each KPI in the list must still be added. You can also highlight a single KPI in a report by using a KPI Details Web Part.

KPIs are often used as part of a multi-report summary page, or dashboard. Dashboards use filter Web Parts to filter the data displayed in Web Parts based on certain values. Filter KPIs can be applied dynamically, which enables a business decision maker to quickly compare performance over different periods of time. Dashboards can also filter by other properties.

KPIs in dashboards are more than a single view into data. KPIs are calculated across broad categories, such as total or average sales for employees in an organization. When you plan for KPIs and the lists and Web Parts used to display them, ensure that you know how each KPI will be evaluated during initial deployment and that you identify the data source and calculation method for each KPI.

## Plan data sources for KPIs

Each KPI in a KPI list is based on a data source. When you plan for KPIs in your sites, you also plan for data sources.

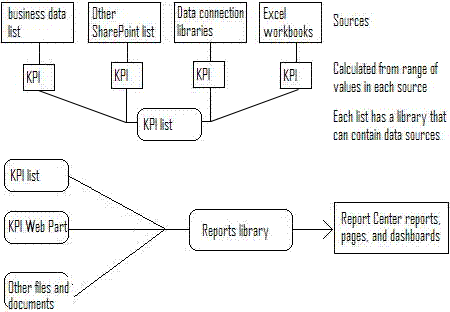
If a KPI is based on a SharePoint list, you must plan for the list, including its properties. Often, KPI lists are based on business data lists that use columns that are linked to business data applications. The values for those columns are updated as the underlying data is updated. You must plan to register these applications in the Business Data Catalog and import the properties that will be used for KPIs.

SharePoint lists used by KPIs must also be created before you can create the corresponding KPIs. Include every list necessary for KPI deployment in your planning for each site in each site collection.

If a KPI is based on an Office Excel 2007 workbook, ensure that the correct workbooks exist to display meaningful information. Sometimes workbooks are poorly organized or missing information that could be used by KPIs, and this is an opportunity to improve them. Those improvements will help when viewing that same data in an Excel Web Access Web Part, or working directly within the Office Excel 2007 application window.

For data in a SQL Server 2005 Analysis Services cube, plan to include that data in a data connection library.

For SharePoint lists, Excel workbooks, and SQL Server 2005 Analysis Services cubes used as KPI sources, you should consider where the lists, workbooks, and data connection libraries reside. It is usually a good idea to store this content in the site where it is being used. If you are putting a KPI on the home page of the portal site, it makes sense to create a KPI list on the home page. If you are putting a KPI in a report in the Report Center site, it is a good idea to put the lists, workbooks, and data connection libraries for the KPIs in the KPI list, and the KPI list itself in the reports library. If you are putting a KPI in a personalization site, it helps to put the related data sources there. The following figure shows a KPI in relation to other data sources.



It is possible to use data sources stored in document libraries and data connection libraries of other sites, which encourages collaboration and the reuse of valuable KPI lists. However, during initial deployment, it is good to keep your information organized simply and logically. This also simplifies security planning, because you can assume that a site and its content are stored in the same place and not scattered throughout the site collection.

Manually entered values are typically used for testing or temporary purposes, so you will probably only use them in planning and initial deployment to test KPI functionality before you begin a full-scale deployment.

Regardless of the data source for each KPI, you must decide on an appropriate set of values to use when indicating performance. Think about how you will calculate a comparative value from the data source. Which columns of data will you use? Will you calculate a value from a total, an average, a maximum, a minimum, or by some other means?

By planning ahead, you can avoid delays when you realize that an Excel workbook, for example, does not contain the actual set of data that you want to display performance for in the KPI. Plan ahead, select different data sources if you realize the sources you initially select will not provide the information you need for useful KPIs, and then record the plan so that you can finish deployment as quickly and effectively as possible.

|  |
| --- |
| Worksheet action |
| Use the [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) to record your KPI planning decisions. |

## Plan KPIs in reports

KPIs are common features of reports in the Report Center site and other sites that contain report libraries. One of the three main types of reports is a KPI list page report. This report includes a KPI List Web Part to which you can add KPIs for a particular business process, along with a summary of the related processes and any related content and Web Parts.

When planning KPI list pages, focus on the key business processes for each site collection, and combine as many KPIs on each list as you can for related processes. Continue until you have KPIs planned for each business process related to the central purpose of the site collection. This produces a manageable number of KPI list pages, for which you can plan KPI lists and KPIs, in addition to the SharePoint lists, Excel workbooks, and SQL Server 2005 Analysis Services cubes used by each KPI.

You will also want to decide which KPI list pages are important enough to include in the home page of the Report Center site and which should be linked from the page.

You will also want to consider which KPIs work together in dashboards. For large site collections that serve a large number of business applications and business processes, you will want to consider whether to plan more than one Report Center page. For more information about reports, see [Plan reports](#DSDOC_fbe7fe46_8d60_4de2_a699_7921c13dbd).

## Plan KPIs in dashboards

Dashboards, also known as multi-report summary pages, allow you to filter Web Parts at the page level so that every Web Part shows only filtered results. This can be useful for creating pages for monthly or weekly results, results for a team, or results filtered by several other criteria.

KPIs are often a key part of dashboards. KPIs cannot be connected to every kind of filter, but they can be connected to many of them. When deciding whether to include a KPI in a dashboard, consider how closely it relates to the other parts on the page. For more information about dashboards, see [Plan dashboards and filters](#DSDOC_5fe87ec1_431e_4b7f_ae33_1e2edd8613).

|  |
| --- |
| Worksheet action |
| Use the [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) to record the KPIs, KPI lists, and data sources used for dashboard pages and other key sites that use KPIs. |

## Plan KPIs in My Site

KPIs tend to be more useful in reports and dashboards than in the personalization sites, personal sites, and the public profile page that make up each My Site. However, you might still want to add KPI Web Parts to these sites.

For personalization sites, which are built by using a current user filter Web Part that can be connected to Web Parts on the page, KPIs are not connected but show information across the group of people that uses the personalization site to supplement the Web Parts that are connected and filtered. On a personalization site for a call center team, a KPI List Web Part that shows customer satisfaction, average call time, and number of resolved issues for the entire team supplements an Excel Web Access Web Part personalized to display data for the specific customer service representative who is viewing the page.

You cannot filter a KPI Web Part directly by using the current user filter on a personalization site. The reason for this is that the data in a KPI is often not meaningful when it is calculated across a filtered subset of its original data. A Web Part that tracks the number of sales for the group and the number of sales for one person will produce widely different values, and the KPI can only evaluate against one of the sets of values. Therefore, filtering the KPI that way is not possible.

You can target KPIs so that they appear only in personalization sites when the current viewer is a member of the correct audience. This allows you to target the whole list of KPIs or each individual KPI in the list depending on the scope of the KPI, just as you target the items in any list. If the KPI is of interest only to some users, such as those in the same work group, you can target it to an audience defined to include only the users in the work group. Using the example of a sales team, you might only show the results in the New York sales office to associates in the New York office.

You can use the KPI List Web Part to display several status indicators within one Web Part, such as sales records across the last few quarters. You can also use a KPI that shows sales volume, total value of sales, and improvement compared to the previous quarter in one Web Part.

You might decide during planning to modify the personal site template to include one or more KPI Web Parts, perhaps connected to prepopulated lists. This might be worthwhile for KPIs that you want to display more prominently, even though users might remove the KPI from their personal sites later on.

KPIs are less useful on public profile pages, which show information about a person rather than business processes. Planning for initial deployment is probably not a good time to consider adding KPIs to the public profile.

Consider the KPIs for each personalization site to ensure that they reflect the purpose of the site and the overall site collection. If the site collection is a team site for a sales team, sales data KPIs in a personalization site are appropriate. If it is a site collection intended for collaboration across a larger organization, the KPI will have to be targeted if it is included at all. If it is a site for human resources information, which is not used by any group in the organization to meet its goals but instead simply provides policies and business applications, it is inappropriate to use a KPI.

|  |
| --- |
| Worksheet action |
| Use the [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) to record the KPIs, KPI lists, and data sources used in personalization sites and other personalized sites that use KPIs. |

## Worksheets

Use the following worksheets to plan KPIs:

 [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409)

 [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409)

# Plan reports

In this article:

 [About reports](#DSDOC_section1fbe7fe46_8d60_4de2_a699_79)

 [Plan Web Parts for reports](#DSDOC_section2fbe7fe46_8d60_4de2_a699_79)

 [Plan reports for the Report Center site](#DSDOC_section3fbe7fe46_8d60_4de2_a699_79)

 [Plan the reports library](#DSDOC_section4fbe7fe46_8d60_4de2_a699_79)

 [Plan other features of the Report Center site](#DSDOC_section5fbe7fe46_8d60_4de2_a699_79)

 [Worksheets](#DSDOC_section6fbe7fe46_8d60_4de2_a699_79)

Reports are Web-based views of business data that is from various sources. In Microsoft Office SharePoint Server 2007, reports are displayed in pages by using business data and key performance indicator (KPI) Web Parts. These reports can be used alone or in multi-report dashboards to analyze and act on business data and business intelligence.

As part of planning for your initial deployment of Office SharePoint Server 2007, you should understand which Web Parts to use in reports and how to configure those Web Parts to use business data. You should also understand how to combine reports in report pages such as the Report Center site, how to configure management of report libraries, and what other information and features to enable for the Report Center site and other reports-enabled pages.

## About reports

You create reports by using business data Web Parts and KPI Web Parts to summarize data and Excel Web Access Web Parts for business intelligence analytics. Reports are displayed in the Web browser interface.

Each report is built around one or more Web Parts. The sources of data in the Web Parts in a report can be Microsoft SQL Server 2005, from either SQL Server 2005 Analysis Services or SQL Server 2005 Reporting Services, or line-of-business applications such as SAP and Siebel. Data in report Web Parts is often available in business data lists, which might be the direct source of the data.

Reports can appear in the following SharePoint sites in your site collections:

 Report Center site   Created when the site collection is created, the Report Center site contains a reports library, dashboards, and supporting content, and a home page that links to reports and supporting content.

 Other Report Center sites   Additional Report Center sites can be created for site collections that contain a large number of reports associated with distinct business processes.

 Report libraries in other sites   Anyone who can create document libraries on a site collection can choose to create report libraries. These libraries create reports that use one of three content types: a report, a Microsoft Office Excel 2007 report, or a dashboard page.

Reports also appear as items in lists and search results.

The business data Web Parts used in reports can appear in additional sites, including personalization sites, workspaces, and team collaboration sites, but those sites are not reports.

## Plan Web Parts for reports

Reports are pages built around one or more business data Web Parts, including:

 Business Data List Web Part

 KPI List Web Part and KPI Details Web Part

 Excel Web Access Web Part

 Reporting Services Report Web Part

When you create a report, you must provide the location of a business data Web Part or KPI Web Part.

The Web Part gallery suggests these same Web Parts, along with the Content Editor Web Part, but you can add any business data Web Part including other Web Parts with different views of business data lists, the Business Data Actions Web Part, or other specialized Web Parts. For more information about these Web Parts, see [Plan business data Web Parts](#DSDOC_165f1afe_11e5_4c45_8f93_bf16e18338).

Reports also include the following Web Parts:

 Summary Web Part   This is a Content Editor Web Part in the left zone intended to convey the purpose of the report and the business data it contains.

 Contact Details Web Part   This contains a picture and key properties for a person associated with the report page, usually the page owner.

Dashboard pages contain additional Web Parts. For more details about dashboard pages, see [Plan dashboards and filters](#DSDOC_5fe87ec1_431e_4b7f_ae33_1e2edd8613).

Each report is based around a set of business data in a business data Web Part. Each report is supplemented by a summary that explains the purpose of the report and provides details about the owner of the report. The Web Parts to use for each report should be narrowly focused on a single task or related set of tasks. Many reports contain only a single Business Data List Web Part or KPI Web Part.

Use the following steps to plan Web Parts for reports:

1. Identify a business process.

2. Plan to include a report for that business process.

3. Identify the Web Parts that will convey the information users need to act within that business process.

For example, a common business process in a sales organization is to identify which teams are meeting their sales goals. You decide to create a team sales KPI report that highlights the information. You decide to use a KPI List Web Part to list the relevant teams, and the KPI for each team will be evaluated by calculating the total sales for everyone on each team. You implement a business data list that connects to your sales database, and you include columns that will list the team name, employee names, and sales for each team. You will also need an explanation of the team goals that you can put in the Summary Web Part. In your planning, you record the report, Web Part, list, and list columns, and update the corresponding planning worksheets. In the case of reports based on Business Data List Web Parts, you might have several properties to record, each associated with a different business data type in the Business Data Catalog.

|  |
| --- |
| Worksheet action |
| Use the [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) to record business data and business intelligence Web Parts. Record connected Web Parts, data sources, and SharePoint lists used by the Web Part in the same table. |
| Use the [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) to record the key dashboard sites identified during site planning, and to record the Web Parts used by those sites. Also record the features enabled for the Report Center site, such as document libraries, documents, and images for each site. |

## Plan reports for the Report Center site

The Report Center site is a page that is created automatically for site collections in Office SharePoint Server 2007. It is a single location that has links to all of the reports and dashboards in the site collection. Users view the Report Center site by clicking Reports in the Quick Launch.

The default layout of the Report Center site includes the following Web Parts:

 In the left zone:

 Using the Report Center site   This is a Content Editor Web Part that contains introductory information about the Report Center site. The text here can be modified by site administrators depending on the content and business needs of the site collection and the Report Center site.

 Announcements   This is a List View Web Part that is used for posting announcements relevant to the Report Center site. By default, it has a welcome announcement. Report Center site contributors can add announcements.

 Highlights   This is a summary link Web Part tool that can be used to highlight reports, KPIs, and dashboards. By default, it includes a link to a quick reference guide. From the design mode, users who have the appropriate permissions can add links or group headings or configure the style and layout of this Web Part.

 In the right zone:

 Contact Details Web Part   Contributors can add one or more contacts here that are relevant to the Report Center site.

 Upcoming events   This is a List View Web Part used for adding events relevant to the business processes for the Report Center site. Contributors can add events.

The other zones are empty to start, but are often used to present important KPI or business data lists without having to open a separate report.

The Quick Launch in the Report Center site contains links to reports, dashboards, and resources. The Reports link opens up the reports library, which contains a list of all reports for the Report Center site.

There are three kinds of report pages:

 Report   This page highlights a business data Web Part, such as a Business Data List Web Part or a KPI List Web Part.

 Excel report   This page highlights data from a particular Excel worksheet.

 Dashboard page   This page highlights more than one business data Web Part, commonly filtered at the page level by particular properties. By default, each dashboard page contains a KPI List Web Part and an Excel Web Access Web Part.

Each type of report page includes a summary page and contact details for the owner of the report.

You can create additional Report Center sites focused around particular sets of business data and business intelligence by selecting the Report Center Site template when creating a site. The number of Report Center sites you have, and which reports are included in each Report Center site, depends on the purpose of each site collection. For most deployments, starting off with one Report Center site is sufficient. If planning the Report Center site becomes complex, you can consider additional folders for the reports library, or even additional report libraries to organize a large number of reports.

The number of potential reports for a Report Center can be fairly large even for a simple business process that uses a single business application. Consider the example of a sales reporting application. You might want to create reports that track employee performance, customer satisfaction, sales for a particular product, sales by location, and total quarterly revenues, among others. Some of the reports will be composed of KPI List Web Parts that show performance in scorecard format, some will be composed of KPI Details Web Parts that focus on a single item in a KPI list, and some might be business data lists that track several properties.

Many business processes use more than one application. You can use Excel Web Access Web Parts to perform analytics or update information in spreadsheets. You can use SQL Server 2005 Analysis Services to view information in a related data warehouse.

There are several actions you can perform to simplify Report Center planning:

 Focus the purpose of each site collection and related Report Center site as much as possible.

 Select only the most important cross-group KPIs and business data lists to implement during initial deployment, and defer the rest for ongoing operations.

 Present related Web Parts in dashboard pages, and use filters and Web Part targeting to improve relevancy and flexibility. For more information about dashboard pages and filters, see [Plan dashboards and filters](#DSDOC_5fe87ec1_431e_4b7f_ae33_1e2edd8613). For more information about targeting Web Parts, see [Plan for personalized Web Parts](#DSDOC_c976bea3_148c_4be6_96b7_6400c12692).

 Plan business data lists and Web Parts for reusability, so that you can use the same underlying lists for reports, dashboards, personalization sites, and Web Part galleries for other sites.

 Record the lists that you will need to implement the high-priority reports, include that information in business data list planning, and record the relevant business data types and properties of business applications in planning for business data profiles.

 Plan to observe usage patterns so that you can effectively update the Report Center site during ongoing operations.

## Plan the reports library

The reports library contains links to all reports for the Report Center site. It includes a version history for each report, and archives previous versions so you can view them. This enables you to create new versions of reports for special events or milestones, and later revert back to a previous report.

You can also change the view of the reports library list. The views available by default are:

 Current reports   This view shows the current versions of all reports.

 All reports and dashboards   This view shows all versions of reports, with the most recent versions listed first.

 Dashboards   This view shows only dashboard pages.

You can edit these views to add columns or filter content, or create new views.

Reports based on Excel Web Access Web Parts have a report profile page that includes additional information about the Excel spreadsheet.

When you plan for the reports library, consider who is likely to manage reports in the site collection, and whether reports need to be organized into folders by business application, work team, or business process. These decisions will be influenced by your information architecture planning and the purpose of each site collection as identified during site planning.

## Plan other features of the Report Center site

If you click Manage Content and Structure on the Site Actions menu of the Report Center site, you will see a list that contains links to every report and the following information:

 Announcements

 Data connections

 Documents

 Handbook

 Images

 Pages

 Reference library

 Reports library

 Report calendar

 Sample KPIs

 Workflow tasks

Each of these items is used to store content that can be used in the reports in the Report Center site. When you plan for Report Center sites in your site collection, make note of this content so you can include it for reports you make available during the initial deployment.

Examples of useful content for initial deployment includes documents that describe business processes related to key reports, data connections that are used by SQL Server 2005 Analysis Services and SQL Server 2005 Reporting Services reports, and images for report owners. Most supplementary content will be added during ongoing operations after the initial deployment.

You can also add additional report libraries to the Report Center site, or to other sites. You might want to plan for multiple report libraries if a Report Center is particularly complex. For example, a departmental portal site might include reports for several different applications or work teams. Each of these can be deployed by using a separate reports library, and you can use the targeting feature of Web Parts in the Report Center site so that users can view only the reports relevant to their job. Permissions can be set separately for each library if different users are managing different sets of reports.

## Worksheets

Use the following worksheets to plan reports:

 [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409)

 [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409)

# Plan dashboards and filters

In this article:

 [About dashboards and filters](#DSDOC_section15fe87ec1_431e_4b7f_ae33_1e)

 [Plan Web Parts for dashboards](#DSDOC_section25fe87ec1_431e_4b7f_ae33_1e)

 [Plan filters](#DSDOC_section35fe87ec1_431e_4b7f_ae33_1e)

 [Worksheets](#DSDOC_section45fe87ec1_431e_4b7f_ae33_1e)

Dashboards display reports and key performance indicators (KPIs) about the business data and business processes in your organization. The view of these reports can be filtered automatically or filtered by properties selected by users, enabling comparative data analysis across an organization.

As part of planning for your initial deployment of Microsoft Office SharePoint Server 2007, you should understand which Web Parts are common to dashboards, how filters are used on dashboards and other SharePoint sites, how to connect filters and business data Web Parts, and how to display those filters for people who use dashboards and other filter-enabled SharePoint sites.

## About dashboards and filters

Dashboards, also known as multi-report summary pages, contain one or more Web Parts, such as business data Web Parts, Excel Web Access Web Parts, or KPIs that can be filtered to provide a unified but flexible view of data and content from several sources. The data displayed on dashboards can be filtered at the page level or by Web Part by using the functionality of Microsoft SQL Server 2005 Reporting Services. For example, you can create a Customer Report dashboard that displays all KPIs and business data Web Parts for your organization's key business processes that relate to a particular customer.

Dashboards are one of the three content types that can be added to a reports library. The Report Center site that is created automatically for portal sites and other site collections contains a reports library, but users can add report libraries to other sites.

Dashboards are composed of a collection of business data Web Parts and a collection of filter Web Parts that connect Web Parts and change the data displayed based on data shared among the connected Web Parts. You can also create sites that filter data such as dashboards by adding connected filter and business data Web Parts to other site templates.

Some filter Web Parts filter data automatically. Some filter Web Parts enable users who view a dashboard to enter values or to select values from a list and then apply those values by clicking the Apply Filter button on the page. The Apply Filter button is implemented as another Web Part that is invisible on the dashboard until one or more filters that have user-specified values are added to the page.

The Apply Filter button and user-specified filters appear in a special filter zone in the dashboard template.

By default, a dashboard contains the layout and Web Parts listed and described in the following table.

|  |  |  |
| --- | --- | --- |
| Zone | Web Part | Description |
| Top left | Summary Web Part | This is a Content Editor Web Part that can be modified to add explanatory text for the information provided on the dashboard. |
| Top right | Contact Details Web Part | This contains contact information for the owner of the dashboard. |
| Filter | Apply Filter Web Part | Other filters added to the dashboard appear in this zone. |
| Bottom left | Excel Web Access Web Part | This Web Part can be configured to display data from Microsoft Office Excel 2007 worksheets. Depending on the purpose of the dashboard, administrators can remove this Web Part or supplement it with similar additional Web Parts. |
| Bottom middle | No default Web Part | This zone is empty, but it is a good place to add additional business data Web Parts, such as KPI List Web Parts and Business Data List Web Parts. |
| Bottom right | Related Information Web Part | This Web Part is used to add links to related reports, documents, sites, and other content. |

The usefulness of dashboards depends on the underlying Web Parts and filters and the connections you make between those components. Therefore, carefully planning which Web Parts and filters you use and how they interact can make a big difference in how effectively people can use business data in your organization.

## Plan Web Parts for dashboards

Dashboards are created to present a view of important business data used in common business processes. The first factor to consider when creating a dashboard or a site based on the same types of Web Parts is what the purpose of the site is. This will ensure that the common business processes associated with that purpose can be displayed in the dashboard.

When you plan site collections, you should consider the purpose of each site, which is usually based around groups of users in an organization and the different projects they work on. Some large site collections, such as centralized corporate portal sites, have a fairly broad set of purposes and organize diverse groups of users that work on a wide variety of business processes. Often you will have smaller site collections for more focused groups, projects, and business processes.

Whatever the structure of your site collections, you will want to create dashboards that organize the information in each discrete set of business processes. Some groups of users might have a single set of processes that they use regularly, while others might work across different processes. The number of dashboards and the content on each of them should reflect the work done by users and groups in your organization.

For each site, you should group business processes, identify Web Parts that can be used to display the data necessary to understand the status of key projects, and provide a single point of entry into more detailed information about those projects. These Web Parts contain important business data that can be filtered by other Web Parts.

The business data Web Parts that are commonly added to dashboards include:

 Additional Excel Web Access Web Parts

 Business Data List Web Parts

 KPI List Web Parts and KPI Details Web Parts

 Reporting Services Report Web Part

When you plan each of the business data Web Parts in a dashboard, consider the implications of the underlying connections to data sources and filter Web Parts. For data connections, you will want to add document libraries for Excel workbooks, register line-of-business applications in the Business Data Catalog, and import the proper set of properties into business data profiles. You will also want to create SharePoint lists for KPIs and add connections to the data connection library for SQL Server 2005 Analysis Services and SQL Server 2005 Reporting Services.

### Plan Excel Web Access Web Parts for dashboards

Excel Web Access Web Parts provide information from Excel workbooks directly within the dashboard page. The default view is a subset of cells selected by the site owner when adding the Web Part. Any automatic filters are applied before anyone views the page. Filters that have user-specified values are displayed as list menus or text boxes. These filters enable anyone to select values and filter the view on those values. Users who have the appropriate permissions on a spreadsheet can open it for editing by clicking the appropriate link in the Web Part. For example, you might want to use data from an Excel workbook to show sales data for all employees in a division.

### Plan business data Web Parts for dashboards

Business Data List Web Parts contain data from lists that are generated from applications registered in the Business Data Catalog. The most common type of this Web Part is a simple list, but you can also add Web Parts that detail individual items in a data source, or display lists of data related to associated properties in the data source. For example, you can add a Web Part that displays a list of customers, a detailed set of information about one customer, or a list of customers in a particular region. You can also add a Business Data Action Web Part that performs a previously defined action related to data that is contained in one of your business data applications.

All of these business data Web Parts can be connected to each other so that they can share data. The amount of data that can be shared and how it is shared depends on the Web Part, as described in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| Web Part | Maximum data rows shared with other Web Parts | Web Parts that can send data to this Web Part | Type of data this Web Part can receive |
| Business Data List Web Part | Up to two rows of data, each connected to a single other business data Web Part | Other business data Web Parts, Current User Filter Web Part, Property Profile Filter Web Part | Filter, parameter, filter values, or query values |
| Business Data Related List Web Part | Up to two rows of data, each connected to a single other business data Web Part | Other business data Web Parts, Current User Filter Web Part, Property Profile Filter Web Part | Filter, parameter, filter values, query values, or related items |
| Business Data Item Web Part | One row of data to one other business data Web Part | Other business data Web Parts, Current User Filter Web Part, Property Profile Filter Web Part | Filter, parameter, or new item |
| Business Data Action Web Part | Cannot send data to other Web Parts | Other business data Web Parts, Current User Filter Web Part, Property Profile Filter Web Part | Any |

These connections allow you to use multiple Web Parts to create or supplement data in another Web Part dynamically. You can:

 Use data in Business Data List Web Parts to create Business Data Item Web Parts or Business Data Related List Web Parts.

 Send a row in a business data Web Part to a Business Data Action Web Part as a new action.

 Filter data for a Web Part based on values passed from other business data Web Parts or the Current User Filter Web Part or Property Profile Filter Web Part.

For more information about Current User Filter Web Parts, Property Profile Filter Web Parts, and the other filter Web Parts that can be used to filter all Web Parts in a single dashboard page, see [Plan filters](#DSDOC_section35fe87ec1_431e_4b7f_ae33_1e) later in this article.

### Plan KPI Web Parts for dashboards

KPI Web Parts show the status of business processes by comparing a value, which is calculated from an underlying data source that has a value representing a goal for that process, and indicating the status by using a simple graphic. For example, a KPI can use traffic light icons to indicate that customer satisfaction is exceeding, meeting, or failing to meet goals. If customer satisfaction exceeds a preset goal, calculated by counting the percentage of positive satisfaction ratings across your organization, the customer satisfaction KPI is displayed with a green traffic light icon. If customer satisfaction is failing to meet minimum goals, the customer satisfaction KPI is displayed with a red traffic light icon. Otherwise, it is displayed with a yellow traffic light icon.

KPIs can be based on data from SharePoint lists, Excel workbooks, or SQL Server 2005 Analysis Services. Reporting Services Report Web Parts present data directly from SQL Server 2005 Reporting Services.

## Plan filters

Filters are Web Parts that connect to other filter Web Parts and business data Web Parts to enable dynamic views of business data in dashboards and other sites that use filters and business data Web Parts. There are several supported data types for filters, each associated with a different filter Web Part.

Some of the filters are applied to Web Parts on a page automatically without any input from users who view the page. These filters are added by dashboard owners to limit the scope of data on any dashboard site. Depending on the properties of each filter Web Part, most, but not all, of these filters are applied to all Web Parts on a page.

The other filters are applied to all data in all Web Parts on the page, according to values selected by users of the page. Three of those filter Web Parts use user-specified values for data, while the rest enable users to select values from a list that is created from values selected from various data sources by the site owner.

Not every Web Part can be connected to a filter. Each filter shows which Web Parts on the page it can connect to when you select the Web Part menu in design mode, point to Connections, and then point to Send Filter Values To. Every Web Part that can accept values from filters also shows that information in its Connections menu.

The supported data types and Web Parts are listed in the following table.

|  |  |  |
| --- | --- | --- |
| Data type | Selection format | Web Part |
| Text | User | Text Filter Web Part |
| Number | User | Number Filter Web Part |
| SharePoint list | List | SharePoint List Filter Web Part |
| Business Data Catalog | List | Business Data Catalog Filter Web Part |
| SQL Server 2005 Analysis Services | List | Analysis Services Filter Web Part |
| Manually entered list | List | Any filter Web Part that uses a manually entered list in Web Part properties |
| Values based on targeted Web Parts | List | Any targeted Web Part |
| Current user | Automatic | Current User Filter Web Part |
| Query string parameter | Automatic | Query String (URL) Filter Web Part |
| Fixed value | Automatic | Choice Filter Web Part |
| Page field value | Automatic | Page Field Filter Web Part |

### Plan automatic filter Web Parts

Several filters are applied automatically when the dashboard is displayed in a Web browser. These filters are configured by the owner of the site to limit the scope of displayed data. These filters are visible only in design mode. Because all other filters are applied after these filters by the option of users, these filters should be planned and implemented first.

The filter Web Parts that apply filters automatically are:

 Current User Filter Web Part

 Query String (URL) Filter Web Part

 Authored List Filter Web Part

 Page Field Filter Web Part

 Organization Filter (Direct Reports) Web Part

The Current User Filter Web Part and the related Property Profile Filter Web Part are included in the personalization site template and can also be added to dashboard sites. They filter respectively by the account name and preferred name properties of the user profile of the current user. They can pass these properties to other filters as default values and to business data Web Parts. For certain personalization Web Parts, this results in a personalized view that has information relevant to the user currently viewing the site.

The Property Profile Filter Web Part is used only on personalization pages. It is not available in Web Part galleries for other pages. For more information about personalization Web Parts, see [Plan for personalized Web Parts](#DSDOC_c976bea3_148c_4be6_96b7_6400c12692).

The Authored List Filter Web Part enables you to filter the page based on a list of properties that is authored by the site owner.

The Query String (URL) Filter Web Part automatically filters one or more Web Parts according to a query string provided by the dashboard owner. A default URL can be provided for the filter if the query string does not produce a valid URL.

The Page Field Filter Web Part enables you to filter content on the page based on the columns in the page list for the dashboard or any other Web Part page. You can filter one or more connected Web Parts based on the values in the selected column. You can also add columns to the list to expand your ability to filter Web Parts on the page.

### Plan filters that use user-specified values

The filters that use user-specified values are based on the following filter Web Parts:

 Text Filter Web Part

 Number Filter Web Part

Each of these filters enables individual users to enter values that are used to filter every Web Part on the dashboard. Filtering begins when the user clicks the Apply Filter button on the dashboard page. The default values for the Text Filter Web Part can be taken from the Current User Filter Web Part or the Property Profile Filter Web Part.

Planning for these filters is straightforward. If you want users to have the ability to quickly filter by values that are not in a list, you can enable these filters. It is usually a good idea to enable these filters first, so that some filtering is available with minimal effort by the site owner, with filters based on lists from data sources implemented later. However, after you have created more complex filters that are more relevant for the purpose of the site, these might no longer be necessary. Plan for more complex filters, but you can enable these filters early in deployment without any additional planning.

### Plan filters that use values selected from a list

Some of the filters that use user-specified values provide those values in a list created from other data sources. The filters are:

 Manually entered list (used by any filter Web Part)

 SharePoint List Filter Web Part

 Business Data Catalog Filter Web Part

 Analysis Services Filter Web Part

If you want to enable filtering by a simple list of values and do not want to create a SharePoint list or find other data sources that have those values, you can use a manually created list created from the Advanced Filter Properties page of filter Web Parts. Creating a list such as this is quick and easy, and it is a good early step along with enabling simple date and text filters to provide dashboard functionality until more complex filters are deployed.

More often, and particularly later in your deployment, you will want to use properties from more sophisticated data sources. It is worth taking the time to plan these kinds of filters, because they require that you also plan for the underlying data sources. You will want to create SharePoint lists, register business applications in the Business Data Catalog, and add connections to SQL Server 2005 Analysis Services cubes in data connection libraries before you create filters based on these sources.

The Business Data Catalog Filter Web Part filters other Web Parts on a page based on values of properties found in SQL Server 2005 Reporting Services or in applications that are registered in the Business Data Catalog. It is often used in combination with business data Web Parts to filter the view, and any recognized property can be used by this filter.

Analysis Services Filter Web Parts are selected from a hierarchical tree view. They enable you to filter Web Parts on a page based on values from SQL Server 2005 Analysis Services cubes and status indicators. This is often used to filter KPIs that are based on SQL Server 2005 Analysis Services data.

This view also enables you to show data from complex data stores so that anyone who uses a dashboard can quickly select any node in the tree and filter on that node. This provides analytics on complex data that are difficult to build any other way. This is a good option for large data warehouses that have read-only or infrequently updated data, but can be used for all kinds of data.

Access to some data sources, such as applications in the Business Data Catalog and SQL Server 2005 Analysis Services cubes, might require configuration of single sign-on to properly connect to data. Incorporate single sign-on planning into your plans for these data sources to ensure that filters and related Web Parts work properly. For more information, see [Plan for single sign-on](#DSDOC_3c78e886_5d20_44cb_b4e4_f823c4c019).

|  |
| --- |
| Worksheet action |
| Use the [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) to record business data and business intelligence Web Parts used by dashboards. Record connected filter Web Parts and the properties used by each filter, data sources, and SharePoint lists used by the Web Part in the same table. |
| Use the [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) to record the key dashboard sites identified during site planning, and to record the Web Parts used by those sites. |

## Worksheets

Use the following worksheets to plan dashboards and filters:

 [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409)

 [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409)

# Plan Excel Services security

In this article:

 [About Excel Services security](#DSDOC_section1a49883a7_de84_4a66_8fa0_7c)

 [Plan user authentication](#DSDOC_section2a49883a7_de84_4a66_8fa0_7c)

 [Plan communication among servers](#DSDOC_section3a49883a7_de84_4a66_8fa0_7c)

 [Plan external data authentication](#DSDOC_section4a49883a7_de84_4a66_8fa0_7c)

 [Worksheets](#DSDOC_section5a49883a7_de84_4a66_8fa0_7c)

## About Excel Services security

In addition to the security requirements for deploying Microsoft Office SharePoint Server 2007, you need to review security considerations for a deployment that includes Excel Services. Microsoft Windows SharePoint Services 3.0 provides the platform on which Office SharePoint Server 2007 is built.

Excel Services functionality, coupled with Office SharePoint Server 2007, is the primary way to control, secure, and manage access to Excel workbooks in the enterprise. Excel Services is an enterprise-class application server that is designed for performance, scalability, and security. An Excel Services deployment provides thin rendering of — and interactivity with — workbooks, and it enables you to easily reuse workbook components, such as charts and PivotTable reports, that can be rendered in business intelligence dashboards.

Excel Services enables you to leverage server-side Excel spreadsheet calculations for custom applications, and it provides users with the ability to lock workbooks and to secure private data and intellectual property. This ensures that data within your workbooks is protected while users interacting with workbooks on a server can take full advantage of the data refresh and recalculation functionality provided by Excel Services.

Security is an important component for enabling these data rendering scenarios. You need to consider many factors when planning for an environment that helps to ensure the security of workbooks that are rendered on a server. You need to plan for managing the security of workbooks and managing the security of the server itself. Excel Services provides you with a significant level of granular control for the processing and displaying of Excel workbooks. You can control how workbooks are opened on the server and the specific capabilities that are enabled for each workbook.

This article is an overview of the security settings for Excel Services and related components that you must consider when planning a deployment. In addition, this article provides prescriptive guidance for using Excel Services to help secure and manage access to workbooks on the server.

The security model for Excel Services is based on the concept that to ensure data integrity and quality, an administrator must be able to centrally manage shared resources and user access to corporate intellectual property contained in workbooks. To accomplish this, Excel Services enables you to specify:

 Trusted file locations   These are SharePoint document libraries, UNC paths, or HTTP Web sites that have to be explicitly trusted before Excel Calculation Services is allowed to access them. Excel Calculation Services opens workbooks that are stored in trusted file locations only.

 Trusted data providers   These are external databases that Excel Calculation Services is explicitly configured to trust when processing data connections in workbooks. Excel Calculation Services attempts to process a data connection only if the connection is to a trusted data provider.

 Trusted data connection libraries   These are SharePoint document libraries that contain Office data connection (.odc) files. The .odc files are used to centrally manage connections to external data sources. Instead of allowing embedded connections to external data sources, Excel Calculation Services can be configured to require the use of .odc files for all data connections. The .odc files are stored in data connection libraries, and the data connection libraries have to be explicitly trusted before Excel Calculation Services will allow workbooks to access them.

note_ddNote:

When you open a workbook in Excel Calculation Services, a temporary file is stored in the %TEMP% folder of the application server that is running 2nd\_ExcelCalc.

## Plan user authentication

Excel workbooks that are opened by Excel Calculation Services should be stored in the Office SharePoint Server 2007 content database, because Windows SharePoint Services 3.0 maintains an access control list (ACL) for these files. Excel Calculation Services can also open workbooks from UNC paths and HTTP Web sites, but we recommend using the Office SharePoint Server 2007 content database for workbook storage.

Authentication for user access to a SharePoint portal site is performed by Windows SharePoint Services 3.0. By default, Windows SharePoint Services 3.0 uses Integrated Windows authentication.

In addition to the listed authentication methods, Excel Services also supports generic forms-based authentication. However, configuring Windows SharePoint Services 3.0 to use generic forms-based authentication is beyond the scope of this article.

## Plan communication among servers

You can determine how front-end Web servers communicate with Excel Calculation Services application servers, and how application servers communicate with back-end data sources, by configuring Excel Services to use either trusted subsystem data access or delegation. Trusted subsystem is the default setting for a Windows server farm, because it does not have the extra configuration requirements of the delegation model. In the trusted subsystem model, front-end Web servers and Excel Calculation Services application servers trust the accounts of the associated Office SharePoint Server 2007 applications by using the Shared Services Provider (SSP).

In a trusted subsystem environment, when opening files from Office SharePoint Server 2007, permission checks on the files can be performed against end-user identities even if Kerberos is not configured. If Excel Calculation Services application servers open workbooks from UNC shares or HTTP Web sites, the user account cannot be impersonated, and the process account must be used.

note_ddNote:

To impersonate the user account and implement workbook authorization, you must set up constrained Kerberos delegation between Excel Calculation Services application servers and UNC or HTTP resources.

Constrained Kerberos delegation is the most secure configuration for communication between front-end Web servers and Excel Calculation Services application servers. Constrained Kerberos delegation is also the most secure configuration for accessing back-end data sources from application servers. Constrained Kerberos delegation is the preferred configuration for deploying Excel Services. For external data connections, Integrated Windows authentication will only work if the delegation model is implemented.

## Plan external data authentication

Workbooks can contain embedded direct data connections and links to data connection files that are stored in data connection libraries. On refresh, depending on the configuration of Excel Services, the embedded direct data connection can be used to query the data source, or the data connection library link can be used to query the .odc file. The .odc file contains data connection information and must be stored in a data connection library.

To configure Excel Services to process connections to external data sources, select a setting in the External Data section of the Excel Services Add Trusted File Location page of the SharePoint Central Administration Web application.

To configure administrative settings for Excel Services, open the SharePoint Central Administration Web application from Office SharePoint Server 2007 and perform the following procedure.

procedure_ddConfigure administrative settings for Excel Services

|  |
| --- |
| 1. On the Central Administration home page, click Application Management.  2. On the Application Management page, in the Office SharePoint Server 2007 Shared Services section, click Create or Configure this Farm's Shared Services.  3. On the Manage this Farm's Shared Services page, click SharedServices1 (Default). This is the SSP that you will configure.  4. On the Shared Services home page, in the Excel Services Settings section, click Trusted file locations.  5. On the Excel Services Trusted File Locations page, click Add Trusted File Location.  6. In the Address section, type the location and name of the SharePoint document library that you want to add as a trusted file location in Excel Services. If the document library is stored in the Windows SharePoint Services 3.0 content database, make sure Windows SharePoint Services 3.0 is selected as the Location Type. |

Delegation is required for most farm deployments that have integrated connections. When Excel Calculation Services retrieves connection information, credentials are designated as Stored (to be retrieved from the SSO database), Integrated, or None. For data connections with integrated credentials, delegation is required for deployments that are scaled out to multiple servers. In a stand-alone deployment, delegation is not required.

Imagine a data connection in a workbook opened in an Excel Calculation Services application server that uses the Stored credentials method. Excel Calculation Services has to retrieve valid credentials from a single sign-on (SSO) authentication database. Then, it uses the credentials to authenticate against a data source, before the data connection can be established.

Excel Services supports three data authentication methods: Integrated Windows authentication, SSO authentication, and None.

### Integrated Windows authentication

Integrated Windows authentication usually requires constrained Kerberos delegation, which is the most secure authentication method. We recommend that you enable constrained Kerberos delegation for authentication from front-end Web servers to application servers running Excel Calculation Services, and from Excel Calculation Services to external data sources. For Excel Services scenarios, we recommend using Integrated Windows authentication.

### SSO authentication

SSO authentication enables users to access multiple system resources without having to provide authentication credentials more than once. Office SharePoint Server 2007 implements SSO authentication by including a Windows service and a secure credentials database. Using the pluggable SSO functionality supported by Excel Services, you can implement your own SSO provider. Office SharePoint Server 2007 includes a Windows SSO provider that works with Excel Services.

Any SSO provider that you implement with Excel Services should maintain a flag for each SSO entry that specifies whether the SSO entry is using Windows-based credentials or credentials from another environment. The Windows SSO provider in Office SharePoint Server 2007 maintains a flag for this purpose. Excel Services uses the SSO database to retrieve credentials for connection authentication.

SSO authentication in Office SharePoint Server 2007 supports individual mappings and group mappings. SSO maintains a set of credentials for the application identities (App IDs) of resources that are stored in the Office SharePoint Server 2007 SSO database. For individual mappings, a security layer checks user credentials against multiple individual listings for an App ID that is stored in the SSO database. Individual mappings are useful if you need logging information about individual user access to shared resources.

For group mappings, a security layer checks group credentials for multiple domain users against a single set of credentials for a resource identified by an App ID that is stored in the SSO database. Group mappings are easier to maintain than individual mappings, and performance is better.

To enable SSO functionality for Office SharePoint Server 2007, start the Microsoft Single Sign-On service and then configure SSO settings in the SharePoint Central Administration Web application. Use the following procedures to set up and configure an SSO database to authenticate data connections.

procedure_ddStart the Single Sign-On service

|  |
| --- |
| 1. From Administrative Tools, click Services.  2. Double-click Microsoft Single Sign-On Service.  3. On the Log On tab of the Single Sign-On Service Properties page, click This account, and then type the domain, user name, and password that you have used to install and manage your server.  4. Click Apply.  5. On the General tab of the Single Sign-On Service Properties page, change the startup type to Automatic, click Start, and then click OK.  note_ddNote:  Start the Single Sign-On service on all front-end Web servers and all application servers in your farm that run Excel Calculation Services. |

procedure_ddManage SSO settings

|  |
| --- |
| 1. From Administrative Tools, open the SharePoint Central Administration Web application.  2. On the Central Administration home page, click Operations.  3. In the Security Configuration section, click Manage settings for single sign-on.  4. On the Manage Settings for Single Sign-On page, click Manage server settings.  5. In the Account Name box for the SSO Administrator account, type the same domain and user name that you used to configure the Single Sign-On service. If the user name that you used to configure the Single Sign-On service is a member of a Windows security group, you can type the name of the Windows security group instead of a user name.  6. In the Enterprise Application Definition Administrator Account box, type the same domain and user name that you used to configure the Single Sign-On service. |

### None

When you specify None as the authentication method for your Excel Services deployment, Excel Services tries to use inbound connection strings to connect to the database specified in the string. Depending on the specific database provider, the database might be able to use the connection string to authenticate the user.

Excel Services does not parse connection strings to determine an authentication method. The connection strings are simply passed to the database provider. Connection strings can specify that Integrated Windows authentication is required. Connection strings can also contain a specific user name and password. In either case, when you specify None as the authentication method, Excel Services requires the impersonation of an unattended service account.

If the database provider determines that the connection string specifies Integrated Windows authentication, and if the database authorizes access, the connection is established by using the security context of the unattended account. If the connection string contains a user name and password, and if the database authorizes access, the connection is established by using the security context of the authorized user account.

### Unattended service account

The unattended service account is a low-permissions account that Excel Calculation Services can impersonate when establishing a data connection that uses SSO credentials from an environment that is not Windows-based, or None, as the authentication method. If an unattended service account is not configured, data connections will fail if SSO from an environment other than Windows, or None, is used as the authentication method.

Impersonating the unattended account protects Office SharePoint Server 2007 databases, and any other data sources that Excel Services can directly access, from unauthorized connections by client computers that are using Excel Calculation Services to open external data connections. When an unattended service account is impersonated, the credentials associated with an Excel Calculation Services application thread cannot be used to access any other databases. Also, when an unattended service account is impersonated, external data queries are run under the security context of a low-permissions account, instead of running under the security context of an Excel Calculation Services application thread that has greater permissions.

You can configure the unattended service account either as a domain account or as a local computer account. If the unattended service account is configured as a local computer account, ensure that the configuration is identical on every application server running Excel Calculation Services. Restrict the permissions of the unattended service account to enable only logging on to the network. Verify that the unattended service account does not have access to any data sources or Office SharePoint Server 2007 databases. Use the following procedure to enable the unattended service account.

procedure_ddEnable the unattended service account

|  |
| --- |
| 1. In the Name and Password boxes in the External Data section of the Excel Services Settings page, type the name and password that you want to use.  2. Click OK. |

### Security settings

To configure administrative settings for Excel Services, including security settings, open the SharePoint Central Administration Web application from Administrative Tools in Microsoft Windows Server 2003, and perform the following procedure.

procedure_ddConfigure security settings for Excel Services

|  |
| --- |
| 1. On the Central Administration home page, click Application Management.  2. On the Application Management page, in the Office SharePoint Server 2007 Shared Services section, click Create or Configure this Farm's Shared Services.  3. On the Manage this Farm's Shared Services page, click SharedServices1 (Default). This is the SSP that you will configure.  4. On the Shared Services home page, in the Excel Services Settings section, click Edit Excel Services settings. |

You can also use the Excel Services Settings page to configure the options for file access method and data encryption, which have a direct impact on secure deployment.

### File access method

On the Excel Services Settings page, in the Security section, under File Access Method, select either Impersonation or Process account.

 Impersonation   This enables a thread to run in a security context other than the context of the process that owns the thread. Select Impersonation to require Excel Calculation Services to authorize users when they try to access workbooks that are stored in UNC and HTTP locations. Selecting this has no affect on workbooks that are stored in Office SharePoint Server 2007 databases. In most server farm deployments in which front-end Web servers and Excel Calculation Services application servers run on different computers, impersonation will require constrained Kerberos delegation.

 Process account   If Excel Calculation Services application servers are opening workbooks from UNC shares or HTTP Web sites, the user account cannot be impersonated, and the process account must be used.

### Data encryption

You can use Internet Protocol Security (IPsec) or Secure Sockets Layer (SSL) to encrypt data transmission among Excel Calculation Services application servers, data sources, client computers, and front-end Web servers. To require encrypted data transmission between client computers and front-end Web servers, change the Connection Encryption setting from None to All connections. None is the default setting. If you change the Connection Encryption setting to All connections, the Excel Calculation Services application server will only allow data transmission between client computers and front-end Web servers over SSL connections.

If you decide to require encrypted data transmission, you will have to manually configure IPsec or SSL. You can require encrypted connections between client computers and front-end Web servers while allowing unencrypted connections between front-end Web servers and Excel Calculation Services application servers.

### Trusted file locations

Trusted file locations are SharePoint sites, UNC paths, or HTTP Web sites from which a server running Excel Calculation Services is permitted to access workbooks.

In the Location section of the Excel Services Add Trusted File Location page, you can configure the address, the location type, and whether child libraries of trusted file locations are also trusted. By selecting Trust Children you can improve manageability, but you can also create a potential security issue by enabling subsites and subdirectories of trusted locations to be automatically trusted as soon as they are created.

|  |
| --- |
| Worksheet action |
| Use the [Trusted file locations worksheet](http://go.microsoft.com/fwlink/?LinkId=73327&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73327&clcid=0x409) to record the names of trusted SharePoint sites, UNC paths, and HTTP Web sites. |

In the Session Management section, you can configure settings to help conserve resource availability and improve Excel Calculation Services performance and security. Performance can suffer when a large number of users have multiple Excel Calculation Services sessions open concurrently. You can control resource consumption and limit the duration of open Excel Calculation Services sessions by configuring two different time-out settings for open sessions.

The Session Time-out setting determines the amount of time an Excel Calculation Services session can remain open and inactive after each user interaction. The Short Session Time-out setting determines the amount of time an Excel Calculation Services session can remain open and inactive after the initial session request. You can also control the number of seconds allowed for any single session request by configuring a Maximum Request Duration value. By limiting the amount of time that sessions remain open, you can help reduce the risk of denial-of-service attacks.

In the Workbook Properties section, you can configure a maximum size of any workbook that is permitted to be opened in an Excel Calculation Services session. Performance and resource availability can be compromised when users open extremely large workbooks. Unless you control the allowable size of workbooks running in open Excel Calculation Services sessions, you risk users exceeding your resource capacity and causing the server to fail.

note_ddNote:

If an application server running Excel Calculation Services fails or is shut down, all open sessions on the server are lost. In a stand-alone installation, Excel Services will no longer be available. This means that workbooks cannot be loaded, recalculated, refreshed, or retrieved by Excel Calculation Services. In a server farm deployment that includes multiple application servers running Excel Calculation Services, shutting down one server does not affect open sessions that are running on other servers. Users with sessions running on a server that is shut down are prompted to reopen their workbooks. When users start a new session, they are automatically routed to active application servers running 2nd\_ExcelCalc.

In the External Data section, you can determine whether workbooks stored in trusted file locations and opened in Excel Calculation Services sessions can access an external data source. You can designate whether Allow External Data is set to None, Trusted data connection libraries only, or Trusted data connection libraries and embedded. If you select either Trusted data connection libraries only or Trusted data connection libraries and embedded, the workbooks stored in the trusted file locations are allowed to access external data sources.

External data connections can be accessed only when they are embedded in or linked from a workbook. Excel Calculation Services checks the list of trusted file locations before opening a workbook. If you select None, Excel Calculation Services will block any attempt to access an external data source. If you manage data connections for a large number of workbook authors, consider specifying Trusted data connection libraries only. This ensures that all data connections in all of the workbooks generated by authenticated workbook authors have to use a trusted data connection library to access any external data sources.

If you manage data connections for a small number of workbook authors, consider specifying Trusted data connection libraries and embedded. This enables workbook authors to embed direct connections to external data sources in their workbooks, but still have access to trusted data connection libraries if the embedded links fail.

In the Warn on Refresh area of the External Data section, you can specify whether a warning is displayed before a workbook refreshes from an external data source. By selecting Refresh warning enabled, you ensure that external data is not automatically refreshed without user interaction.

In the Stop When Refresh on Open Fails area, you can specify if Excel Calculation Services stops opening a workbook if the workbook contains a Refresh on Open data connection that fails. By selecting Stopping open enabled, you ensure that cached values are not displayed if a refresh operation fails when the workbook is opened. When Refresh on Open is successful, cached values are purged. By clearing the Stopping open enabled check box, you risk displaying cached values if Refresh on Open fails.

In the External Data Cache Lifetime area of the External Data section, you can specify the maximum amount of time cached values can be used before they expire.

To ensure that only trusted users have access to workbooks stored in trusted locations, it is important to enforce ACLs on all trusted file locations.

There are three core scenarios for deploying Excel Services with Office SharePoint Server 2007: enterprise, small department, and custom.

In an enterprise deployment, consider the following guidelines:

 Do not configure support for user-defined functions.

 Do not allow workbooks to use embedded data connections to directly access external data sources.

 Limit the use of data connection libraries for external data source access from workbooks.

 Restrict the size of workbooks that can be opened in Excel Calculation Services.

 Selectively trust specific file locations and do not enable Trust Children for trusted sites and directories.

In a small department deployment, consider the following guidelines:

 Enable trust for all file locations that are used by department members to store workbooks.

 Enable Trust Children for all trusted sites and directories.

 Selectively restrict access to specific file locations if problems arise.

In a custom deployment, consider the following guidelines:

 Enable Excel Calculation Services to open large workbooks.

 Configure long session time-out settings.

 Configure large data caches.

 Create a single trusted location for this deployment.

 Do not enable Trust Children for this trusted location.

### Trusted data providers

You can control access to external data by explicitly defining the data providers that are trusted and recording them in the list of trusted data providers. The list of trusted data providers designates specific external data providers to which workbooks opened in Excel Calculation Services are permitted to connect.

Before instantiating a data provider to enable a workbook to connect to an external data source, Excel Calculation Services checks the connection information to determine whether the provider appears on the list of trusted data providers. If the provider is on the list, a connection is attempted; otherwise, the connection request is ignored.

|  |
| --- |
| Worksheet action |
| Use the [Trusted data providers worksheet](http://go.microsoft.com/fwlink/?LinkId=73325&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73325&clcid=0x409) to record the names of trusted data providers. |

### Trusted data connection libraries

A trusted data connection library is a document library from which you have determined that it is safe to access .odc files. Data connection libraries are used to secure and manage data connections for workbooks that are accessed by a server running Excel Calculation Services. A list of trusted data connection libraries designates specific data connection libraries from which workbooks opened in Excel Calculation Services are permitted to access .odc files.

If a data connection is linked from a workbook that is accessed by a server running Excel Calculation Services, the server checks the connection information and the list of trusted data connection libraries. If the data connection library is on the list, a connection is attempted by using the .odc file from the data connection library; otherwise, the connection request is ignored.

|  |
| --- |
| Worksheet action |
| Use the [Trusted data connection libraries worksheet](http://go.microsoft.com/fwlink/?LinkId=73324&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73324&clcid=0x409) to record the names of trusted data connection libraries. |

### View Only permissions

You can specify users who are only permitted to view workbooks by adding them to the Office SharePoint Server 2007 Viewers group or by creating a new group configured with View Only permissions. The Viewers group is configured with View Only permissions by default. Users added to a group configured with View Only permissions can view, open, interact with, refresh, and recalculate workbooks, but they are prevented from accessing the file source in any way, other than by using Excel Services. This helps you protect your proprietary information. The source data is never displayed to the designated users.

Workbooks and workbook data objects configured with View Only permissions cannot be opened in Office Excel 2007; however, a snapshot of the workbook, displaying only values and formatting of the server-viewable ranges, can be rendered in Office Excel 2007.

You can configure site settings in Office SharePoint Server 2007 to control access to workbook data by setting View Only permissions on centrally managed workbooks that are rendered in a Web browser. You can also configure site settings in Office SharePoint Server 2007 to enable workbooks to refresh external data on the server, and to secure and manage external data connections. Use the following procedure to save specified data objects as View Only items.

procedure_ddSave specified data objects as View Only items

|  |
| --- |
| 1. Open a workbook that contains data objects, such as charts and tables, in Office Excel 2007.  2. Publish the workbook to a SharePoint document library that is listed as a trusted location for Excel Services.  3. In the File Name box on the Save As dialog box, type the URL for the SharePoint document library where you want to save the file. Ensure the Open this workbook in my browser after I save check box is selected.  4. Click Excel Services Options.  5. On the Excel Services Options dialog box, select Items in the Workbook from the drop-down menu.  6. Select the items you want to render, and then click OK.  7. On the Save As dialog box, click Save. |

### External data connections

The Excel Calculation Services component of Excel Services is used to connect to external data sources. Excel Calculation Services processes external data connection information that contains everything the server needs to connect to a data source, including how to authenticate, which connection string to use, which query string to use, and where and how to gather credentials to use for the connection. These connections can be defined in two places: embedded within workbooks and in .odc files. The connection information is identical in both places. The .odc files are small files that persist connection information in plain text and in a format that is reusable.

You can use the Office Excel 2007 client to author and edit .odc files and connections embedded in workbooks. In the Office Excel 2007 client, you can run the Data Connection Wizard or configure the settings in the Connections properties page. You can also export an .odc file based on these settings. The Connections properties page shows connection information, including Excel Services authentication properties.

|  |
| --- |
| Worksheet action |
| Use the [External data connections worksheet](http://go.microsoft.com/fwlink/?LinkId=73323&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73323&clcid=0x409) to record the names of .odc files and the locations of corresponding external data sources. |

### .odc files

Workbooks can contain links to .odc files and embedded connection information. This enables workbooks to retrieve the .odc file, read the contents, and attempt to connect to an external data source if the embedded connection information fails. The .odc files must be managed and maintained to ensure that they contain accurate data connection information.

You can also configure Excel Calculation Services to use connection information from the .odc file exclusively instead of first trying to connect by using the embedded information. This approach enables administrators to deploy a small set of managed .odc files that provide updated connection information to many workbooks.

Workbook authors can specify, on a per-connection basis, which connection information the workbook can use. To do this, open Office Excel 2007 client and click Workbook Connections on the Data tab. Add a connection to a workbook, open Workbook Connections, and then view the properties of the connection you just added. On the Definition tab, select Always use connection file. This setting enables the workbook to retrieve a connection file from a data connection library and use the connection information within the file to connect to an external data source. You can also configure this setting by selecting Always use connection file on the final page of the Data Connection Wizard.

### Managing .odc files

Data connection libraries provide a repository for collections of .odc files. Administrators can manage data connections on the server by creating a data connection library and .odc files that require workbooks to always use a connection file. Workbooks that consume connections directly from a data connection library will always get updated connection information before connecting to a data source.

If data source information changes (for example, the server name), you only need to update one .odc file in the data connection library and all of the workbooks that consume the .odc file will be automatically updated the next time they refresh. You can also use View Only permissions to restrict access to .odc files.

### User-defined functions

If your deployment scenarios include workbooks that contain user-defined functions to extend the capabilities of Excel Calculation Services, you need to configure Excel Services to support user-defined functions.

To configure this support, you must enable user-defined functions on trusted file locations containing workbooks that require access to user-defined functions. In addition, you must register user-defined function assemblies on the Excel Services user-defined function assembly list. Use the following procedures to enable user-defined functions.

procedure_ddEnable user-defined functions

|  |
| --- |
| 1. In the Excel Services section of the Shared Services home page, click User-defined functions.  2. On the Excel Services User-Defined Functions page, click Add User-Defined Function Assembly.  3. In the Assembly box, type the assembly strong name or the file path of the user-defined function assembly that you want to register.  4. In Assembly Location, perform the following actions:  a. Select the global assembly cache (GAC) if you are deploying a user-defined function assembly to the GAC on each Excel Calculation Services application server in your farm.  b. Select Local file if you want to save a user-defined function to a directory on an Excel Calculation Services application server (a local path), or to a network share (a UNC path).  c. Ensure the Enable Assembly check box is selected, and then click OK. |

procedure_ddEnable user-defined functions for workbooks in a trusted file location

|  |
| --- |
| 1. In the Excel Services section of the Shared Services home page, click Trusted file locations.  2. On the Excel Services Trusted File Locations page, click the URL of the trusted file location whose properties you want to edit.  3. In the User-Defined Functions section of the Excel Services Edit Trusted File Location page, select User-defined functions allowed, and then click OK. |

## Worksheets

Use the following worksheets to plan Excel Services security:

 [External data connections worksheet](http://go.microsoft.com/fwlink/?LinkId=73323&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73323&clcid=0x409)

 [Trusted data connection libraries worksheet](http://go.microsoft.com/fwlink/?LinkId=73324&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73324&clcid=0x409)

 [Trusted data providers worksheet](http://go.microsoft.com/fwlink/?LinkId=73325&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73325&clcid=0x409)

 [Trusted file locations worksheet](http://go.microsoft.com/fwlink/?LinkId=73327&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73327&clcid=0x409)

# Determine resource requirements to support Excel Services

In this article:

 [About Excel Services topologies](#DSDOC_section1fb6928ce_49f8_492a_abff_5b)

 [Plan for simultaneous client connections](#DSDOC_section2fb6928ce_49f8_492a_abff_5b)

 [Plan for concurrent Excel Calculation Services session requests](#DSDOC_section3fb6928ce_49f8_492a_abff_5b)

 [Excel Services performance testing](#DSDOC_section4fb6928ce_49f8_492a_abff_5b)

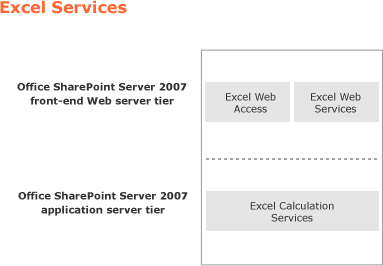
 [Limit the number and duration of open sessions](#DSDOC_section5fb6928ce_49f8_492a_abff_5b)

Many factors can affect the performance and availability of your Microsoft Office SharePoint Server 2007 deployment, including network bandwidth and resource consumption. Excel Services in Office SharePoint Server 2007 can affect system performance, depending on the volume of client connections and the number of simultaneous Excel Calculation Services session requests. Calculation size and complexity can also affect Excel Calculation Services resource consumption.

The scope and complexity of Excel calculations can affect the performance and availability of Excel Services in an Office SharePoint Server 2007 deployment. As calculation volume, complexity, and frequency increase, more system resources are consumed. Define baseline hardware requirements for system memory, CPU speed, and storage for each application server that runs Excel Calculation Services.

## About Excel Services topologies

Office SharePoint Server 2007 is logically divided into three tiers: the front-end Web server tier, the application server tier, and the database tier. During installation, Excel Services installs two components (Excel Web Access and Excel Web Services) on the front-end Web server tier, and one component (Excel Calculation Services) on the application server tier, as shown in the following diagram.



A network load balancer enables Office SharePoint Server 2007 to scale out front-end Web servers. The network load balancer is available to all Office SharePoint Server 2007 applications. You can scale out application servers by adding computers within the shared services framework in Office SharePoint Server 2007.

There are three schemes for load balancing Excel Calculation Services requests: Workbook URL, Round-Robin, and Local. You can configure separate load balancing schemes for each Shared Services Provider (SSP).

For information about how to install the Office SharePoint Server 2007 Excel Services components, see the following articles:

 Deploy Office SharePoint Server 2007 on a stand-alone computer

 Deploy Office SharePoint Server 2007 in a server farm environment

### Data access models

There are two data access models you can use for any of the Excel Services server farm topologies: trusted subsystem and constrained Kerberos delegation.

 Trusted subsystem   This is the default setting for a Windows server farm, because it does not have the extra configuration requirements of the delegation model. In the trusted subsystem model, front-end Web servers and application servers running Excel Calculation Services trust the accounts of the associated Office SharePoint Server 2007 applications by using the SSP. In a trusted subsystem environment, when opening files from Microsoft Office SharePoint Server 2007, permission checks on the files can be performed against end-user identities even if Kerberos is not configured. If Excel Calculation Services application servers are opening workbooks from UNC shares or HTTP Web sites, the user account cannot be impersonated, and the process account must be used.

 Constrained Kerberos delegation   This is the most secure configuration for communication between front-end Web servers and Excel Calculation Services application servers. Constrained Kerberos delegation is also the most secure configuration for accessing back-end data sources from application servers. Constrained Kerberos delegation is the preferred configuration for deploying Excel Services. For external data connections, Integrated Windows authentication will only work if the delegation model is implemented.

### Excel Services topologies

The following Excel Services topologies are described in this section:

 [Excel Services single-server topology](#DSDOC_subsection1fb6928ce_49f8_492a_abff)

 [Excel Services small farm trusted subsystem topology](#DSDOC_subsection2fb6928ce_49f8_492a_abff)

 [Excel Services small farm Kerberos topology](#DSDOC_subsection3fb6928ce_49f8_492a_abff)

 [Excel Services medium farm trusted subsystem topology](#DSDOC_subsection4fb6928ce_49f8_492a_abff)

 [Excel Services medium farm Kerberos topology](#DSDOC_subsection5fb6928ce_49f8_492a_abff)

 [Excel Services large farm trusted subsystem topology](#DSDOC_subsection6fb6928ce_49f8_492a_abff)

 [Excel Services large farm Kerberos topology](#DSDOC_subsection7fb6928ce_49f8_492a_abff)

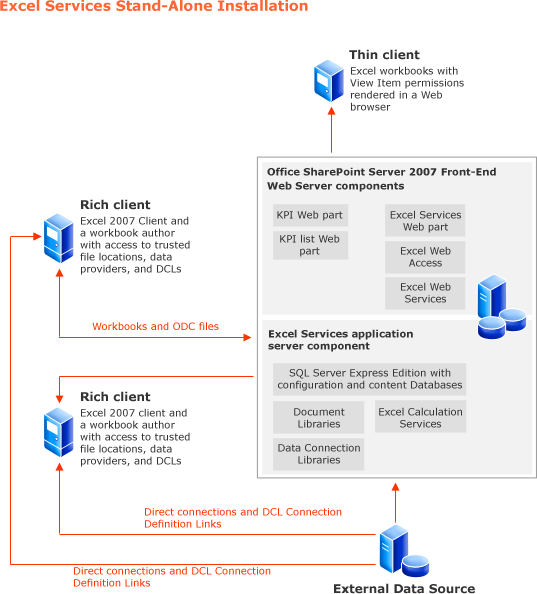
 [Excel Services extranet topology](#DSDOC_subsection8fb6928ce_49f8_492a_abff)

 [Excel Services corporate intranet topology](#DSDOC_subsection9fb6928ce_49f8_492a_abff)

 [Excel Services high-performance computing topology](#DSDOC_subsection10fb6928ce_49f8_492a_abf)

#### Excel Services single-server topology

The following topology diagram shows the logical architecture for a stand-alone Excel Services deployment on a single server.

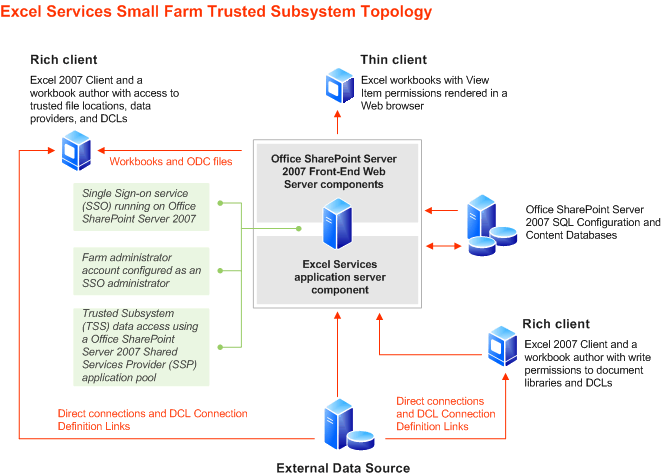


In this example, all Office SharePoint Server 2007 components are installed on a single computer. This includes the Excel Services front-end Web server components and Excel Calculation Services, the application server component of Excel Services. This also includes the configuration and content databases, which are installed by using Microsoft SQL Server Express Edition. This topology is useful for testing the core functionality of Excel Services, but it is not recommended as a scalable solution.

This configuration supports multiple Microsoft Windows SharePoint Services 3.0 Web applications by using Integrated Windows authentication. In this configuration, external data access can be provided by using data connection libraries, the Microsoft Single Sign-On service (SSO), or data connections embedded in workbooks. Load balancing is provided by the Excel Services load–balancing component. This topology uses the trusted subsystem data access method. The file access method is an Excel Calculation Services process account configured as an SSO administrator.

#### Excel Services small farm trusted subsystem topology

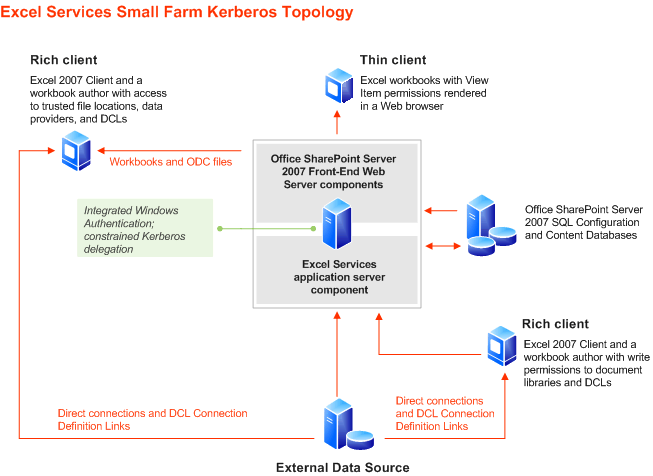
The following topology diagram shows the logical architecture for a small farm Excel Services deployment that uses the trusted subsystem data access model.



In this example, the Excel Services front-end Web server components and the application server component are installed on one server, and the SQL Server 2005 configuration and content databases are installed on a separate server. This configuration also shows the Single Sign-On service running on the Office SharePoint Server 2007 server. The configuration also shows the Excel Calculation Services process account configured as an SSO administrator.

#### Excel Services small farm Kerberos topology

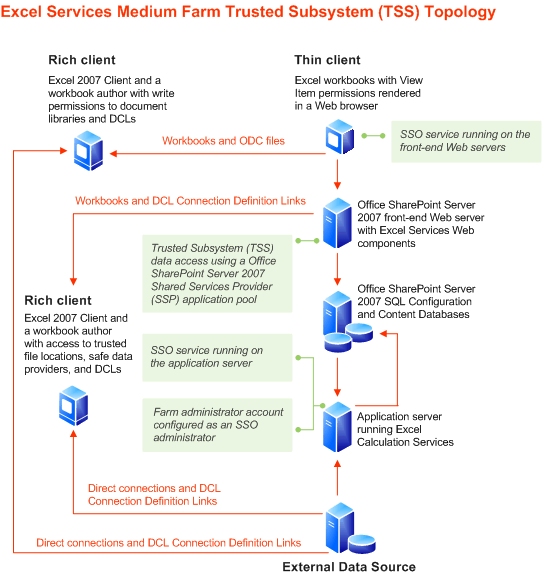
The following topology diagram shows the logical architecture for a small farm Excel Services deployment that uses the constrained Kerberos delegation data access model.



In this example, the Excel Services front-end Web server components and the application server component are installed on one server, and the SQL Server 2005 configuration and content databases are installed on a separate server. This configuration also shows the Single Sign-On service running on the Office SharePoint Server 2007 server. The configuration also shows the Excel Calculation Services process account configured as an SSO administrator.

#### Excel Services medium farm trusted subsystem topology

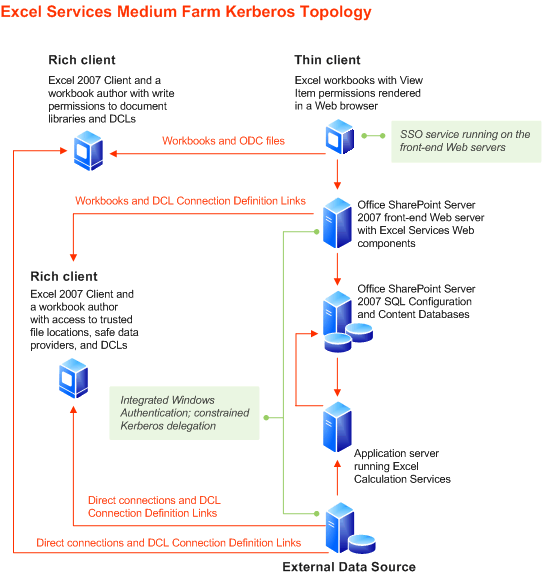
The following topology diagram shows the logical architecture for a medium farm Excel Services deployment that uses the trusted subsystem data access model.



In this example, the Excel Services front-end Web server components, the application server component, and the SQL Server 2005 configuration and content databases are installed on three separate servers. This configuration also shows the Single Sign-On service running on the Office SharePoint Server 2007 front-end Web server and on the Excel Services application server. The configuration also shows the Excel Calculation Services process account configured as an SSO administrator.

#### Excel Services medium farm Kerberos topology

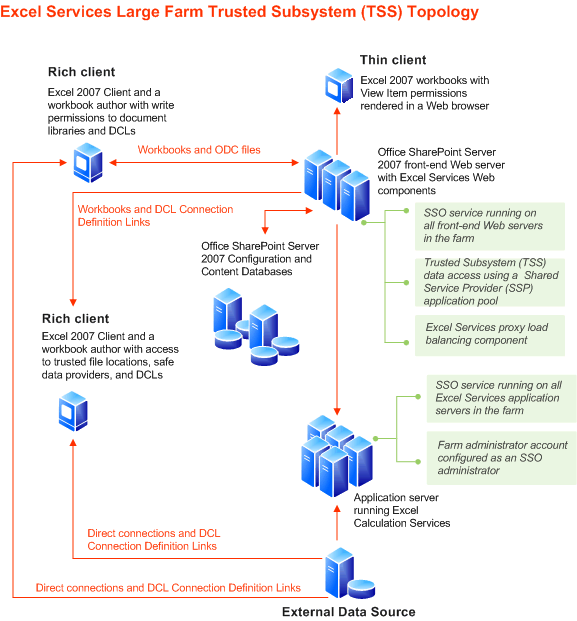
The following topology diagram shows the logical architecture for a medium farm Excel Services deployment that uses the constrained Kerberos delegation data access model.



In this example, the Excel Services front-end Web server components, the application server component, and the SQL Server 2005 configuration and content databases are installed on three separate servers. This configuration also shows the Single Sign-On service running on the Office SharePoint Server 2007 front-end Web server and on the Excel Services application server. The configuration also shows the Excel Calculation Services process account configured as an SSO administrator.

#### Excel Services large farm trusted subsystem topology

The following topology diagram shows the logical architecture for a large farm Excel Services deployment that uses the trusted subsystem data access model.



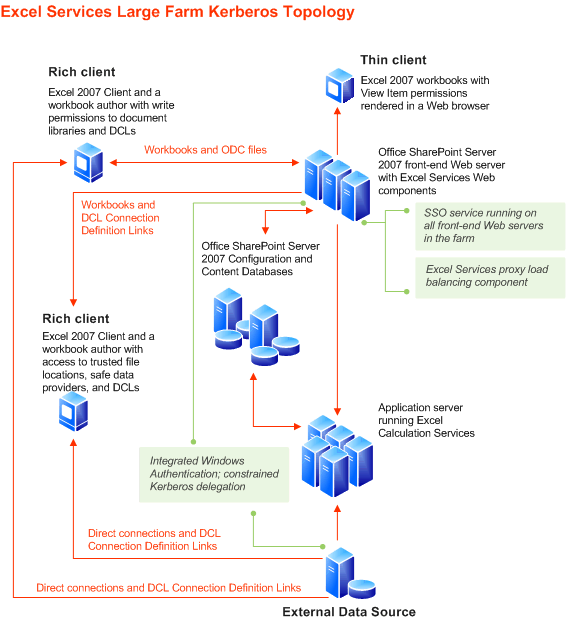
In this example, multiple Excel Services front-end Web server components, multiple application server components, and multiple SQL Server 2005 configuration and content databases are each installed on separate servers. This configuration also shows the Single Sign-On service running on the Office SharePoint Server 2007 front-end Web server and on the Excel Services application server. The configuration also shows the Excel Calculation Services process account configured as an SSO administrator.

important_ddImportant:

For large farm deployments, it is recommended to run Office SharePoint Server 2007 in a homogeneous environment. All of the servers in a large farm should run either a 32-bit version of Windows Server 2003 or a 64-bit version of Windows Server 2003. It is not recommended to run Office SharePoint Server 2007 in a mixed environment.

#### Excel Services large farm Kerberos topology

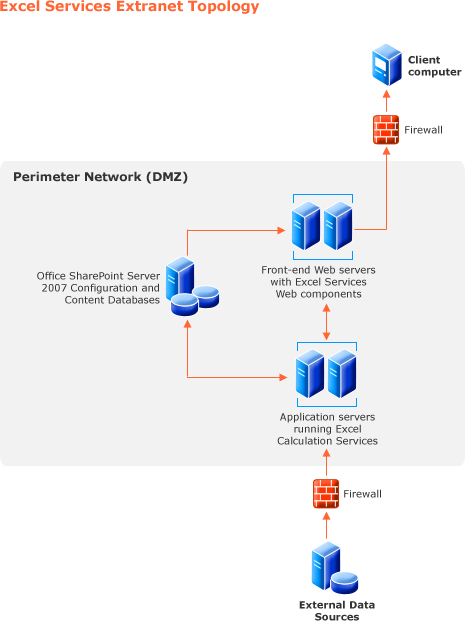
The following topology diagram shows the logical architecture for a large farm Excel Services deployment that uses the constrained Kerberos delegation data access model.



In this example, multiple Excel Services front-end Web server components, multiple application server components, and multiple SQL Server 2005 configuration and content databases are each installed on separate servers. This configuration also shows the Single Sign-On service running on the Office SharePoint Server 2007 front-end Web server and on the Excel Services application server. The configuration also shows the Excel Calculation Services process account configured as an SSO administrator.

#### Excel Services extranet topology

The following topology diagram shows the logical architecture for Excel Services front-end Web server components, application server components, and SQL Server 2005 configuration and content databases deployed in a perimeter network.



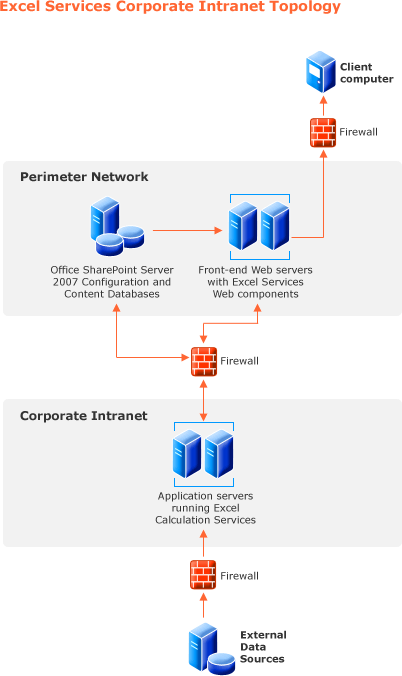
In this example, Excel Services components are isolated from external data sources and client computers in a secure perimeter network behind firewalls. This configuration provides enhanced security for data sources and helps prevent data corruption and unauthorized access to data.

note_ddNote:

If you have a Windows firewall enabled on the application servers, you must open the specific port on which the shared services Web site that hosts Excel Calculation Services is running.

#### Excel Services corporate intranet topology

The following topology diagram shows the logical architecture for an Excel Services deployment that isolates front-end Web server components and SQL Server 2005 configuration and content databases in a perimeter network that is separated from the corporate intranet. Excel Services application servers are deployed within the corporate intranet and all Excel Services components are isolated from remote client computers and from external data sources.



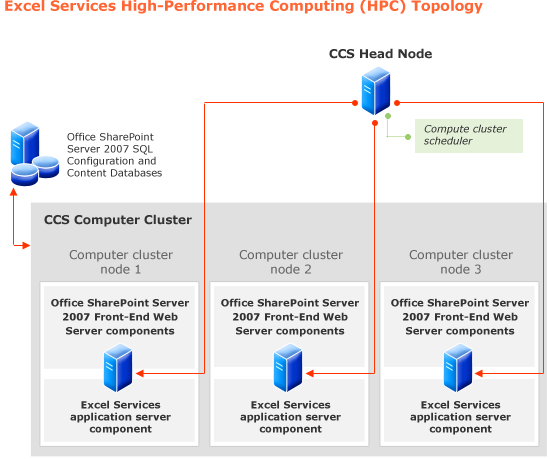
In this example, Excel Services application servers are deployed within the corporate network and are protected from direct external access. This configuration enables you to tightly control who can access your application servers and data. By isolating front-end Web servers in a perimeter network, you limit the attack surface of your environment to public-facing Web servers.

note_ddNote:

If you have a Windows firewall enabled on the application servers, you must open the specific port on which the shared services Web site that hosts Excel Calculation Services is running.

#### Excel Services high-performance computing topology

The following topology diagram shows the logical architecture for a deployment that includes Microsoft Windows Compute Cluster Server 2003 and Excel Services.



In this example, the Excel Services front-end Web server components and the application server component are installed on individual compute cluster nodes that comprise a compute cluster. These nodes share a SQL Server 2005 configuration and content database that runs on a server that is external to the compute cluster. A head node runs the compute cluster scheduler that schedules and load balances jobs among the nodes in the cluster.

## Plan for simultaneous client connections

The number of simultaneous client connections can impact the performance and availability of front-end Web servers. For a deployment designed to support a large number of client connections, you need to plan for the deployment of enough front-end Web servers to support an adequate level of system performance and availability. Determine the number of front-end Web servers that are required for your deployment scenario. Define baseline hardware requirements for system memory, CPU speed, and storage for each front-end Web server.

## Plan for concurrent Excel Calculation Services session requests

To determine the appropriate scale of a deployment to support Excel Calculation Services in Office SharePoint Server 2007, you need to know how many concurrent Excel Calculation Services session requests the scenario needs to support. For a deployment designed to support a large volume of Excel Calculation Services sessions, you need to plan for enough Excel Calculation Services servers to support an adequate level of performance and availability. Add Excel Calculation Services servers to improve performance and availability. Excel Calculation Services Proxy is a front-end Web server component used to load-balance session requests among the available application servers that run Excel Calculation Services.

You can configure a per-user session limit for application servers that run Excel Calculation Services. This value is the maximum number of concurrent sessions allowed for each user. Windows SharePoint Services 3.0 Web sites can be configured to allow anonymous user access. In this case, the Excel Calculation Services session limit for a single user will still apply. All anonymous users share the same session limit value that is configured for a single user.

The following configuration changes are recommended for an Excel Services environment that supports a large volume of Excel Calculation Services session requests and workbook calculations.

 IIS time-out   If calculations in Excel Services are expected to take longer than 110 seconds, increase the IIS time-out value. A ThreadAbort exception will occur when calculations exceed the IIS time-out setting. The default IIS time-out setting is 110 seconds.

 ASP.NET MaxConnection   When the number of client connection requests requires front-end Web servers to open multiple concurrent connections to application servers running Excel Calculation Services, you need to increase the maximum number of ASP.NET connections. In ASP.NET, configure the MaxConnection setting to a maximum connection limit of 10, as shown in the following example:

<configuration>

<system.net>

<connectionManagement>

<add address="\*" maxconnection="10" />

</connectionManagement>

</system.net>

<system.web>

Consider configuring the following Windows Server 2003 registry settings to improve Excel Calculation Services performance.

caution_ddCaution:

Incorrectly editing the registry might severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.

 HeapDeCommitFreeBlockThreshold   During a period when Excel Calculation Services application servers are experiencing a high volume of requests, the application servers might encounter performance issues caused by memory allocation failures. Because of memory fragmentation, this can occur even if application servers have adequate amounts of RAM installed to handle the volume of requests. To alleviate this problem, use the Registry Editor to change the HeapDeCommitFreeBlockThreshold setting to REG\_DWORD 0x00040000. To change the setting, use the following registry path:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager

 MaxUserPort   You might need to increase the range of available ports by changing the value of the MaxUserPort registry setting. The MaxUserPort setting specifies the highest port number that TCP can assign when an application requests an available user port from the system. To change this registry setting, run the Registry Editor and use the following registry path:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

 TcpNumConnections   You might need to increase the maximum number of connections that TCP can have open simultaneously by changing the value of the TcpNumConnections registry setting. If the TcpNumConnections registry key does not exist, run the Registry Editor to create and configure the key. To change this registry setting, run the Registry Editor and use the following registry path:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

 TcpTimedWaitDelay   During a period when Excel Calculation Services application servers are experiencing a high volume of requests, there is a possibility that some requests will be denied. If this occurs, you might be encountering a problem with the default setting of the TcpTimedWaitDelay registry key. By default, the TcpTimedWaitDelay setting is set to 240 seconds, or four minutes. This is the amount of time that must elapse before a closed TCP session can be released and the resources can be reassigned. To alleviate this problem, use the Registry Editor to change the TcpTimedWaitDelay setting from 240 seconds to 30 seconds. If the TcpTimedWaitDelay registry key does not exist, run the Registry Editor to create and configure the key by using the following registry path:

HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet\Services\Tcpip\Parameters

## Excel Services performance testing

The following performance test results provide guidance based on comparisons of throughput, response times, and resource utilization of Excel Services by using different topologies and data sets. These recommendations are also based on comparisons of performance factors by using different external data authentication schemes for online analytical processing (OLAP) and relational external data connections. Resource requirements and response times in Excel Services depend on workbook size, workbook complexity, the number of concurrent users, and external data latency. Tests are run by using a defined data set, and results vary depending on data set design.

The baseline configuration for each tested data set includes Office SharePoint Server 2007 dashboards, with each dashboard rendering two Excel Web Access Web Parts and two key performance indicator (KPI) Web Parts. The result is four Excel Calculation Services sessions for each page hit.

Twenty percent of the sessions are assumed to have some interactivity, such as paging or data refresh. The tests are based on the assumption that 5,000 users are actively accessing dashboards and portal KPIs linked to cells in Microsoft Office Excel 2007 workbooks.

### Hardware configuration

Performance testing was run on Office SharePoint Server 2007 front-end Web servers, Excel Calculation Services application servers, and Office SharePoint Server 2007 SQL Configuration and Content Database servers with the following hardware configurations:

|  |  |
| --- | --- |
| Servers | Hardware configuration |
| The Office SharePoint Server 2007 front-end Web servers | Two Dual-Core AMD Opteron 275 CPUs running at 2.2 GHz, with 9.83 GB RAM |
| The Excel Calculation Services application servers | Two Dual-Core AMD Opteron 275 CPUs running at 2.2 GHz, with 9.83 GB RAM |
| The Office SharePoint Server 2007 SQL Configuration and Content Database servers | Four Dual-Core AMD Opteron 880 CPUs running at 2.4 GHz, with 8 GB RAM |

### Data set attribute tables

This section provides information about the attributes of the data set and scenarios used for performance testing. Exceptions to these attributes are noted in individual configurations, as applicable. Excel Services performance depends on the attributes of the data set, including memory usage, CPU usage, throughput, and response time. It is important to consider the characteristics of your data set before using the performance test results provided here. The results you get will vary based on the data used in your environment, and other variables.

#### Performance test scenarios

The performance tests were run using the following test scenarios. The scenarios are based on an assumption of a total of 5000 users actively accessing dashboard pages and Excel workbooks, with Office Excel Web Access. The scenarios are also based on the assumption that a variety of dashboards are accessed with varying degrees of frequency. The tests include:

 A small number of dashboards that are accessed frequently by a large number of users.

 A large number of dashboards that are accessed infrequently by a small number of users.

This range of dashboard usage corresponds to an enterprise environment in which a small number of dashboards are used across the entire organization, and a large number of dashboards are used by groups within the organization.

|  |  |  |  |
| --- | --- | --- | --- |
| Number of users | Frequency of views | Number of dashboards | Number of workbooks |
| 3,750 | Twice a day | 5 | 10 |
| 1,500 | Three times a week | 25 | 24 |
| 1,000 | Once a week | 50 | 50 |
| 250 | Once a month | 150 | 40 |
| 150 | 30% of 1,000 files are viewed by users accessing Excel Web Access Web Parts | 300 | 25 |

#### Workbooks without external data connections

The workbooks in this scenario are not connected to an external data source. Resource consumption is determined by the size, complexity, the amount of formatting, and the number of calculations used in each workbook. Workbook size is determined by the number of rows and columns each workbook contains. All of these factors affect resource consumption and throughput in Excel Services. The workbooks include a range of features, such as formatting, conditional formatting, and charting. The dataset used includes a range of workbooks with the following attributes:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Percentage of workbooks | Rows | Columns | Percentage of calculations | Percentage of formatting | Volatile functions |
| 2% | <5,000 | 10 – 45 | 50% | 50% | Yes |
| 38% | <5,000 | 10 – 45 | 20% | 50% | No |
| 5% | <5,000 | 60 – 365 | 5% | 50% | No |
| 20% | 5,000 – 7,000 | 10 – 40 | 10% | 50% | No |
| 15% | 7,001 – 10,000 | 10 – 50 | 10% | 50% | No |
| 15% | 10,001 – 15,000 | 10 – 50 | 10% | 50% | No |
| 5% | 15,001 – 20,000 | 10 – 50 | 10% | 50% | No |

#### Workbooks with OLAP data connections

The workbooks in this scenario contain data connections to Analysis Services cubes. These workbooks include a range of features, such as formatting and conditional formatting. In addition to the variables that affect resource consumption and throughput in every scenario, the amount of Analysis Services data that is consumed by the workbooks in this scenario, and whether or not the workbooks are refreshed on open, can affect Excel Services performance. This scenario is based on the assumption that 15% of the workbooks have data connections that refresh on open. Caching has a major impact on the performance of external data connections. Typically, Excel Services uses cached data if there is a connection to an external data source, using the same credentials multiple times. Caching performance is also affected by the Excel Services External Data Cache Lifetime setting.

|  |  |  |  |
| --- | --- | --- | --- |
| Percentage | Rows | Row size | Other |
| 10% | <1,000 | 512 – 2,048 | DCL SSO (or Kerberos) |
| 20% | <1,000 | 512 – 2,048 | DCL SSO (or Kerberos), refresh on open |
| 40% | <1,000 | 100 – 512 | One to four PivotTables and one to four PivotCharts embedded in workbooks |
| 20% | <1,000 | <100 | Four to six PivotTables and four to six PivotCharts embedded in workbooks |
| 10% | 1,000 – 5,000 | <100 | Two PivotTables and two PivotCharts embedded in workbooks |

#### Workbooks with relational data connections

The workbooks in this scenario contain data connections to SQL Server relational databases. These workbooks include a range of features, such as formatting and conditional formatting. In addition to the variables that affect resource consumption and throughput in every scenario, whether or not the workbooks are refreshed on open can affect Excel Services performance in this scenario. This scenario is based on the assumption that 15% of the workbooks have data connections that refresh on open. Caching has a major impact on the performance of external data connections. Typically, Excel Services uses cached data if there is a connection to an external data source, using the same credentials multiple times. Caching performance is also affected by the Excel Services External Data Cache Lifetime setting.

|  |  |  |  |
| --- | --- | --- | --- |
| Percentage | Rows | Row size | Other |
| 2% | <1,000 | <512 | DCL SSO (or Kerberos), periodic refresh |
| 20% | <500 | <512 | DCL SSO (or Kerberos), refresh on open |
| 40% | 1,001 – 5,000 | 1024 – 2,048 | One or two PivotTables and one or two PivotCharts embedded in workbooks |
| 20% | 5,000 – 10,000 | 1024 – 2,048 | DCL SSO; one or two PivotTables and one or two PivotCharts embedded in workbooks |
| 10% | 10,000 – 20,000 | 512 – 1,024 | DCL SSO; two to four PivotTables and two to four PivotCharts embedded in workbooks |
| 8% | 20,000 – 65,000 | <512 | DCL SSO; one or two PivotTables embedded in workbooks |

#### Distribution of workbooks by data sources

Performance tests were run using the following distribution of workbooks. Exceptions to this distribution are noted for some of the configurations. In each configuration, workbooks were distributed based on the percentages shown in the data set attribute tables. For Example, 30% of the workbooks contained no external data. Of these, 20% had between 5000 and 7000 rows, as shown in the Workbooks without external data connections table. This resulted in 6% of the total workbook distribution (20% of 30%), consisting of workbooks with no external data and containing between 5000 and 7000 rows. Some of the configurations isolate workbooks of a specific type. For example, workbooks containing OLAP data connections configured to refresh on open.

|  |  |
| --- | --- |
| Workbook type | Percentage |
| Workbooks with no external data | 30% |
| Workbooks with OLAP data connections | 35% |
| Workbooks with relational data connections | 35% |

#### Request mix used in performance tests

Performance tests were run using the following request mix. There are exceptions to this request mix. For example, in tests using workbooks with no external data, there are no interactive operations with external data queries. Exceptions are noted for some of the configurations.

|  |  |
| --- | --- |
| Request type | Percentage of total requests |
| OpenWorkbook (includes one GetRange) | 65% |
| Interactive requests with external data queries | 15% |
| GetRange (paging) | 10% |
| Find, Sort, and Filter interactive requests within workbooks | 10% |

### Performance test results

The tables in this section show test results for each tested configuration.

#### Excel Services small farm trusted subsystem configuration

The following table shows the data set for this configuration.

|  |  |
| --- | --- |
| Workbook type | Percentage |
| Workbooks with no external data | 30% |
| Workbooks with OLAP data connections | 35% |
| Workbooks with relational data connections | 35% |

The following table shows front-end Web server test results for this configuration:

|  |  |
| --- | --- |
| Performance counter | Result |
| Requests per second | 14.32 |
| Average response time in seconds | 5.52 |
| ASP.NET queue | 1.91 |
| CPU | 41.97 |
| W3wp process private bytes | 822 |

The following table shows Excel Calculation Services application server test results for this configuration:

|  |  |
| --- | --- |
| Performance counter | Result |
| Requests per second | 15.52 |
| Average response time in seconds | 2.05 |
| Sessions per second | 2.94 |
| ASP.NET queue | 1.91 |
| CPU | 41.97 |
| W3wp process private bytes | 3844 |

#### Excel Services large farm trusted subsystem configuration

The following table shows the data set for this configuration.

|  |  |
| --- | --- |
| Workbook type | Percentage |
| Workbooks with no external data | 30% |
| Workbooks with OLAP data connections | 35% |
| Workbooks with relational data connections | 35% |

The following table shows front-end Web server test results for this configuration.

|  |  |  |  |
| --- | --- | --- | --- |
| Performance counter | Front-end Web server 1 | Front-end Web server 2 | Front-end Web server3 |
| Requests per second | 4.62 | 4.54 | 4.63 |
| Average response time in seconds | 10 | 9.69 | 10.01 |
| ASP.NET queue | 0.12 | 0.2 | 0.25 |
| CPU | 1.13 | 1.21 | 1.21 |
| W3wp process private bytes | 738 | 713 | 742 |

The following table shows Excel Calculation Services application server test results for this configuration.

|  |  |
| --- | --- |
| Performance counter | Result |
| Requests per second | 14.8 |
| Average response time in seconds | 4.74 |
| Sessions per second | 2.58 |
| ASP.NET queue | 33.29 |
| CPU | 37.84 |
| W3wp process private bytes | 3867 |

#### Excel Services large farm Kerberos configuration

The following table shows the data set for this configuration.

|  |  |
| --- | --- |
| Workbook type | Percentage |
| Workbooks with no external data | 30% |
| Workbooks with OLAP data connections | 35% |
| Workbooks with relational data connections | 35% |

The following table shows front-end Web server test results for this configuration.

|  |  |  |  |
| --- | --- | --- | --- |
| Performance counter | Front-end Web server 1 | Front-end Web server 2 | Front-end Web server3 |
| Requests per second | 15.39 | 15.36 | 15.58 |
| Average response time in seconds | 4.48 | 4.3 | 4.35 |
| ASP.NET queue | 0.46 | 0.5 | 0.45 |
| CPU | 4.43 | 4.33 | 4.36 |
| W3wp process private bytes | 906 | 909 | 899 |

The following table shows Excel Calculation Services application server test results for this configuration.

|  |  |
| --- | --- |
| Performance counter | Result |
| Requests per second | 46.36 |
| Average response time in seconds | 1.36 |
| Sessions per second | 9.43 |
| ASP.NET queue | 63.55 |
| CPU | 54.82 |
| W3wp process private bytes | 6387 |

#### Excel Services large farm trusted subsystem configuration using OLAP data with refresh on open and SSO

The following table shows the data set for this configuration.

|  |  |
| --- | --- |
| Workbook type | Percentage |
| Workbooks with OLAP data connections; refresh on open; uses SSO for external data authentication | 100% |

The following table shows front-end Web server test results for this configuration:

|  |  |  |  |
| --- | --- | --- | --- |
| Performance counter | Front-end Web server 1 | Front-end Web server 2 | Front-end Web server3 |
| Requests per second | 1.84 | 1.83 | 1.85 |
| Average response time in seconds | 7.6 | 7.5 | 8.07 |
| ASP.NET queue | 0.001 | 0.001 | 0 |
| CPU | 0.59 | 0.61 | 0.62 |
| W3wp process private bytes | 379 | 375 | 384 |

The following table shows Excel Calculation Services application server test results for this configuration:

|  |  |
| --- | --- |
| Performance counter | Result |
| Requests per second | 6.52 |
| Average response time in seconds | 3.82 |
| Sessions per second | 1.08 |
| ASP.NET queue | 1.22 |
| CPU | 45.29 |
| W3wp process private bytes | 4995 |

#### Excel Services large farm Kerberos configuration using OLAP data with refresh on open

The following table shows the data set for this configuration.

|  |  |
| --- | --- |
| Workbook type | Percentage |
| Workbooks with OLAP data connections; refresh on open; uses Kerberos for external data authentication; user credentials are delegated for authentication with OLAP data sources | 100% |

The following table shows front-end Web server test results for this configuration.

|  |  |  |  |
| --- | --- | --- | --- |
| Performance counter | Front-end Web server 1 | Front-end Web server 2 | Front-end Web server3 |
| Requests per second | 0.99 | 1 | 0.99 |
| Average response time in seconds | 19.29 | 18.32 | 19.36 |
| ASP.NET queue | 0.001 | 0 | 0.001 |
| CPU | 0.41 | 0.41 | 0.38 |
| W3wp process private bytes | 417 | 431 | 425 |

The following table shows Excel Calculation Services application server test results for this configuration.

|  |  |
| --- | --- |
| Performance counter | Result |
| Requests per second | 2.95 |
| Average response time in seconds | 17.39 |
| Sessions per second | 0.59 |
| ASP.NET queue | 11.63 |
| CPU | 54.8 |
| W3wp process private bytes | 10419 |

#### Excel Services large farm Kerberos configuration using SQL Server 2005 Analysis Services groups

The following table shows the data set for this configuration.

|  |  |
| --- | --- |
| Workbook type | Percentage |
| Workbooks with OLAP data connections; refresh on open, using Kerberos for external data authentication; user credentials are delegated for authentication with OLAP data sources; users map to SQL Server 2005 Analysis Services groups | 100% |

The following table shows front-end Web server test results for this configuration.

|  |  |  |  |
| --- | --- | --- | --- |
| Performance counter | Front-end Web server 1 | Front-end Web server 2 | Front-end Web server3 |
| Requests per second | 8.7 | 8.38 | 8.62 |
| Average response time in seconds | 3.63 | 3.69 | 3.7 |
| ASP.NET queue | 0.004 | 0.004 | 0.006 |
| CPU | 2.31 | 2.31 | 2.3 |
| W3wp process private bytes | 435 | 431 | 452 |

The following table shows Excel Calculation Services application server test results for this configuration.

|  |  |
| --- | --- |
| Performance counter | Result |
| Requests per second | 25.67 |
| Average response time in seconds | 1.69 |
| Sessions per second | 5.22 |
| ASP.NET queue | 2.73 |
| CPU | 63.07 |
| W3wp process private bytes | 7850 |

#### Excel Services large farm trusted subsystem configuration using relational data

The following table shows the data set for this configuration.

|  |  |
| --- | --- |
| Workbook type | Percentage |
| Workbooks with relational data connections; refresh on open, using SSO for external data authentication | 100% |

The following table shows front-end Web server test results for this configuration.

|  |  |  |  |
| --- | --- | --- | --- |
| Performance counter | Front-end Web server 1 | Front-end Web server 2 | Front-end Web server3 |
| Requests per second | 24.07 | 24.2 | 24.6 |
| Average response time in seconds | 3.17 | 3.16 | 3.15 |
| ASP.NET queue | 9.15 | 10.41 | 13.77 |
| CPU | 6.49 | 6.65 | 6.78 |
| W3wp process private bytes | 959 | 965 | 1062 |

The following table shows Excel Calculation Services application server test results for this configuration.

|  |  |
| --- | --- |
| Performance counter | Result |
| Requests per second | 76.16 |
| Average response time in seconds | 0.43 |
| Sessions per second | 14.84 |
| ASP.NET queue | 17.79 |
| CPU | 46.62 |
| W3wp process private bytes | 35.88 |

#### Excel Services large farm Kerberos configuration using relational data

The following table shows the data set for this configuration.

|  |  |
| --- | --- |
| Workbook type | Percentage |
| Workbooks with relational data connections; refresh on open, using constrained Kerberos delegation for external data authentication | 100% |

The following table shows front-end Web server test results for this configuration.

|  |  |  |  |
| --- | --- | --- | --- |
| Performance counter | Front-end Web server 1 | Front-end Web server 2 | Front-end Web server3 |
| Requests per second | 22.78 | 22.6 | 23.1 |
| Average response time in seconds | 3.03 | 2.97 | 2.98 |
| ASP.NET queue | 0.59 | 0.5 | 0.39 |
| CPU | 6.18 | 6.15 | 6.16 |
| W3wp process private bytes | 836 | 838 | 843 |

The following table shows Excel Calculation Services application server test results for this configuration.

|  |  |
| --- | --- |
| Performance counter | Result |
| Requests per second | 68.41 |
| Average response time in seconds | 0.74 |
| Sessions per second | 13.87 |
| ASP.NET queue | 21.46 |
| CPU | 55.87 |
| W3wp process private bytes | 6328 |

## Limit the number and duration of open sessions

In addition to adding resources, limiting the number of open Excel Calculation Services sessions can help mitigate performance and availability issues. One way to limit the number of open Excel Calculation Services sessions is to decrease session time-out settings. Indiscriminately limiting session duration can cause active sessions to close, which can result in data loss.

The preferred solution is to use Office Excel Web Access Short Session Mode to configure shorter initial time-out settings for sessions that have no client-side interactivity when the sessions are opened. You can configure a second time-out setting for sessions that are active as soon as they are opened. In this example, sessions that remain inactive for the duration of the initial time-out setting are closed by the Excel Calculation Services server. Sessions that are active before the initial time-out setting expires will remain open until the second time-out setting expires.

## [[14]](#footnote-15)#See Also

[Microsoft Windows Compute Cluster Server 2003](http://go.microsoft.com/fwlink/?LinkID=76334&clcid=0x409)

# Plan rendering Excel KPI data

In this article:

 [About rendering Excel KPI data](#DSDOC_section1ff3ee313_7293_4611_b9ab_17)

 [KPI List Web Parts for Office SharePoint Server 2007](#DSDOC_section2ff3ee313_7293_4611_b9ab_17)

 [Excel KPI and SQL Server 2005 Analysis Services](#DSDOC_section3ff3ee313_7293_4611_b9ab_17)

## About rendering Excel KPI data

In Microsoft Office SharePoint Server 2007, data in Microsoft Office Excel 2007 spreadsheets can be rendered in individual key performance indicator (KPI) List Web Parts or aggregated into a dashboard on a SharePoint site. A dashboard is a page that contains a set of Web Parts. A dashboard might be a KPI list made up of multiple KPI List Web Parts. Each Web Part can render data derived from several different Excel spreadsheets, or from multiple data objects within the same spreadsheet.

## KPI List Web Parts for Office SharePoint Server 2007

Office SharePoint Server 2007 includes a new KPI List Web Part. This new Web Part is designed to render the current status of volatile data in a way that can be easily understood in business terms. By using KPIs, users can monitor the status and trends of important business measurements as they occur. KPIs can be used to abstract large amounts of data and render the data as easily understood icons.

## Excel KPI and SQL Server 2005 Analysis Services

Microsoft SQL Server 2005 Analysis Services is a source for data that Excel Services renders as KPIs. When a server that runs SQL Server 2005 Analysis Services is deployed and populated with business data, the server functions as a Unified Dimensional Model (UDM) to which Excel Services can connect. The UDM is a logical layer between reporting applications and back-end data sources. The UDM layer can be designed to render data in business terms and make it easier for users to create reports.

The data that Excel Services consumes from a SQL Server 2005 Analysis Services server can be formatted on the server by a UDM designer. The UDM designer can set server-based conditional formatting rules that can be implemented to draw attention to values that compromise the integrity of a database, such as a negative balance or any other values that violate business rules. The UDM designer can also set up visual status and trend indicators that help users quickly understand rendered KPI data in business terms.

# Plan Excel reports against OLAP cubes

In this article:

 [About building Excel reports against OLAP cubes](#DSDOC_section1bbaa06e5_a953_4637_9114_bd)

 [OLAP functions](#DSDOC_section2bbaa06e5_a953_4637_9114_bd)

 [OLAP formulas](#DSDOC_section3bbaa06e5_a953_4637_9114_bd)

## About building Excel reports against OLAP cubes

You can use the new Microsoft Office Excel 2007 online analytical processing (OLAP) functions and formulas to create highly customizable reports and analytic models that can be automatically updated to include the most current business data from external data sources.

## OLAP functions

By using the new Office Excel 2007 OLAP functions, you can use an Office Excel 2007 spreadsheet as a reporting surface for data from OLAP cubes. You can use the following OLAP functions to import Microsoft SQL Server 2005 Analysis Services data directly into Office Excel 2007 spreadsheet cells for unstructured data analysis:

 CUBEMEMBER   Sends a Multidimensional Expression (MDX) to an OLAP cube and fetches a member or tuple.

 CUBEVALUE   Sends one or more MDX to an OLAP cube and fetches an aggregated value.

 CUBESET   Sends an MDX to an OLAP cube that defines a set in the cube and places the set in a spreadsheet cell.

 CUBESETCOUNT   Returns the number of elements in a set.

 CUBERANKEDMEMBER   Fetches the Nth item in a set.

 CUBEMEMBERPROPERTY   Returns a member property value from an OLAP cube.

 CUBEKPIMEMBER   Returns a key performance indicator (KPI) goal, value, status, or trend from an OLAP cube.

## OLAP formulas

Excel OLAP formulas provide an additional way to display SQL Server 2005 Analysis Services data in Office Excel 2007 spreadsheets. By using Excel OLAP formulas, you can build reports with greater control of data placement than is possible by using PivotTable reports. In addition, you can use Excel OLAP formulas to write custom MDXs into a report.

# Plan access to Excel spreadsheets

In this article:

 [About spreadsheet management](#DSDOC_section193f576a4_e549_4675_b083_7f)

 [Plan a strategy to control access to workbooks and ensure data integrity](#DSDOC_section293f576a4_e549_4675_b083_7f)

 [Plan a strategy to restrict access to individual data objects within workbooks](#DSDOC_section393f576a4_e549_4675_b083_7f)

## About spreadsheet management

By using Excel Services, you can control access to workbook data while ensuring data integrity. You can use Excel Calculation Services to enforce centralized management of proprietary information, maintain one version of the truth for Microsoft Office Excel 2007 workbooks, and control how and to whom workbook data is made available based on user permissions.

Depending on the type of access permitted, you can restrict users to View Only permissions, allowing them to view snapshots of workbooks without being able to alter any data in Office Excel 2007. Workbooks that have View Only restrictions still allow users to open, interact with, refresh, and recalculate workbooks in a Web browser. You can also grant open permission to users, which allows them to access and update workbooks.

## Plan a strategy to control access to workbooks and ensure data integrity

By configuring View Only permissions, you can ensure that Excel workbooks are only rendered in a Web browser. Users who have View Only permissions can be restricted to opening a snapshot of the workbook in Office Excel 2007.

In Microsoft Office SharePoint Server 2007, you can configure View Only permissions and access restrictions to document libraries in a SharePoint site. This enables you to restrict the availability of workbook data to users who have authenticated access to the site.

## Plan a strategy to restrict access to individual data objects within workbooks

Access to selected data objects within a workbook, such as PivotTable components and charts, can be controlled independently from the rest of the workbook when the workbook is published to an application server that runs Excel Calculation Services. The view of the workbook in Excel Services, when rendered in a Web browser, is always the published view, which might be limited to the server-viewable items in the workbook.

Users who have View Only permissions will be able to open only a snapshot of the published items. Users who have full permissions will be able to open the full workbook, including items that have not been designated server viewable.

# Plan for business data connections with the Business Data Catalog

In this article:

 [About the Business Data Catalog](#DSDOC_section1c803c1fa_cb0f_4a26_b439_de)

 [Plan connections to the Business Data Catalog](#DSDOC_section2c803c1fa_cb0f_4a26_b439_de)

 [Plan business data presentation](#DSDOC_section3c803c1fa_cb0f_4a26_b439_de)

 [Worksheets](#DSDOC_section4c803c1fa_cb0f_4a26_b439_de)

The Business Data Catalog is used to connect data from line-of-business applications that have managed properties used by enterprise search in Microsoft Office SharePoint Server 2007. After applications are registered in the Business Data Catalog, the business data types and properties selected by administrators can be used in SharePoint sites, SharePoint lists, and relevant business data Web Parts. These sites, lists, and Web Parts can then be used to analyze and act on business data.

The line-of-business data used by the Business Data Catalog can combine with the core business intelligence functionality of Microsoft SQL Server 2005 Analysis Services and SQL Server 2005 Reporting Services, Excel Services, and key performance indicators (KPIs) based on data sources in data connection libraries. The result is an integrated view of business data and business processes across your organization.

As part of planning for your initial deployment Office SharePoint Server 2007, you should understand how to connect applications to the Business Data Catalog and how to present that data in sites, lists, and Web Parts. Then, you can plan for more specific features that use business data, such as business data profiles, business data actions, reports, and dashboards. Together these plans form a comprehensive deployment plan that you can use along with planning worksheets during the initial deployment of Office SharePoint Server 2007.

## About the Business Data Catalog

The Business Data Catalog is a service for registering line-of-business applications and certain business data types and properties of those applications. The Business Data Catalog is managed from the Shared Services Administration page for each Shared Services Provider (SSP). For each line-of-business application used by the Web applications and site collections of an SSP, you must first register the line-of-business application and the business data types and properties that you want to expose to users.

After registering applications in the Business Data Catalog, you can decide how to present and use the data of those applications in sites, lists, and Web Parts. Properties in the Business Data Catalog appear in business data profiles and can be used in business data lists and Web Parts, or in filter Web Parts that filter the view of business data Web Parts. These Web Parts can then be used in building SharePoint sites, including reports and dashboards, that display business data. You can find data by crawling properties of business data as part of business data content sources. As with any other crawled properties, the crawled properties of business data are mapped to managed properties for search, and those properties are used during queries to prioritize relevant search results. Properties about users can be associated with properties in user profiles imported by profile services from directory services, such as the Active Directory directory service or Lightweight Directory Access Protocol (LDAP) directory services, or added as additional properties of user profiles.

By using line-of-business data in your SharePoint sites, you can integrate data analysis from these sites with data analysis based on data connection libraries. This allows you to build knowledge about your key business processes, make decisions, and act on those decisions.

For example, a sales department for a large organization uses a line-of-business application that tracks products, sales associates, customers, sales offices, and individual sales. The SSP administrator registers the applications, along with relevant business data types for products, customers, and sales offices. For each of these business data types, the SSP administrator includes relevant properties. For example, for customers, the properties for location, address, description, and purchasing manager are included.

You can create a business data list from sales data in a data connection library, and you can add columns for properties registered in the Business Data Catalog. This list of customers and sales can then be used in business data Web Parts used by reports, so you can compare sales across customers in the Report Center site. By mapping the relevant properties to managed properties in search, someone searching for a specific location where a customer is located will find that customer near the top of search results.

## Plan connections to the Business Data Catalog

Start the plan for the Business Data Catalog by considering the line-of-business applications used by your organization. Large databases and data warehouses will typically be accessed by using data connection libraries, and not the Business Data Catalog. The Business Data Catalog is the place to register line-of-business applications.

For each application, it is important to consider the following factors:

 Properties that will be helpful in analyzing business processes and making business decisions.

 Properties that are less relevant or contain data that you do not want to display widely in your organization.

 Sites that will use business data, such as reports, dashboards, and personalization sites.

 Web Parts that are used by SharePoint sites that have business data, including Business Data List Web Parts and KPI Web Parts.

 Lists you need to build business data Web Parts.

 Business data actions you want to create and the properties those actions are based on.

 Properties you expect users to use when searching for business data.

The details of planning properties of business data profiles, business data lists and Web Parts, business data actions, and the properties for searching for business data are described in greater detail in other articles. When you plan for the connections to the Business Data Catalog, it is important to first focus on which applications to connect and how to make those connections.

You should consider that most users in your organization will not have direct access to the line-of-business applications. This is a good idea for several reasons. Some data might be sensitive and not all data in the application will be displayed in sites, lists, and Web Parts. You also want to limit the performance impact on the servers that host line-of-business applications. For these reasons, a common practice is to copy data in a line-of-business application to another server, and then use that location in the Business Data Catalog and business data content sources.

To further limit access to the data, it is a good idea to use a single account or a group that contains a small number of accounts both for accessing the business data in the application and for crawling the data for search. In the case of search, it is a good idea to create a crawl rule for business data applications that uses the administration account for each line-of-business application as the crawling account for each business data start address.

After applications are connected, all included business data types and properties can be used in sites, lists, and Web Parts by any users who have the appropriate permissions. Typically, site collection administrators will create a SharePoint group for viewing business data and include users who have responsibilities to analyze and act on business data. Often, users will act on business data by making business decisions that are not directly involved with the application itself. If acting on data requires changing the data in the underlying database, each user can make changes based on their permissions to the relevant database.

For business data actions that use forms hosted by InfoPath Forms Services, the proper security settings must be configured according to plans for InfoPath Forms Services, so that users who use the forms can expect the data to be updated in the underlying application and not just a duplicated location used by the Business Data Catalog.

If a duplicated location is used, it is a good idea to plan for how often the data in that location is synchronized with the line-of-business data on the application server.

After you decide who has access to data and which applications you want to register, you should consider which business data types and properties to include. The simple rule to use is that if you want users in your organization to analyze data based on a set of business data types, those business data types should be included in the Business Data Catalog.

As you plan for the initial deployment, start with the business data types that you know are most likely to be analyzed by users in your organization, based on the purpose and key business processes of your sites. Include those business data types and plan for the properties that are most likely to produce useful results. For example, for a customer service site, it makes sense to include business data types for customers and for sales associates, enabling users that have the appropriate business data permissions to view and compare sales across customers or sales associates and make business decisions based on the results.

|  |
| --- |
| Worksheet action |
| Use the [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) to record each connected application and the relevant business data types and properties, along with the accounts that have permission to the application server, any server that contains a copy of data that is used by the Business Data Catalog, and the accounts that are members of SharePoint groups that have access to the data in the Business Data Catalog.  For data sources based on SQL Server databases and other relational databases that will be stored in data connection libraries, record the planned data source and the relevant business data types and properties used by SQL Server 2005 Analysis Services and SQL Server 2005 Reporting Services when analyzing and displaying the data. |

For more information about the business data types and properties used in the Business Data Catalog, see [Plan for business data profiles](#DSDOC_560cb26b_f530_464e_ab9f_f506df8d8d).

## Plan business data presentation

After you have connected line-of-business applications and the data for relevant business data types and properties to the Business Data Catalog, you can consider how you will present that data in the organization so that it can be used in data analysis, collaboration, and business decision-making.

You should consider the business data that you want for each site in your planned site structure. Based on the purpose of each planned site, you can identify the applications, business data types, and properties to use in building the business data lists and Web Parts used in each site. After you ensure that the relevant data is available in the Business Data Catalog, you can plan the relevant Web Parts and SharePoint lists used by each site.

|  |
| --- |
| Worksheet action |
| Use the [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) to record the KPIs, reports, and business data lists and Web Parts based on each data source, and add the properties used by each list or Web Part. For KPIs, record the planned calculation method and the targets for each indicator level of the KPI. |
| Use the [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) to record the sites that use business data applications for your site collection hierarchy and for each site collection. Also record the business data Web Parts and SharePoint lists that are used for each site. |

For more information about planning business data in personalization sites or sites that use targeted Web Parts, see [Plan My Sites](#DSDOC_4edf74cf_8808_4277_ba10_b1f925d7c4).

For more information about planning business data in SharePoint lists, see [Plan business data lists](#DSDOC_10008f02_d602_4749_b89a_15f7406aea).

For more information about planning business data Web Parts, see [Plan business data Web Parts](#DSDOC_165f1afe_11e5_4c45_8f93_bf16e18338).

For more information about planning business data actions, see [Plan business data actions](#DSDOC_60b8a5be_c54e_488c_90b0_80f4aeba40).

For more information about planning business data search, see [Plan for business data search](#DSDOC_2b7121fc_a1f2_469d_ac1c_7b12283897).

## Worksheets

Use the following worksheets to plan for business data connections with the Business Data Catalog:

 [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409)

 [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409)

# Plan for business data profiles

In this article:

 [About business data profiles](#DSDOC_section1560cb26b_f530_464e_ab9f_f5)

 [Plan connections to the Business Data Catalog](#DSDOC_section2560cb26b_f530_464e_ab9f_f5)

 [Plan to include business data content sources](#DSDOC_section3560cb26b_f530_464e_ab9f_f5)

 [Plan properties of business data profiles](#DSDOC_section4560cb26b_f530_464e_ab9f_f5)

 [Worksheets](#DSDOC_section5560cb26b_f530_464e_ab9f_f5)

Good planning for business data profiles can transform a site collection from a place where users collaborate on documents and link to content and sites that support that content to a place where users can easily interact dynamically with key business data that is synchronized between the Web browser and underlying data sources.

As part of planning your initial deployment of Microsoft Office SharePoint Server 2007, you should understand which business data applications you want to connect to the Business Data Catalog, and which business data types and properties of those applications you want to make available in Office SharePoint Server 2007. Then, you can use these plans during your initial deployment of Office SharePoint Server.

## About business data profiles

Business data profiles describe the properties of every important person, organization, product, business location, or any other type of data tracked by your business applications. You can create profiles for all types of data, depending on the needs of your organization and the purpose of each site collection you plan. The properties of business data profiles are also used by other features of Office SharePoint Server 2007.

## Plan connections to the Business Data Catalog

The Business Data Catalog is a service that exposes data from enterprise applications to Microsoft Windows SharePoint Services 3.0 and Office SharePoint Server 2007. The Business Data Catalog can be used by multiple site collections in one or more server farms. Each line-of-business application is represented by a Web application instance that contains its data in the Shared Services Provider (SSP), consolidated into a single Business Data Catalog for all business data.

The Business Data Catalog enables line-of-business applications to make data available as Office SharePoint Server 2007 properties. These properties can be used in lists, Web Parts (including reports and multi-report summaries, such as dashboards), and key performance indicators (KPIs) created from business data lists. These properties can also be used as metadata for search, user and business data profiles, and custom Web applications. Examples of line-of-business applications include:

 SAP Business Information Warehouse or mySAP ERP

 Siebel eBusiness Applications

 Attunity Legacy Data Access Solutions

 Microsoft BizTalk Server

The Business Data Catalog can also recognize properties from database servers, such as Microsoft SQL Server and Oracle, and properties from Excel Calculation Services. Application data can be managed interactively by using business data actions, often by using Microsoft Office InfoPath 2007 forms.

Before you can use data from line-of-business applications in business data profiles and other features of Office SharePoint Server 2007, you must perform the following steps:

1. Register the application in the Business Data Catalog.

2. Map the application properties to properties in the site collection and SSP schema.

3. Create and crawl the content source for the business data application.

## Plan to include business data content sources

You can create content sources to crawl business data. The properties of business data profiles are updated whenever a content source that contains the location of the business application is crawled. For more information about crawling business data, see [Plan for business data connections with the Business Data Catalog](#DSDOC_c803c1fa_cb0f_4a26_b439_de7ff4195e).

## Plan properties of business data profiles

Business data profiles are created when an application is registered in the Business Data Catalog. Business data profiles are created for every business data type in a business application that the SSP administrator chooses to display. Copies of these profiles exist for every site collection that uses the same SSP.

Business data profiles are similar to user profiles in that they contain a set of properties and associated values. The properties of each profile are crawled by the SSP and are then available for use in search queries and business data features of Office SharePoint Server 2007.

In addition to the properties of business data types, business data profiles include links for all business data actions that have been created for the application. For more information, see [Plan business data actions](#DSDOC_60b8a5be_c54e_488c_90b0_80f4aeba40).

The properties of business applications in the Business Data Catalog should be considered as part of your overall information architecture planning. Based on the purpose of each site collection, decide whether it will need to use each business application.

After you identify site collections that will use data from business applications, think about which features used by each site collection will use that data, and how data will be used across the SSP. Examples of types of data that might be used by your organization within each site collection include:

 Users, such as customers, employees, and business partners.

 Organizations that might also be customers, partners, internal groups or divisions, and other groups associated with the data in one of your organization's core business applications.

 Places, such as different sales regions.

 Products or services provided by your organization.

Many business applications track these types of data. Importing that data into the Business Data Catalog as business data types with business data profiles is relatively simple. The important planning considerations include:

 Which properties to include during import.

 How those properties are displayed in the business data profile.

 How those properties are displayed in other features that depend on the properties of business data.

Only SSP administrators can view the properties in the business data profiles in the Business Data Catalog. However, anyone else can view the business data profile for each business data type by clicking a link to that business data type in a business data list or Web Part. For example, in a list of recent customer transactions, clicking the name of the customer displays the profile for that customer, including the customer's name, address, telephone number, and e-mail address. Similarly, clicking the product name within the same list displays a profile for the product that contains its name, description, and price.

The properties of business data profiles can be displayed in the following additional ways:

 Business data search

 Business data lists

 Business data Web Parts

 Filter Web Parts that filter by properties in the Business Data Catalog (such as the filters in personalization sites and dashboards)

 KPIs based on business data sources

 Reports built around one or more KPIs or business data Web Parts

 Business data actions

 InfoPath Forms Services browser-enabled forms

Business properties that refer to user profile data or discussion list properties redirect to the profile stores for those types of profile data, which are not stored within the Business Data Catalog. For example, personnel records stored in SAP, which are imported by the People and Audiences Shared Service, appear as user profiles that can be managed from the relevant SSP.

Each of the features in the previous list that is built on business data has its own detailed planning considerations. When planning business data profiles, it is important to focus on including the relevant properties that will make the profiles useful in themselves, while also being useful for these other features. In this case, it might be useful to work backwards, starting with planning sites, then highlighting the business data features for each site and planning for each of them, and then listing all of the relevant properties to include in the business data profile for each business data type used in that site. By the time you evaluate all of your sites, you will have a list of applications, business data types, and properties for each business data type. Then, you can simply ensure to include those properties when registering applications in the Business Data Catalog.

For example, when you plan your site collections, you might decide to track business sales on a single site collection. You plan to use the portal site template to host a central site that has news and information relevant to all sales associates and managers, personalization sites that track sales for each employee, and a dashboard that presents sales across the organization that can be filtered by date, sales associate, product line, or location. You also want employees to be able to search for customers, particularly when managing key business accounts.

The administrators and planners for the site collection plan the Web Parts and lists needed to meet these business needs. The dashboard will have a set of business data Web Parts such as KPIs, Excel Web Access Web Parts, and Web Parts that display data from applications that are registered in the Business Data Catalog. Each of those business data Web Parts will gather its data from a different business data type in the central business application that is tracking sales. The relevant data — and associated properties — will depend on what is being tracked. Each filter Web Part used will filter based on a different property of business data. Search is built on a subset of managed properties that is used in queries and search scopes when users search for customers, products, or sales offices. Finally, the business actions you implement often use business data properties.

For each of the pages and sites you plan for the site collection, you plan the business data types and relevant properties you will need. By the time you are done, you will have a list of business data types for the application, the properties you want to track for each one, and the properties that are used most often across the site collection. Every site collection will be planned similarly, and the SSP administrator for the Business Data Catalog will end up with a complete list of business data profiles to implement during initial deployment.

Business data property and profile planning is an iterative process in which you first plan information architecture, then consider the sites planned based on that information architecture, then identify features for each site, and then use information about the properties needed by those features to plan and create business data profiles in the Business Data Catalog. In that process, you might also identify gaps in the information architecture planning or find that some business data properties are lower priority and can wait until later deployment. It can be just as important to decide what not to include in the initial deployment.

|  |
| --- |
| Worksheet action |
| Use the [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) to record the sites that use business data applications for your site collection hierarchy and for each site collection. Also record the business data Web Parts and SharePoint lists that are used for each site. |
| Use the [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) to record the applications registered in the Business Data Catalog, along with the included business data types and properties for each business data profile.  For data sources based on SQL Server databases and other relational databases that will be stored in data connection libraries, record the planned data source and the relevant business data types and properties used by SQL Server 2005 Analysis Services and SQL Server 2005 Reporting Services when analyzing and displaying the data.  For each data source on the worksheet, record the KPIs, reports, and business data lists and Web Parts based on that data source, and add the properties used by each list or Web Part. For KPIs, record the planned calculation method and the targets for each indicator level of the KPI. |

## Worksheets

Use the following worksheets to plan for business data profiles:

 [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409)

 [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409)

# Plan business data lists

In this article:

 [About business data lists](#DSDOC_section110008f02_d602_4749_b89a_15)

 [Plan business data columns](#DSDOC_section210008f02_d602_4749_b89a_15)

 [Plan dependent columns](#DSDOC_section310008f02_d602_4749_b89a_15)

 [Plan business actions in business data lists](#DSDOC_section410008f02_d602_4749_b89a_15)

 [Plan Web Parts for business data lists](#DSDOC_section510008f02_d602_4749_b89a_15)

 [Worksheets](#DSDOC_section610008f02_d602_4749_b89a_15)

In Microsoft Office SharePoint Server 2007, business data lists are lists that contain columns that have data from other data sources, such as data connection libraries, Excel Calculation Services, other SharePoint lists, or the Business Data Catalog. In Office SharePoint Server 2007, you use business data lists to display the business data types and properties of business data applications within SharePoint lists and to create Business Data List Web Parts. These lists and Web Parts can then be used in sites throughout the Web applications and site collections used by your organization.

As part of planning for your initial deployment of Office SharePoint Server 2007, you should understand how to add business data columns to SharePoint lists, how to add business data actions to business data lists, and how to create business data Web Parts based on business data lists. Then, you can plan for lists in your initial deployment of Office SharePoint Server 2007.

## About business data lists

Business data lists enable you to display data from business applications in SharePoint lists. You create business data lists by adding business data columns to any existing SharePoint list. You can also create business data lists by creating and configuring a Business Data List Web Part, which automatically creates the corresponding list that has selected business data fields.

Business data lists are used as a source of data when you create the Web Parts for pages, such as the Report Center site, other SharePoint sites that have reports or business intelligence Web Parts, multi-report summary pages known as dashboards, and personalization sites.

The data in business data lists can be taken from the applications registered in the Business Data Catalog and from underlying line-of-business applications. Additionally, data from Microsoft SQL Server and Excel Calculation Services can be displayed in SharePoint lists and list Web Parts.

## Plan business data columns

From any SharePoint list, users who have permissions to add and remove columns to the list have the option to include one or more business data columns. These columns enable you to connect to data sources to bring business data into any existing list.

Business data columns are associated with business data types in the Business Data Catalog. The heading for the column is the business data type, and each row in the column contains a different item of that type. For example, a business data column for the "customer" business data type appears as a "customer" column that includes different customers for each item in the list.

The data in business data columns is taken directly from business applications. Every item of business data has a corresponding business data profile. This enables you to create lists that link directly to valuable business data. For example, in a customer service scenario, clicking the name of the customer in the customer column opens a profile of that customer. The profile contains a list of relevant properties for the customer, such as the customer's location, number of purchases, address, e-mail address, and telephone number.

When planning the sites in your site collection, it is important to consider which business data lists to include in the initial deployment. Most business data lists will be created during ongoing operations by individual users, but some lists are so central to the business data in your organization that you might want to create and deploy them from the beginning. Some lists are used by Business Data List Web Parts.

For every Business Data List Web Part you create that relies on a SharePoint list, plan to create the list and include the columns that will be needed in each Web Part. Each column you identify during planning is a business data type that you can import when you register a business application in the Business Data Catalog.

|  |
| --- |
| Worksheet action |
| Use the [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) to record the needed columns for the planned lists and Web Parts. |

## Plan dependent columns

Business data columns might be associated with dependent columns that appear automatically next to the main column. These dependent columns cannot be edited, because their values are taken from the connected data source. The values update automatically every time the view of the list is refreshed, after a set amount of time, or when someone who has the appropriate permissions clicks the Update Business Data button at the top of the list.

Users can filter and sort on dependent columns just as any other columns. The person who adds business data columns decides which dependent columns to include.

Dependent columns represent properties related to a particular business data type in the Business Data Catalog, which might or might not be business data types themselves. When you plan for the business data lists in your initial deployment of Office SharePoint Server 2007, make a note of the properties you will need to create for these dependent columns.

|  |
| --- |
| Worksheet action |
| Use the [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) to record the properties you will need to create for the dependent columns. Use that information when you register each business application in the Business Data Catalog. |

## Plan business actions in business data lists

When you add a business data column to a list, you also add a set of actions associated with the business data type for that business column. These actions appear when users hold their pointer over the item they want to act on. In the customer database example, users who use the list can perform an action for any customer simply by pointing at the customer's name in the list and then selecting an action from the menu that appears. For example, a common action is "Edit Customer Profile," which opens a Microsoft Office InfoPath 2007 page that has properties for the selected customer.

## Plan Web Parts for business data lists

Business data lists are used when creating Business Data List Web Parts. The following Web Parts are based on business data lists:

 Business Data List Web Part

 Business Data Details Web Part

 Business Data Association Web Part

 Key performance indicator (KPI) List Web Part

The first three Web Parts use data from applications in the Business Data Catalog in business data lists to display business intelligence in reports, dashboards, personalization sites, and other business intelligence sites. For more information, see [Plan business data Web Parts](#DSDOC_165f1afe_11e5_4c45_8f93_bf16e18338).

The KPI List Web Part can be based on information in business data lists, by selecting a SharePoint list as the source for a particular KPI. KPIs can also be created from SQL Server 2005 Analysis Services databases that are accessed by data connection libraries. For more information, see [Plan key performance indicators](#DSDOC_d8f9b41e_e324_490d_bf85_1370c8b63b).

|  |
| --- |
| Worksheet action |
| Use the [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) to record the SharePoint lists and related Web Parts used for dashboard pages and other key sites that use business data lists. |

## Worksheets

Use the following worksheets to plan business data lists:

 [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409)

 [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409)

# Plan business data Web Parts

In this article:

 [About business data Web Parts](#DSDOC_section1165f1afe_11e5_4c45_8f93_bf)

 [Plan core business data Web Parts](#DSDOC_section2165f1afe_11e5_4c45_8f93_bf)

 [Plan specialized business data Web Parts](#DSDOC_section3165f1afe_11e5_4c45_8f93_bf)

 [Plan KPI Web Parts](#DSDOC_section4165f1afe_11e5_4c45_8f93_bf)

 [Plan Excel Web Access Web Parts](#DSDOC_section5165f1afe_11e5_4c45_8f93_bf)

 [Plan SQL Server 2005 Analysis Services Web Parts](#DSDOC_section6165f1afe_11e5_4c45_8f93_bf)

 [Plan filter Web Parts connected to business data Web Parts](#DSDOC_section7165f1afe_11e5_4c45_8f93_bf)

 [Plan deployment of Web Parts](#DSDOC_section8165f1afe_11e5_4c45_8f93_bf)

 [Worksheets](#DSDOC_section9165f1afe_11e5_4c45_8f93_bf)

In Microsoft Office SharePoint Server 2007, business data Web Parts are used in reports, reports-enabled pages such as the Report Center site, and other SharePoint sites including personalization sites to display a Web-based view of business data that promotes analyzing, reporting, and acting on that data in a way that builds knowledge within your organization.

As part of planning for your initial deployment of Office SharePoint Server 2007, you should understand the different varieties of business data Web Parts, understand how they are used to display business data and promote business intelligence, and plan the specific Web Parts to deploy for each site.

## About business data Web Parts

Business data can be displayed in SharePoint lists and Web Parts for the pages and sites in each site collection used by your organization. The sources of this data include Microsoft SQL Server 2005 and its related applications, such as SQL Server 2005 Reporting Services, and line-of-business applications registered in the Business Data Catalog.

Business data can be exposed directly in lists by using the Business Data List Web Part. It also can be exposed through Web Parts designed specifically for personalization features. Depending on where the Web Parts are used, the experience is completely different. If it is just a simple list, the experience is much like using any SharePoint list, except that the data is connected to the data source and updates automatically. If it is a single Web Part within a report, the owner of the page controls the interactivity and it might simply be a display of that data. If it is on a multi-report summary page, it can be filtered along with other business data Web Parts on the page. If it is on a personalization site or personal site, the information in the Web Part is targeted by audience, and only information relevant to the viewer is presented. There are also specific Web Parts for common line-of-business applications, such as SAP.

Types of Web Parts that are used to display business data on SharePoint sites include:

 Core business data Web Parts

 Specialized business data Web Parts

 Key performance indicator (KPI) Web Parts

 Excel Web Access Web Parts

 SQL Server 2005 Analysis Services Web Parts

 Filter Web Parts that are connected to business data Web Parts (for example, the Current User Filter Web Part and the Property Profile Filter Web Part used on personalization sites, and the Business Data Catalog Filter Web Part)

These Web Parts are used to create pieces of business intelligence that can be displayed in reports linked from the Report Center site, other SharePoint sites that have reports or business data, in multi-report summary pages also known as dashboards, and on personalization sites.

Data connection libraries expose Office data connection (.odc) files and universal data connection (.udcx) files.

## Plan core business data Web Parts

The core business data Web Parts include:

 Business Data List Web Parts

 Business Data Details Web Parts

 Business Data Association Web Parts

 Business Data Actions Web Parts

 Business Data Catalog Filter Web Parts

The first four business data Web Parts are used to display information based on the data stored by SQL Server and reported by SQL Server 2005 Reporting Services, and the properties of line-of-business applications registered in the Business Data Catalog. The first three of these Web Parts then can be added to reports in the Report Center site or other pages that display reports or business data.

The Business Data List Web Part presents business data in a simple list form, including several items from one type of business data in the Business Data Catalog. An example is a list of customers from a customer service database. That list can be connected to a filter Web Part to show information that is based only on the current user or a specific value for a property of the relevant business application. You also can edit the view properties of a Business Data List Web Part, just as you can edit the view of any list, to filter by property or limit the number of items shown in the Web Part. The Web Part also can be targeted to audiences so that only some users see the Web Part.

The Business Data Details Web Part displays the details of a single item, such as a single customer in a customer database.

The Business Data Association Web Part presents a related list that shows a list of items related to an item of another business data type. An example is a list of customers who work in a particular sales region. Related lists can be associated with more than one source business data type to narrow the focus of the list. An example is a list of sales orders by a customer in a particular sales division. The source business data types are the customer and the sales division, and the items in the list are sales orders. As with the view for the Business Data List Web Part, the view for the Business Data Association Web Part can be filtered or limited to a specified number of list items, and can be connected to filter Web Parts or targeted to audiences.

The Business Data Actions Web Part adds a simple URL to a page associated with the action named in the link. It is used to enable users to perform common actions from business applications directly from the Web browser. Often, a Business Data Actions Web Part is found on the same page with a related business data Web Part, so users can see information and act on it immediately. For example, a Business Data Actions Web Part for the "View Customer Profile" action could be found on a dashboard that has an Excel Web Access Web Part that displays sales for a customer and a KPI Web Part that shows customer satisfaction. An analyst seeing a low customer satisfaction KPI could correlate that information with recent sales reports and then click the business data action link to find out more about the customer and contact them to improve customer service.

The Business Data Catalog Filter Web Part filters other Web Parts on a page based on values found in SQL Server 2005 Reporting Services or the Business Data Catalog. It is often used in combination with business data Web Parts to filter the view, and any recognized property can be used by this filter. For more information about filtering data, see [Plan dashboards and filters](#DSDOC_5fe87ec1_431e_4b7f_ae33_1e2edd8613).

## Plan specialized business data Web Parts

Specialized business data Web Parts include:

 IView Web Part (SAP)

 WSRP (Web Services for Remote Portlets) Consumer Web Part

The IView and WSRP Consumer Web Parts support the presentation of data from SAP and WSRP portlets, respectively. If your organization uses SAP or remote portlets, these Web Parts enable you to integrate these Web Parts into your Web Part pages so that you can have a single view of all business data instead of different sites for different Web-based views of business data.

To use the IView Web Part, you must perform the following steps:

1. Configure SAP for the site.

2. Select an SAP server and IView for the Web Part.

3. Ensure that both the SAP server and IView are trusted on the site.

To use the WSRP Consumer Web Part, you must perform the following steps:

1. Configure WSRP producers for the site.

2. Select a portlet server and portlet for the Web Part.

3. Ensure that both the portlet server and portlet are trusted on the site.

## Plan KPI Web Parts

KPI Web Parts present business data with graphical indicators of the current status of a key business process. For example, a KPI can use traffic light icons to indicate that customer satisfaction is exceeding, meeting, or failing to meet goals. If customer satisfaction exceeds a preset goal, calculated by counting the percentage of positive satisfaction ratings across your organization, the customer satisfaction KPI is displayed with a green traffic light icon. If customer satisfaction is failing to meet minimum goals, the customer satisfaction KPI is displayed with a red traffic light icon. Otherwise, it is displayed with a yellow traffic light icon.

Each KPI in a KPI List Web Part and the single KPI in each KPI Details Web Part is evaluated based on a single value from a data source, either from a single property or by calculating an average or total across the selected data. Because they are calculated across a range of data rather than displaying data in list form, they can be more useful when measuring performance across groups or projects. However, by calculating a range of data for a specific person, such as a list of sales for a single employee, a KPI can evaluate individual performance.

The two KPI Web Parts display a list of KPIs calculated independently, or details for a single KPI. You can connect KPI Web Parts to filter Web Parts to filter each KPI by specific properties or users. Data sources for KPI lists include:

 SharePoint lists   The data comes from a SharePoint list that might include business data from the Business Data Catalog or SQL Server 2005.

 Excel workbooks   The data comes from an Excel workbook.

 SQL Server 2005 Analysis Services   The data comes from database stores known as cubes, for connections in a data connection library.

 Manually entered information   The data comes from a static list, rather than based on underlying data sources. This is used less frequently, for test purposes prior to deployment or on occasions when regular data sources are unavailable but you still want to provide performance indicators.

If the KPI List Web Part is added to a page, you must provide a link to a KPI list that contains KPIs. KPI List Web Parts can include links to the details of each KPI. When you click the link for the KPI, a customizable details Web page appears that contains additional information. The view of KPI List Web Parts based on SharePoint lists can be limited or filtered just as the view of any list.

The KPI Details Web Part displays performance indicators for a single item in a KPI list.

For more information about planning KPI Web Parts, see [Plan key performance indicators](#DSDOC_d8f9b41e_e324_490d_bf85_1370c8b63b).

## Plan Excel Web Access Web Parts

Excel Web Access Web Parts are available for personal sites and personalization sites. The Excel Web Access Web Part is used to provide information from a specific worksheet directly within the Web Part by using Excel Calculation Services. It also enables the ability to perform analytics in the Web browser without affecting the underlying worksheets or data sources. Users who have the appropriate permissions can start an Microsoft Office Excel 2007 window directly from this Web Part to edit the worksheet. The Excel Web Access Web Part also can be used to perform analytics on data from SQL Server 2005 Analysis Services.

## Plan SQL Server 2005 Analysis Services Web Parts

SQL Server 2005 Analysis Services Web Parts are available for personal sites and personalization sites. The SQL Server 2005 Analysis Services Web Part presents data directly from SQL Server 2005 Analysis Services. This part can be used in reports or multi-report summary pages, or in other sites that use business data such as personalization sites.

## Plan filter Web Parts connected to business data Web Parts

One feature of business data Web Parts is the ability to filter the data displayed on each Web Part by using one or more filter Web Parts. Filters can be connected to a single Web Part or to all the Web Parts on a page. When several business data Web Parts are connected to a single filter, the data in all of the business data Web Parts can be filtered by the same property and value. For example, a page can filter data from all of its business data Web Parts over the last month or for a certain user. Such multi-report summary pages, known as dashboards, can be very useful in presenting a uniform view of business data in your organization.

## Plan deployment of Web Parts

Each of these Web Parts must be added to a site and then connected to the underlying data source. After that connection is made and the Web Part displays business data, it can be used to create a page around the Web Part called a report. It can also be used in a multi-report summary page that displays multiple business data Web Parts. Reports can appear in the Report Center site or any other reports site, and business data Web Parts can be used in other sites such as personalization sites.

Site planning enables you to identify the Web Parts you plan to create that use business data. Each Web Part requires certain properties. You will want to decide which properties are most relevant for the viewers of each Web Part on a site.

The sites and pages that commonly use business data Web Parts include:

 The Report Center site

 Other sites that use reports

 The default dashboard for the site collection

 Personalization sites

For an initial deployment, consider the Web Parts that you will use for each of these sites. Although you can use business data Web Parts on any site, it is not necessary to plan for the Web Parts of those sites, which are created during ongoing operations. For each Web Part:

 List the applications and business data types you need to implement the Web Part.

 List the properties you need to implement the Web Part, so that you can include those properties in the business data profile for the appropriate business applications and business data types.

 Ensure that the information for each property and business data type of each application is complete enough to be useful when it is imported.

 Plan to create lists that business data Web Parts are based on.

 Consider the security implications of each list, and note the SharePoint groups that will have access to each list and corresponding Web Part.

 Decide whether the Web Part's view should be limited or filtered. For more information, see [Plan business data lists](#DSDOC_10008f02_d602_4749_b89a_15f7406aea).

 Decide whether the Web Part is connected to filter Web Parts. For more information, see [Plan dashboards and filters](#DSDOC_5fe87ec1_431e_4b7f_ae33_1e2edd8613).

 Decide whether the Web Part should be targeted to specific audiences, for each site that uses the Web Part. For more information, see [Plan for personalized Web Parts](#DSDOC_c976bea3_148c_4be6_96b7_6400c12692).

 Consider whether the purpose of this Web Part is already fulfilled by another Web Part or site to minimize unnecessary duplication of functionality. For more information, see [Determine sites and subsites](#DSDOC_462e12d6_1a5d_4b7c_a0d5_14c551262b).

Although planning Web Parts will take time, it allows you to understand the scope of your Web Part deployment before you begin, so that you can prioritize what is most important for initial deployment, and schedule lower priority sites and Web Parts for later deployment. It also reduces deployment time by identifying data sources and lists on which business data Web Parts are dependent.

|  |
| --- |
| Worksheet action |
| Use the [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) to record business data and business intelligence Web Parts. Record connected Web Parts, data sources, and SharePoint lists used by the Web Part in the same table. |
| Use the [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) to record Web Parts used by each site planned in your site collection hierarchy. |

## Worksheets

Use the following worksheets to plan business data Web Parts:

 [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409)

 [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409)

# Plan business data actions

In this article:

 [About business data actions](#DSDOC_section160b8a5be_c54e_488c_90b0_80)

 [Plan the scope of business actions](#DSDOC_section260b8a5be_c54e_488c_90b0_80)

 [Plan properties for business actions](#DSDOC_section360b8a5be_c54e_488c_90b0_80)

 [Plan Business Data Action Web Parts](#DSDOC_section460b8a5be_c54e_488c_90b0_80)

 [Plan custom business actions](#DSDOC_section560b8a5be_c54e_488c_90b0_80)

 [Worksheet](#DSDOC_section660b8a5be_c54e_488c_90b0_80)

Business data actions provide a way to enable users who view business data in reports, dashboards, or other reports-enabled pages to act immediately on the data that they are viewing. By using InfoPath Forms Services and configuring permissions to the relevant databases, users who have the correct permissions can make direct changes to the underlying business data.

As part of planning for your initial deployment of Microsoft Office SharePoint Server 2007, you should understand how to create business actions, how to plan for the pages that perform the action, how to plan the properties used in business data actions, how to determine who has access to an action, and how the action is displayed in search results, SharePoint lists, and sites containing the Business Data Action Web Part. Then, you can use these plans during your initial deployment of Office SharePoint Server 2007.

## About business data actions

Business data actions are actions configured by administrators. The actions open a Web page that provides meaningful information about business data so that users can meaningfully collaborate based on the data displayed in your organization. Business data actions enable you to provide ways for users in your organization to directly interact with business data from within the sites in your site collections.

For every application registered in the Business Data Catalog, each business data type has a business data profile. You create actions for common tasks by using business data from within the profile.

The business action has two simple properties: an action name and a URL for a Web page that is used to process the action and to provide results of some kind. The Web page is typically one of the following:

 A static Web page that has a fixed result.

 A SharePoint list.

 A Microsoft Office InfoPath 2007 forms-enabled page that can interact with business data on the database or business application server.

 A customized page for more complex data interaction or presentation, such as a dynamic .aspx page.

After actions are created, they appear within a specialized Business Data Action Web Part for items in:

 Search results

 SharePoint lists

 Reports and dashboards

Examples of search results that might include actions are employees, customers, sales reports, and regional offices. Any business data type in the Business Data Catalog can be associated with one or more actions in a Business Data Action Web Part, and those actions appear as part of those items when they appear in search results. Similarly, any business data type in a list includes the associated actions that have been created for that business data type. Actions also show up in the business data profiles in the Business Data Catalog for the relevant applications and business data types. The Business Data Action Web Part can be used in other pages, such as the Report Center site and personalization sites.

For example, you can implement a Resolve action for a customer database application. After searching for a particular incident in the database, a customer service representative sees the Resolve action next to the customer's incident report in the search results. The representative clicks the link for the action, which opens a page that has form fields for type of resolution, date of resolution, and the name of the representative who is resolving the issue. The customer service representative might also see this action in his or her personal site, in a personalization site designed for tracking and resolving customer issues, or in a personalized Web Part displayed on another page, such as the Report Center site.

## Plan the scope of business actions

When planning for business actions, consider the common actions that people use for each business application. Every action that you make available from Office SharePoint Server 2007 is likely to increase the number of users who perform that action, which can affect planning in several areas:

 Security   Security is handled by the destination page associated with each action. That page can be a simple Web page, a Office InfoPath 2007 form, or a more customized page. Whatever the destination page, only users who have access to that page can perform the action. If the destination is not a SharePoint site, users who use the page must log in separately. When you plan for business actions, be sure that the users who perform the action have the appropriate permissions for the destination site. You can do this by comparing the membership and permissions plan for each site and noting the differences. Then, for each action, note where the differences affect the actions you are planning to create during initial deployment. If there are discrepancies, you can either change permissions so that the right users have access to a site, or you can change the planned destination location.

 Performance   When you enable users in your organization to easily access business applications from business actions in your site collection, you will likely increase the use of those applications. This produces an additional load on the databases and application servers for business applications. In most organizations, this will be a manageable increase. However, in large organizations, server performance might be affected.

 Site design   Consider the costs in time and resources for site planning when designing more complex actions. You might have limited time to design and develop more complex pages for handling interaction between your SharePoint sites and your business applications. Prioritize the most important actions first. Additional actions can be added as needed as part of normal operations after initial deployment and configuration.

Site administrators should make a note of the business actions they want to develop and the schedule for implementing those actions, and then provide those details to the IT administrators on the planning team. This helps IT administrators plan for any potential impact in capacity planning for both initial deployment and long-term operations.

## Plan properties for business actions

Business actions often require users to provide values in forms for certain business properties. Business actions can also open Web pages that use certain properties in performing calculations. You can make the correct properties available by noting the properties you need and including them in a comprehensive list of business data properties to include in business data profiles. The important information to plan for includes:

 The business applications that have important actions that you want to make available in each site collection.

 The business data types in the Business Data Catalog associated with each action.

 The properties associated with the each business data type.

For example, you might want a business action that resolves customer service records to be associated with the business data type for customer service records, and to appear when anyone views a customer service record. During planning, record the customer service database, the customer service record business data type, and the properties tracked for each customer service record, such as service date, issue type, customer name, and location of service. Provide this information to the users who plan shared services, so Shared Services Provider (SSP) administrators can import the properties when registering properties in the Business Data Catalog.

|  |
| --- |
| Worksheet action |
| Use the [Business data worksheet](http://go.microsoft.com/fwlink/?LinkId=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73271&clcid=0x409) to record your business data action plans. List data sources and related business data types and properties, both for databases in data connection libraries and for line-of-business applications registered in the Business Data Catalog. Business data actions that use those properties should also be recorded. |

## Plan Business Data Action Web Parts

The Business Data Action Web Part adds a link to a page associated with the action. When you create business actions for any business data type in the Business Data Catalog, this Web Part is included in search results and list items for any example of that business data type. If you create a resolve customer service report issue for the customer service report business data type, a Web Part that contains the Resolve action appears in any search results or lists containing any customer service reports.

You can use that same Web Part in additional sites, such as the Report Center site or personalization sites. When the Business Data Action Web Part is added, you can add one or more actions associated with a single business data type. You can use multiple action links on the same site to provide actions that are associated with more than one business data type, bringing business data interactivity wherever it is appropriate. Often, a Business Data Action Web Part is found on the same page as a related Web Part, such as a key performance indicator (KPI) Web Part, Business Data List Web Part, or Excel Web Access Web Part, so users can view information and immediately act on it.

You can choose Web Parts for each page based on the best way of fulfilling the purpose of each page as determined during information architecture and site structure planning. As you plan the key sites in site collections, update your site planning to incorporate opportunities for business data actions.

## Plan custom business actions

You can use the developer tools for Office SharePoint Server 2007 to customize business actions so that they do more than forward to a particular URL. Creating a custom action might be worth the development time and resources if the action relates directly to a key business process. For more information about creating custom actions, see the [Office SharePoint Server 2007: Software Development Kit](http://go.microsoft.com/fwlink/?LinkId=72208) (http://go.microsoft.com/fwlink/?LinkId=72208).

## Worksheet

Use the following worksheet to plan business data actions:

 [Business data worksheet](http://go.microsoft.com/fwlink/?LinkId=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73271&clcid=0x409)

# Plan for business data search

In this article:

 [About business data search](#DSDOC_section12b7121fc_a1f2_469d_ac1c_7b)

 [Plan business data search](#DSDOC_section22b7121fc_a1f2_469d_ac1c_7b)

 [Worksheets](#DSDOC_section32b7121fc_a1f2_469d_ac1c_7b)

The integration of business data with other features of Microsoft Office SharePoint Server 2007 provides an opportunity to use the full power of enterprise search to find, view, and act on relevant business data. This integration is available only in the enterprise version of Office SharePoint Server 2007. Deployments of the standard version of Office SharePoint Server 2007 cannot register business data applications or search for business data by using enterprise search.

When planning for business data search, it is important to understand the search functionality. It is also important to consider the following:

 Plan for inclusion of business data in content sources.

 Select the appropriate properties of business data to map to managed properties in the search schema.

 Create access control lists (ACLs) for business data types.

 Use search scopes and search filters to change how search queries are grouped and which search results are found.

 Plan to integrate business data search capability into the sites in your site collection.

## About business data search

Business data results are excluded from general search results. Business data search results can be displayed in four distinct ways:

 When a search scope that includes business data is used to search, the search results include business data results. A business data search scope is not provided by default, but administrators can create search scopes that include business data.

 Users can refine initial search results by selecting the option to search business data sources.

 Users can select a business data tab provided in the Search Center site, and the search will include all business data for the tab. A tab for all business data is not included by default, but administrators can add tabs for searching all business data or for searching data from specific business applications.

 If the search term in a standard search query matches a keyword phrase selected by an administrator, the business data result appears in recommended results.

Administrators of the search service and individual site collections must configure several options before business data is available in search results. Use the following procedure to make business data available for search.

procedure_ddMake business data available for search

|  |
| --- |
| 1. For line-of-business applications, register the application in the Business Data Catalog and set the number of connections.  2. Create a content source for the business application data.  3. Crawl the content source for the application data to add its properties as new crawled properties in the portal site schema.  4. Select the relevant properties in the Configure Search section of the Business Data Catalog and map them to managed properties for search.  5. Create ACLs for business data types in the Business Data Catalog.  6. Crawl the content source for the business data source again to update managed properties and ACLs.  7. Create search scopes for business data.  8. Configure keywords for business data. |

Most of these tasks are performed by the administrator of the search shared service or by the administrator of the Business Data Catalog. Some tasks are performed by site collection administrators. Both shared services administrators and site collection administrators will help plan search for business data.

## Plan business data search

When planning for business data search, it is important to consider your business needs and how you can use search features to improve the visibility of business data and the usability of business intelligence features.

The first thing to consider is which business processes are relevant to each site collection, and which business applications are used in evaluating and working within those processes. When you identify those applications, think about how users will search for that business data, and what the scope of the business data is. Often, users will look for business data from a particular application from several sites and site collections, but not every site will use the same business data. Based on the scope of business processes and the associated business applications and business data, several decisions will be affected.

### Plan Shared Services Providers for business data

You can often rely on the security for business applications to limit access to business data, but for particularly sensitive data that is used frequently by one group of users in your organization but not by the entire organization, you might want to consider separate Shared Services Providers (SSPs). Content and data are not shared across SSPs, so users who search by using the search shared service of one SSP will not see results for another SSP. This option is usually a good idea only when the content sets, including documents and sites other than business data, are fully distinct. Otherwise, you can use application security, SharePoint groups, and search scopes and search filters to limit availability of data.

Within the Business Data Catalog for each SSP, you will register every line-of-business application that has data you want to make available through search and other Office SharePoint Server features, such as business data Web Parts, InfoPath forms templates, workflows, and so on. SSP administrators should talk with farm administrators about capacity and performance implications for business applications. For more information, see [Plan for business data connections with the Business Data Catalog](#DSDOC_c803c1fa_cb0f_4a26_b439_de7ff4195e).

|  |
| --- |
| Worksheet action |
| Use the [Information architecture worksheet](http://go.microsoft.com/fwlink/?LinkId=73273&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73273&clcid=0x409) to record the number of SSPs and the data sources for each SSP's Business Data Catalog. |
| Use the [Site hierarchy planning tool](http://go.microsoft.com/fwlink/?LinkId=73143&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73143&clcid=0x409) to plan the number of SSPs and the data sources for each SSP's Business Data Catalog. |
| Use the [Estimate data capacity requirements worksheet](http://go.microsoft.com/fwlink/?LinkId=73274&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73274&clcid=0x409) to record the number of connections for each business data source. |

### Plan business data content sources

To use business data in search results, you must create business data content sources. Business data content sources are added just like other content sources, but have some additional configuration steps that you should consider during planning.

Business data start addresses include locations of databases for Microsoft SQL Server 2005 or other databases, and various line-of-business applications. These locations are often on separate servers that exist prior to the deployment of Office SharePoint Server 2007, although the applications can be hosted on the same server. For load-balancing purposes, you might want to host databases on separate servers. When you plan the server farms for your deployment, consider how they will connect to application servers. For more information about deploying application servers, see Design server farms and topologies.

To help preserve security and limit the performance impact on your business data applications, you do not want to use the actual location where business data is stored when crawling business data content sources. Typically, you will create a data warehouse that has a copy of the data, including all of the relevant business data types, properties, and values. That location will be used in the content source for the business application.

You might want to create additional content sources to support the following scenarios:

 You want to crawl business data in one application more frequently than business data in other applications.

 You want to create search scopes that are limited to a specific set of data from one or more applications, by using content sources. You can create search scopes based on properties instead of on content sources, so content sources are not necessary if properties enable you to accomplish the same result.

 You want to create a Search Center tab that points to a specific set of business data that is defined by content source. As with search scopes, this is not the only way to define how business data is displayed in the Search Center site.

The frequency with which you crawl business data content sources depends on the impact to business data application servers. Work with the administrators of each business data application to implement a reasonable schedule.

|  |
| --- |
| Worksheet action |
| Use the Content Sources section of the [Plan to crawl content](http://go.microsoft.com/fwlink/?LinkId=73748&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73748&clcid=0x409) to record the decisions you make about business data content sources, along with the expected crawling schedule for each content source. |

For more information about content sources, see [Plan to crawl content [Office SharePoint Server]](#DSDOC_82c09ad6_6137_438d_a324_16a7f99e12).

### Plan search properties for business data

To use business data, you must select the properties of business data that will be available to search as managed properties. Properties from SQL Server can be mapped directly after they have been crawled, but line-of-business applications must first be registered in the Business Data Catalog. Managed properties will be the subset of properties that you want to use when you search for business data.

The key business processes identified during information architecture planning will suggest the most likely managed properties. You can map multiple crawled properties to a single managed property, and select whether one takes precedence or whether the managed property is multi-valued and includes all values found for crawled properties.

When you decide which properties and which business data types for a business data application you want to make available for search, you must think about what you want users to be able to find, how that information will be presented, and what the crawling impact is on the data warehouse that contains the data. Frequently, you will not want to display all data, but only data about certain properties. For example, an organization that has several offices in several regions might only want to display results for specific offices in a few key regions, depending on business needs. You decide which business data types to include and which properties to include for each business data type. Factors to consider when deciding which properties to make available include:

 Confidentiality policies   You might have good business reasons to keep certain records confidential. For example, records that might be relevant only to key business planners and not to most users who work with data in the application. You can decide to display the properties for business data types that are not confidential, but not to display those that are.

 Performance impact   Some properties might not be confidential, but the impact of crawling those properties and potentially enabling users to access and change those properties by using business actions might outweigh the business gains of that decision. Carefully consider the performance of each group of business data types that you enable.

|  |
| --- |
| Worksheet action |
| Use the Plan managed properties section of the [Plan the end-user search experience](http://go.microsoft.com/fwlink/?LinkId=74967&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=74967&clcid=0x409) to record the managed properties. |

For more information about crawled and managed properties for search, see [Plan the end user search experience [Office SharePoint Server]](#DSDOC_a56532d7_9814_4a0c_a308_f2369eaf30).

### Plan access and security for business data search results

You can use the security for each business application to limit access to business data search results. You can also limit access to business data search by using SharePoint groups.

Any user who has access to a business data application, whether it is a database application, such as SQL Server 2005 or a line-of-business application, can also access the business data in that application. Business data search results use that security to ensure that only users who have the correct permissions can see the search results.

However, you can also apply permissions to business data and business data search results from within Office SharePoint Server 2007. A user without permissions to the database can still see search results if they have the correct SharePoint permissions.

It is a good practice to limit the number of users who have direct access to a business application. In many organizations, this might be a single account or a group that contains a small number of users. You can create SharePoint groups that have the correct permissions to view business data and related search results for each application, and then assign users in your organization to those groups. When granting permissions, consider your larger security needs and the users to whom the data in each business application is relevant. Match each application with the users who will need to find business data to do their jobs.

|  |
| --- |
| Worksheet action |
| Use the [Custom permission levels and groups worksheet](http://go.microsoft.com/fwlink/?LinkId=73134&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73134&clcid=0x409) to record access to applications. |
| Use the [Site and content security worksheet](http://go.microsoft.com/fwlink/?LinkId=73135&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73135&clcid=0x409) to record access to applications. |

### Plan search scopes for business data

Search scopes can be used to enable users to search for certain subsets of business data. When you plan your information architecture, you identify key business processes or groups of processes. Some of these processes will be closely linked to specific business data applications. To create a search scope for specific applications and content related to those applications, you can either apply scope rules based on properties of business data to narrow the scope of search results, or create a content source that includes only start addresses for that business process and base the search scope on that content source.

For more information about planning search scopes, see [Plan the end user search experience [Office SharePoint Server]](#DSDOC_a56532d7_9814_4a0c_a308_f2369eaf30).

### Plan keywords for business data

For each business application, you will also want to consider the most relevant search results, and consider the search terms that users are likely to use when they perform search queries. For example, if you have a key performance indicator (KPI) list that tracks a key business process, you might decide that it should appear at the top of search results when users search business data by using common terms for that business process. You can use special terms, also known as keywords and Best Bets, to highlight key business data. You can highlight lists, databases, specific business data types for an application in the Business Data Catalog. For example, you can highlight a customer business data profile as a Best Bet for a keyword relating to that customer, and the profile will be promoted to the top of search results.

You can prioritize the important special terms to configure during initial deployment by considering key phrases for each business process and associated application. Then, you can consider the most important content for those terms. Record those terms to create a reference you can use during deployment to test search terms and see if the key content appears high enough in the search results. If it does not, you can create special terms to promote those results.

|  |
| --- |
| Worksheet action |
| Use the Keywords section of the [Plan the end-user search experience](http://go.microsoft.com/fwlink/?LinkId=74967&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=74967&clcid=0x409) to record keywords. |

For more information about keywords and special terms, see [Plan the end user search experience [Office SharePoint Server]](#DSDOC_a56532d7_9814_4a0c_a308_f2369eaf30).

### Plan business data tabs in the Search Center site

The Search Center site provides a business data tab that can be used to search across all business data sources. You might want to identify additional business data tabs for specific applications, databases, or records within an application or database. Look at your information hierarchy and consider adding business data tabs for each of the key business processes for your organization. If it is likely that users will want to search a specific set of data, it is probably worth creating a tab for that purpose. Using business data tabs in the Search Center site also provides a way to expand search without creating long lists of search scopes in the Search Scopes menu.

You might also want to customize the appearance and functionality of each tab. For more information about customizing the Search Center site, see [Searching in Office SharePoint Server 2007](http://msdn2.microsoft.com/en-us/library/ms497338.aspx) (http://msdn2.microsoft.com/en-us/library/ms497338.aspx) in the [Microsoft Office SharePoint Server 2007 Software Development Kit](http://msdn2.microsoft.com/en-us/library/ms550992.aspx) (http://msdn2.microsoft.com/en-us/library/ms550992.aspx).

### Example

Contoso, Ltd., is a technology company that has a customer call center to handle support calls. The call center is set up on a single site collection. Support representatives keep track of customers and customer issues by using a line-of-business application, and they have an archive of past customer issues stored on SQL Server 2005 databases that they can analyze by using SQL Server 2005 Analysis Services. Each of these applications and the related customers and product lines are recorded in the [Information architecture worksheet](http://go.microsoft.com/fwlink/?LinkId=73273&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73273&clcid=0x409).

The Business Data Catalog administrator plans to register the customer issues application in the Business Data Catalog, map business application data properties to managed properties used by search, and create business data profiles for key business data types, such as customer, region, business unit, and product line. The planned properties are recorded in the [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409). The managed properties used by search are recorded in the Plan managed properties section of the [Plan the end-user search experience worksheet](http://go.microsoft.com/fwlink/?LinkId=74967&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=74967&clcid=0x409).

Because the content on the site collection concerns an integrated set of business processes and users who share information across teams and processes, there is no need for additional SSPs to isolate content. Only one SSP is needed. This should be recorded on the [S](http://go.microsoft.com/fwlink/?LinkId=73143&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73143&clcid=0x409).

The search service administrator plans to create a content source for the customer service application, so customer and customer issue data can be updated more frequently than the rest of the content on the site collection. This content source is recorded in the content sources section of the [Plan to crawl content worksheet](http://go.microsoft.com/fwlink/?LinkId=73748&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73748&clcid=0x409).

The Business Data Catalog administrator decides to use a single account that has access to the customer service application to crawl the data in the application. Additional users will be granted permissions not directly to the application, but by being added to SharePoint groups that have access to business data in the site collection. Permissions to data in the SQL Server 2005 database will be limited by cube so that each person can view only the data relevant to his or her areas of responsibility. Most users in your organization will be granted read-only access for the data directly relevant to their jobs. This information is recorded in the [Site and content security worksheet](http://go.microsoft.com/fwlink/?LinkId=73135&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73135&clcid=0x409).

The planning team plans scopes for customers and customer issues, along with other search scopes not related to business data. The planning team records this information in the Plan scopes section of the [Plan](http://go.microsoft.com/fwlink/?LinkId=74967&clcid=0x409)  (http://go.microsoft.com/fwlink/?LinkId=74967&clcid=0x409).

When considering special terms for business data, the search service administrator for Contoso, Ltd., identifies support experts for each major product line and creates Best Bets for each expert based on keywords related to their area of expertise.

The team plans a dedicated Search Center site for the team that contains information about customers and customer service reports, and important documents and sites relevant to customer service representatives. The team starts with the Search Center site provided by the portal site template and plans features based on business needs. The team plans a customer tab so that customer service representatives can search for specific customers in the database, and a separate tab for customer service reports.

## Worksheets

Use the following worksheets to plan for business data search:

 [Authentication methods worksheet](http://go.microsoft.com/fwlink/?LinkID=73278&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73278&clcid=0x409)

 [Business data worksheet](http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73271&clcid=0x409)

 [Plan to crawl content worksheet](http://go.microsoft.com/fwlink/?LinkId=73748&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73748&clcid=0x409)

 [Custom permission levels and groups worksheet](http://go.microsoft.com/fwlink/?LinkId=73134&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73134&clcid=0x409)

 [Estimate data capacity requirements worksheet](http://go.microsoft.com/fwlink/?LinkId=73274&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73274&clcid=0x409)

 [Information architecture worksheet](http://go.microsoft.com/fwlink/?LinkId=73273&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73273&clcid=0x409)

 [Plan the end-user search experience](http://go.microsoft.com/fwlink/?LinkId=74967&clcid=0x409)  (http://go.microsoft.com/fwlink/?LinkId=74967&clcid=0x409)

 [Site and content security worksheet](http://go.microsoft.com/fwlink/?LinkId=73135&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73135&clcid=0x409)

 [Site hierarchy planning tool](http://go.microsoft.com/fwlink/?LinkId=73143&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73143&clcid=0x409)

# Plan external data connections for Excel Services

Note   This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [About Excel Services connections to external data](#DSDOC_section17e6ce086_57b6_4ef2_8117_e7)

 [Connections and Excel workbooks](#DSDOC_section27e6ce086_57b6_4ef2_8117_e7)

 [Data providers](#DSDOC_section37e6ce086_57b6_4ef2_8117_e7)

 [Authentication to external data](#DSDOC_section47e6ce086_57b6_4ef2_8117_e7)

 [Data connection libraries and managed connections](#DSDOC_section57e6ce086_57b6_4ef2_8117_e7)

 [Excel Services security and external data](#DSDOC_section67e6ce086_57b6_4ef2_8117_e7)

 [Step-by-step server configuration for external data](#DSDOC_section77e6ce086_57b6_4ef2_8117_e7)

 [Step-by-step workbook configuration for external data](#DSDOC_section87e6ce086_57b6_4ef2_8117_e7)

 [Frequently asked questions](#DSDOC_section97e6ce086_57b6_4ef2_8117_e7)

To configure Microsoft Office SharePoint Server 2007 to enable workbooks loaded on Excel Services to successfully refresh external data, you need to understand the relationships and dependencies between Office SharePoint Server 2007 and Excel Services.

The guidance provided in this article helps you resolve the following Data Refresh Failed error message.



## About Excel Services connections to external data

This article provides guidance to help you configure the following Office SharePoint Server 2007 application server components:

 Excel Services

 Single sign-on (SSO)

 Office SharePoint Server 2007

This article also includes background information that provides an overview of application server and external data concepts, some of which are specific to Office Excel 2007. This background information contains important information that will help you successfully set up Excel Services to enable workbooks to consume external data.

This article also shows you how to configure Office Excel 2007 workbooks and provides answers to frequently asked questions, including questions about:

 Server security and external data

 Managed data connections

## Connections and Excel workbooks

Every Excel workbook that uses external data contains a connection to a data source. Connections consist of everything that is required to establish communications with, and retrieve data from, an external data source. This includes:

 A connection string (a string that specifies which server to connect to and how to connect to it).

 A query (a string that specifies what data to retrieve).

 Any other specifics required to get the data.

### Embedded and linked connections

Excel workbooks can contain embedded connections and linked connections. Embedded connections are stored internally as part of the workbook. Linked connections are stored externally as separate files that can be referenced by a workbook.

Functionally, there is no difference between embedded and linked connections. Both will correctly specify all the required parameters to connect to data successfully. Linked connection files can be centrally stored, secured, managed, and reused. They are often a good choice when planning an overall approach to getting a large group of users connected to external data. For more information, see [Data connection libraries and managed connections](#DSDOC_section57e6ce086_57b6_4ef2_8117_e7).

For a single connection, a workbook can have both an embedded copy of the connection information and a link to an external connection file. The connection can be configured to always use an external connection file to refresh data from an external data source. In this example, if the external connection file cannot be retrieved, or if it fails to establish a connection to the data source, the workbook cannot retrieve data. If the connection is not configured to use only an external connection file, Excel attempts to use the embedded copy of a connection. If that fails, Excel attempts to use the connection file to connect to the external data source. The ability to specify that only connection files can be used to establish a communications link to an external data source is a new feature of 2007 Microsoft Office system and provides support for the managed connection scenarios described in [Data connection libraries and managed connections](#DSDOC_section57e6ce086_57b6_4ef2_8117_e7).

Excel Services can use connections coming from an external connection file and connections that are embedded in the workbooks. There are some restrictions for external connection files. For more information, see [Excel Services security and external data](#DSDOC_section67e6ce086_57b6_4ef2_8117_e7).) If both types of connections are allowed on the server, the behavior is the same as the Excel behavior described in the previous paragraph.

For security purposes, Excel Services can be configured to only allow connections from connection files. In this configuration, all embedded connections are ignored for workbooks loaded on the server, and connections are only attempted when there is a link to a valid connection file that is trusted by the server administrator. For more information, see [Trusted data connection libraries](#DSDOC_subsection17e6ce086_57b6_4ef2_8117).

note_ddNote:

There are many types of connection files, and Excel Services only works with Office data connection files (.odc).

## Data providers

Data providers are drivers that client applications (such as Excel and Excel Services) use to connect to specific data sources. For example, a special MSOLAP data provider is used to connect to Microsoft SQL Server 2005 Analysis Services. The data provider will be specified as part of the connection in the connection string. You do not need to know a lot about data providers in the context of this article, but you need to understand that:

 Data providers are typically well-tested, stable sets of libraries that can be used to connect to external data.

 Any data provider used by Excel Services must be explicitly trusted by the server administrator. For information about adding a new data provider to the trusted providers list, see [Adding a trusted data provider for Excel Services](#DSDOC_subsection47e6ce086_57b6_4ef2_8117).

note_ddNote:

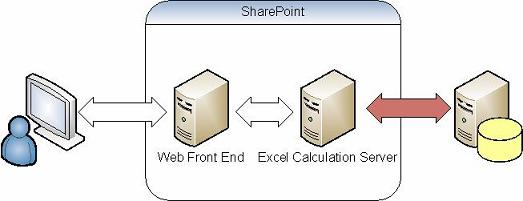
By default, Excel Services trusts many well-known and stable data providers. In most cases, it is not necessary to add a new data provider. Data providers are typically added for custom solutions.

 Data providers handle queries, parsing connection strings, and other connection-specific logic. This functionality is not part of Excel Services. Excel Services cannot control how data providers behave.

## Authentication to external data

Data servers require that a user be authenticated. Authentication is essentially the act of telling the server who you are. The next step is authorization. Authorization is essentially the act of telling the server what you can do. Authentication is required to enable the data server to perform authorization, or to enforce security restrictions that prevent data from being exposed to anyone other than authorized users.

Excel Services needs to tell the data source who is requesting the data. In most scenarios, this is going to be the user who is viewing an Excel report in a browser. Essentially, the purpose of this article is to explain authentication between Excel Services and an external data source. Authentication at this level is shown in the following diagram. The arrow on the right depicts the authentication link from an application server running Excel Calculation Services to an external data source.



There are many ways to implement authentication, but this article is going to focus on the three methods that apply to Excel Services:

 Windows authentication

 SSO

 None

Excel Services determines the type of authentication based on a property of the connection. This property must be explicitly set, and can be set by using Office Excel 2007 client. If the authentication type is missing, the default of Windows authentication is attempted. For more information, see [Specifying the server authentication for an existing connection](#DSDOC_subsection117e6ce086_57b6_4ef2_811).

### Windows authentication

This method uses your Windows user identity to authenticate against a data source. For the scope of this article it is not important to know the specific mechanism that the operating system uses to do this (such as NTLM or constrained delegation). What is important to understand is that Windows authentication is considered to be the most secure way to access external data, and is typically the default method for external data access when using an Excel client to connect to data sources, such as SQL Server 2005 Analysis Services.

In most enterprise environments, Excel Services will be set up as part of a farm with the front-end Web server, back-end Excel Calculation Services server, and data source, all running on different computers, as depicted in the diagram in [Authentication to external data](#DSDOC_section47e6ce086_57b6_4ef2_8117_e7). This means that delegation, or Kerberos, (constrained delegation is recommended) will be required to allow data connections that use Windows authentication. This is because delegation is required to ensure that user identities can be communicated from computer to computer in a trusted and secure way. In a farm deployment, these kinds of connections will not work on Excel Services unless Kerberos is correctly configured.

### SSO

Single sign-on (SSO) is a centralized database that is commonly used to store credentials (a user ID and password pair) that can be used by applications to authenticate to other applications. In this case, Excel Services relies on SSO to store and retrieve credentials for use in authenticating to external data sources.

Each SSO entry contains an application ID that serves as a lookup that is used to retrieve the appropriate set of credentials. Each application ID can have permissions applied so that only specific users or groups can access the credentials that are stored for that application ID.

Given an application ID, Excel Services will retrieve the credentials from the SSO database on behalf of the user who is accessing the workbook (either through the browser or Excel Web Services). Excel Services will then use those credentials to authenticate to the data source and retrieve data.

note_ddNote:

The application ID must be explicitly set for the connection. For information on how to specify an application ID, see [Specifying the server authentication for an existing connection](#DSDOC_subsection117e6ce086_57b6_4ef2_811).

### None

This authentication method simply means that no credential retrieval should take place or that no special action is taken for authentication for the connection. For example, Excel Services should not try to delegate credentials, and should not try to retrieve credentials from the SSO database. In these cases, Excel Services should simply hand the connection string to the data provider and allow the provider to worry about how to authenticate.

In more practical terms, this means that typically a connection string will specify a user name and password that should be used to connect to the data source. However, sometimes the connection string might specify that the integrated security be used. That is, the Windows identity of the user or computer that is issuing the request should be used to connect to the data source. In these cases, the data source will not be connected to as Excel Services, but will instead be connected to as the unattended account. For more information, see [Unattended account](#DSDOC_subsection27e6ce086_57b6_4ef2_8117).

## Data connection libraries and managed connections

A data connection library is a new type of list added to Office SharePoint Server 2007. This is a SharePoint list that is designed to store connection files, which can then be referenced by 2007 Office release applications, such as Office Excel 2007.

Data connection libraries give customers the ability to centrally manage, secure, store, and reuse data connections.

### Reusing connections

Because the data connection library is in a well-known place in Office SharePoint Server 2007 and displays friendly business names and descriptions, people can reuse connections that other people create or configure. A knowledgeable information worker or data expert can create connections, and other people can reuse them without having to understand the details about data providers, server names, or authentication. The location of the data connection library even can be published to Office clients so the data connections will be displayed right in Excel or in any other client application that makes use of the data connection library. For more information, see [Creating a data connection library](#DSDOC_subsection77e6ce086_57b6_4ef2_8117).

### Managing connections

Because workbooks contain a link to the file in a data connection library, if something about the connection changes (such as a server name or an SSO application ID), only a single connection file needs to be updated as opposed to hundreds of workbooks. The workbooks will pick up the connection changes automatically the next time they use that connection file to refresh from Excel or on Excel Services.

### Securing connections

The data connection library is a SharePoint list and supports all the permissions that Office SharePoint Server 2007 does, including per-folder and per-item permissions. The advantage that this provides on the server is that a data connection library can become a locked-down data connection store that is highly controlled. Many users might have read-only access to it so that they can use the data connections, but they can be prevented from adding new connections. By using access control lists (ACLs) with the data connection library, and allowing only trusted authors to upload connections, the data connection library becomes a store of trusted connections. Trusted connections are connections that are known not to contain malicious queries.

Excel Services can be configured to load connection files only from data connection libraries that are explicitly trusted by the server administrator, and to block loading of any embedded connections. In this configuration, Excel Services uses the data connection library to apply another layer of security around data connections.

Data connection libraries can even be used in conjunction with the new Viewer role in Office SharePoint Server 2007 that will allow those connections to be used to refresh workbooks loaded on Excel Services. If the Viewer role is applied, users cannot access the connection file contents from a client application, such as Excel. Therefore, the connection file contents are protected but can still be used for workbooks refreshed on the server.

## Excel Services security and external data

Excel Services has many layers of security. The following subsections address only the concepts that are directly relevant to external data access.

### Trusted file locations

Excel Services will only load workbooks from trusted file locations. A trusted file location is essentially a directory (that might include all subdirectories) that the administrator has explicitly allowed workbooks to be loaded from. These directories are added to a list that is internal to Excel Services. This list is known as the trusted file locations list.

Trusted locations might specify a set of restrictions for workbooks loaded from them. All workbooks loaded from a trusted location will adhere to the settings for that trusted location. Here is a short list of the trusted location settings that affect external data:

 How external data can be accessed. The options for this include:

 No data access allowed (default).

 Only connection files in a Office SharePoint Server 2007 data connection library can be used.

 Connections embedded in workbooks are allowed in addition to connection files from a data connection library.

 Whether to show the query refresh warnings or not.

 Whether to fail the workbook load if external data fails to refresh when the workbook opens. This is used in scenarios where the workbook has cached data results that will change depending on the identity of the user viewing the workbook. The goal is to hide these cached results, and ensure that any user who views the workbook can see only the data that is specific to them. In this case, the workbook will attempt to refresh on open. You can set refresh on open for each connection. If the refresh fails, the workbook is not displayed to users who cannot open it in Excel client.

note_ddNote:

This only works if the workbook is locked down by Viewer role permissions in Office SharePoint Server 2007, because a user who can open the workbook directly in Excel can always see the cached data results.

 External data cache expiration times. Data is shared among many users on the server to improve scale and performance, and these cache life times are adjustable. This accommodates scenarios where query execution should be kept to a minimum because the query might take a long time to execute. In these scenarios, the data often changes only daily, weekly, or monthly as opposed to by the minute or every hour.

### Trusted data connection libraries

As with workbook files, Excel Services will only load connection files from Office SharePoint Server 2007 trusted data connection libraries. A trusted data connection library is a library that the server administrator has explicitly added to an internal trusted list. For information about how data connection libraries allow an administrator to secure and manage connection files, see [Data connection libraries and managed connections](#DSDOC_section57e6ce086_57b6_4ef2_8117_e7). For information about how to trust a data connection library for use with Excel Services, see [Trusting a data connection library on Excel Services](#DSDOC_subsection87e6ce086_57b6_4ef2_8117).

### Trusted data providers

Excel Services will only use external data providers that are added to an internal trusted providers list. This is a security mechanism that prevents the server from using providers that the administrator does not trust. For information about how to trust a data provider, see [Adding a trusted data provider for Excel Services](#DSDOC_subsection47e6ce086_57b6_4ef2_8117).

### Unattended account

The unattended account is a special account that Excel Services impersonates any time it is attempting to authenticate to a data source that is not using Integrated Windows authentication. Because Excel Services has no control over the data provider, and does not directly parse provider-specific connection strings, it needs to mitigate security threats whereby the identity of Excel Services itself can be used to connect to a data source. The unattended account is used to mitigate such threats.

Excel Services will often run with a highly privileged account, and this level of privilege is not appropriate for end users who are trying to only view data. When external data authentication is set to either None or SSO, where the SSO application ID is not storing Windows credentials, the unattended account is impersonated before attempting to connect to data. Because the unattended account is not expected to have privileges to the data source, this will prevent accidental or malicious connections to data sources in the context of a privileged account.

If the unattended account has access to the data source (when authentication type is set to None), a connection will be successfully established by using the credentials of the unattended service account. Use caution when designing solutions that purposely use this account to connect to data. This is a single account that can potentially be used by every workbook on the server. Any user loading a workbook on Excel Services and setting the authentication type to None might be able to view that data by using the server. In some scenarios, this might be needed. However, SSO is the preferred solution for managing passwords on a per-user or per-group basis.

### Trusted subsystem and delegation

When Excel Services is deployed, the method that is used to communicate among the different server farm components is specified. It is configured in either trusted subsystem mode or delegation mode. This mode can be changed only by using the Stsadm.exe command-line tool.

Trusted subsystem (default in a farm deployment) is a mode in which the front-end and back-end server components have a two-way trust. This allows files to be retrieved from Office SharePoint Server 2007 by using the Excel Services account. However, even though Excel Services retrieves the files, it performs a security check to verify that the user requesting the file has the appropriate permissions. In this mode, the back-end Excel Calculation Services server does know the user's identity, but does not have a full user security token and so cannot delegate it to other computers.

Delegation (default in single computer or evaluator deployment) is a mode in which the front-end servers of the farm always delegate the user's identity to the back-end servers. In this case, files are retrieved as the end user who is requesting the workbook instead of the Excel Services account. The back-end Excel Calculation Services server has the user's full identity (security token) and so can delegate it to other servers.

note_ddNote:

In delegation mode, the back-end Excel Calculation Services server can delegate to any computers that are on the same server, but delegation to other computers that reside on a different server requires Kerberos to be configured.

Connections that use Windows authentication will only work when Excel Services is deployed in delegation mode. This is because when the server is in trusted subsystem mode, the back-end calculation component of the application server does not have the end user's (the person viewing the workbooks) full security token and so it cannot delegate the identity to the data source.

## Step-by-step server configuration for external data

This section gives step by step instructions for performing basic configuration on the server side to enable external data connectivity. This includes configuration of all the Office Server components that are required for Excel Services to refresh external data, and therefore covers more than just Excel Services administration.

This section references the SharePoint Central Administration Web site and Shared Services Provider (SSP) administration. This section also contains the instructions for launching those consoles. To complete these steps, you will need access to Central Administration and SSP administration, respectively.

procedure_ddAccess the Central Administration console

|  |
| --- |
| 1. On the taskbar, click Start, point to All Programs, point to Microsoft Office Server, and then click SharePoint 3.0 Central Administration. |

procedure_ddAccess the SSP administration console

|  |
| --- |
| 1. From the Central Administration console, perform either of the following procedures:  2. Select the name of the SSP from the left-hand navigation bar. For example, SharedServices1 as shown in the following figure.  ToAccessSSPadministrationConsole  3. In the top navigation bar, click the Application Management tab.  a. On the Application Management page, click Create or configure this farm's shared services.  b. On the Create or Configure this Farm's Shared Services page, select the name of the SSP. |

### Adding a trusted data provider for Excel Services

Excel Services will only attempt to process connections that use trusted data providers. For most common types of data connections (such as ODBC, OLEDB, SQL Server, and OLAP), it is not necessary to add a provider because by default Excel Services trusts many standard providers. Providers are typically only added for very custom solutions. For more information, see [Data providers](#DSDOC_section37e6ce086_57b6_4ef2_8117_e7).

procedure_ddAdd a new provider for use with Excel Services

|  |
| --- |
| 1. Ensure that the data provider is installed on each server in the farm. This is specific to the data provider being used and is beyond the scope of this article.  2. Launch the SSP administration console. For more information, see [Step-by-step server configuration for external data](#DSDOC_section77e6ce086_57b6_4ef2_8117_e7).  3. In the Excel Services Settings section, click Trusted data providers, as shown in the following figure.  LaunchTheSSPAdminConsole  4. On the Excel Services Trusted Data Providers page, click Add Trusted Data Provider.  5. Fill in the values for the Provider ID, Provider Type, and description, as shown in the following figure.  AddTrustedDataProvider  6. Click OK.  note_ddNote:  The ID that is in the Provider ID should be used in the connection strings that this provider generates. |

### Allowing external data for Excel services

External data must be explicitly enabled per trusted file location.

procedure_ddEnable external data access for a trusted file location

|  |
| --- |
| 1. Launch the SSP administration console. For more information, see [Step-by-step server configuration for external data](#DSDOC_section77e6ce086_57b6_4ef2_8117_e7).  2. In the Excel Services Settings section, click Trusted file locations, as shown in the following figure.  Trusted  3. On the Excel Services Trusted File Locations page, select the name of the trusted file location that you are attempting to load workbooks from, or click the Add Trusted File Location to create a new one, as shown in the following figure.  TrustedFile  4. On the details page for the trusted file location, scroll down to the External Data section, as shown in the following figure.  DetailsPage  5. Select the Trusted data connection libraries only option button to allow access to connection files in a data connection library. Or, select the Trusted data connection libraries and embedded option button to enable connections embedded in a workbook and connections from a data connection library. This is also the location where you can toggle other external data settings that affect the server, such as refresh warnings, data cache time-outs, and so on. |

### Setting the unattended account

The unattended account is required to enable connections that have their authentication set to either None or SSO where the SSO application ID is not using Windows credentials. For more information on the unattended account, see [Unattended account](#DSDOC_subsection27e6ce086_57b6_4ef2_8117). If these types of connections will not be used, the unattended account does not need to be configured.

procedure_ddConfigure the unattended account settings

|  |
| --- |
| 1. Launch the SSP administration console. For more information, see [Step-by-step server configuration for external data](#DSDOC_section77e6ce086_57b6_4ef2_8117_e7).  2. On the Shared Services home page, in the Excel Services Settings section, click Edit Excel Services settings, as shown in the following figure.  ExcelServicesSettings  3. On the Edit Excel Services Settings page, scroll down to the Unattended Service Account section. Enter the domain user name and password of the account you want to use, as shown in the following figure.  UnattendedServiceAccount  4. Click OK. |

### Configuring Office Server single sign-on

SSO enables middle-tier application servers to store and retrieve user credentials. The key to credential retrieval is the application ID.

Application IDs are used to map users to credential sets. This mapping is available for groups and individuals. A group mapping means that every user that is a member of a specific domain group is mapped to the same set of credentials. Group mappings are best for scale and performance on Excel Services because they allow external data cache sharing. Individual mappings map each individual user to that user's own set of credentials.

Office SharePoint Server 2007 can support any SSO provider that implements the pluggable Office SharePoint Server 2007 SSO interface. Office Server ships with its own version of SSO, referred to Office SharePoint SSO. This section only deals with the configuration of Office SharePoint SSO, and does not cover any third-party SSO provider configuration in any detail.

If the user needs more SSO functionality beyond what Office SharePoint SSO provides, another SSO provider can be used.

note_ddNote:

Microsoft also ships a new version of Enterprise Single Sign-On (EntSSO) with Microsoft Host Integration Server and Microsoft BizTalk Server. EntSSO is not supported by Excel Services. EntSSO provides more functionality, such as application IDs that support multiple group mappings, administration of application IDs on a per-application ID basis, and functionality that helps populate and update passwords that are stored in the SSO database.

This section is not intended to be a comprehensive guide on everything a user can do by using SSO. It is only intended to give the basic steps, under common configurations, to get Office SharePoint SSO successfully configured on the server so that it is ready to be used for refreshing data on Excel Services.

#### Start the Microsoft Single Sign-On service on the server

The Microsoft Single Sign-On service should be started on each server in the farm.

procedure_ddStart the Single Sign-On service

|  |
| --- |
| 1. From Administrative Tools, click Services.  2. Double-click Microsoft Single Sign-On Service to launch the Single Sign-On Service Properties page, as shown in the following figure.  ServicesDialog  3. On the General tab of the Single Sign-On Service Properties page, set the startup type to Automatic.  StartTheSSO  4. On the Log On tab of the Single Sign-On Service Properties page, click This account, and then type the domain account that you want to run the service as, as shown in the following figure.  LogOnTab  note_ddNote:  For most evaluator or demonstration deployments, such as a single-click installation, it is easiest to use the same credentials as the account that was used to install Office Server. For more information about account requirements for installing SSO, see [More on Office Server SSO accounts and privileges](#DSDOC_subsection57e6ce086_57b6_4ef2_8117).  5. Click Apply.  6. On the General tab of the Single Sign-On Service Properties page, click Start to start the service, and then click OK. |

#### Configuring SSO on Office Server

SSO must be configured so that application IDs and passwords can be added. For information on how to configure application IDs, see [Creating a new application ID in SSO](#DSDOC_subsection67e6ce086_57b6_4ef2_8117).

procedure_ddConfigure SSO on Office Server

|  |
| --- |
| 1. Launch the Central Administration console. For more information, see [Step-by-step server configuration for external data](#DSDOC_section77e6ce086_57b6_4ef2_8117_e7).  2. On the Operations tab, in the Security Configuration section, select Manage settings for single sign-on, as shown in the following figure.  Operations  3. From the Manage Settings for Single Sign-On page, select Manage server settings, as shown in the following figure.  ManageSingleSign  4. From the Manage Server Settings for Single Sign-On page, enter the credentials of the SSO administrator account and the Enterprise Application Definition administrator account.  note_ddNote:  The Enterprise Application Definition administrator account is used for management of application IDs and passwords in SSO. For most configurations, the account that was used to install the server can be used for both of the SSO administrator account, and the Enterprise Application Definition administrator account. For more information on accounts used to set up SSO, see [More on Office Server SSO accounts and privileges](#DSDOC_subsection57e6ce086_57b6_4ef2_8117).  5. Accept the default database and time-out settings. Click OK to save and close the page. |

#### More on Office Server SSO accounts and privileges

This section provides more detail about the specific memberships, rights, and privileges of the different accounts that are used to configure Office Server SSO. This does not necessarily apply to any third-party pluggable SSO providers.

For evaluation or demonstration purposes, the account that was used to install Office Server can be used to configure SSO. This is the simplest configuration. However, in a production or enterprise deployment, it is considered more secure to ensure the SSO administrator and service account is different from the account that was used to install the server.

 SSO service account   The user that the SSO service account is running as must be a member of the WSS\_Admin\_WPG group on the local machine, and it must be a domain account.

 SSO administrator account   This can be any domain group or user account. The user who is setting the SSO administrator account must be a member of the domain group that the SSO administrator account is getting set to. Or, if an individual account is being used as the SSO administrator account, it must be the account of the current user.

When Excel Services is configured in a trusted subsystem mode, the SSP application pool account must be a member of the SSO administrator group. (For more information, see [Trusted subsystem and delegation](#DSDOC_subsection37e6ce086_57b6_4ef2_8117).) This enables SSO ticketing, which Excel Services uses in such configurations, to work. The SSP application pool account is the security account that is used to run the shared services application pool in IIS.

 SSO Application Manager account   This can be any domain group or individual user account. Accounts that are added as SSO Application Managers must have at least Read access to the Central Administrator site, as this is the site where the SSO accounts are managed from.

 SSO configuration account   This section addresses the requirements of the account that is being used to configure SSO. The account being used to setup and configure SSO must:

 Be a local administrator of the server that stores the master key used for password encryption/decryption. This server is also referred to as the "secret server."

 Be a member of the following SQL Server roles on the SQL Server computer that stores the SSO passwords: Security Admin, Server Admin, and Db Creator.

 Be an Office Server farm administrator. This allows the user to write to the Office SharePoint Server 2007 configuration database during SSO configuration.

 Be a member of the SSO administrator group that is set during SSO configuration.

 Have the ability to log on to the console of the server where SSO is going to be configured.

##### Example of SSO accounts and privileges

An administrator named Bob uses the domain account, CORPDOMAIN\ServerAdmin, to install Office SharePoint Server 2007. This account is an administrator account on every server in the farm, and also has Office Server farm administrative rights. Bob logs on to the computer by using the CORPDOMAIN\ServerAdmin account. Bob adds the account, CORPDOMAIN\ServerService, to the WSS\_Admin\_WPG group on each computer. Bob starts the Single Sign-On service on each computer, running the service as CORPDOMAIN\ServerService.

Bob then launches the Central Administration console to configure SSO. Bob sets the domain group CORPDOMAIN\OfficeServerAdmins to be both the SSO administrator account and the SSO application manager account. The CORPDOMIAN\ServerAdmin account, which Bob is using for this configuration, is a member of the domain group CORPDOMAIN\OfficeServerAdmins. Bob goes to the SSP administration pages to double-check the account that the SSP is running as. He sees that the SSP is running as CORPDOMAIN\SharedServiceAdmin. Bob knows that for Excel Services to work, CORPDOMAIN\SharedServiceAdmin must have rights as an SSO administrator. CORPDOMAIN\SharedServiceAdmin is a member of the domain group CORPDOMAIN\OfficeServerAdmins, which was the group used as the SSO administrator. After configuring the rest of the server and Excel Services, Bob sees that Excel Services can use SSO for external data refresh.

#### Creating a new application ID in SSO

procedure_ddCreate a new application ID in SSO

|  |
| --- |
| 1. Launch the Central Administration console. For more information, see [Step-by-step server configuration for external data](#DSDOC_section77e6ce086_57b6_4ef2_8117_e7).  2. On the Operations tab, in the Security Configuration section, select Manage settings for single sign-on.  3. From the Manage Settings for Single Sign-On page, select Manage settings for enterprise application definitions, as shown in the following figure.  SingleSign  4. From the Manage Enterprise Application Definitions page, click New Item from the toolbar to create a new application ID.  5. Enter the values for the new application. The application name is what users must enter as the SSO application ID into their data connections in Excel client when configuring the connection to work on the server. Typically, the Display name and the Application name should be the same.  6. Enter the e-mail address of the user or group that will be managing this application definition.  7. Select the Account type.  a. Select Group if all users of a specific group should be mapped to a single set of credentials. You will get a chance to define the domain group to map from later.  b. Select Individual if every user should be mapped to a unique set of credentials.  note_ddNote:  Do not choose Group using restricted account. This is not supported by Excel Services.  8. In the Authentication type section, select the Windows authentication check box if the credentials you plan to store for this application ID will be Windows domain credentials.  note_ddNote:  For Excel Services scenarios, because this SSO entry will store user name and passwords, the Field values under the Logon Account Information at the bottom of the page do not need to be altered.  9. If appropriate, configure the settings for an application that uses a group mapping and stores Windows credentials, as shown in the following figure. This will be a common configuration when retrieving from an OLAP source, such as SQL Server 2005 Analysis Services.  GroupMapping  10. Click OK at the bottom of the page to save the application definition.  11. In the Manage Settings for Single Sign-On page, click Manage account information for enterprise applications, as shown in the following figure.  ManageTheActualCredentials  12. From the Manage Account Information for Enterprise Applications page, you can control which accounts can access the credentials stored for an application ID, and manage the actual credentials that are stored for an application ID.  13. From the Enterprise application definition drop-down list, select the application ID that you entered in the last step, as shown in the following figure.  AccountInformation  14. In the Group account name text box, enter the group that should be granted access to the credentials stored for this application ID. This is not the account that is used to access the data source, this is simply the domain group or user account that should map to the credentials that are actually used to authenticate to the data source.  note_ddNote:  If every user in the domain should be allowed to access these credentials, enter DOMAIN\domain users in this text box.  15. Ensure the Update account information option button is selected, and click the Set button.  16. The account information page will launch. Enter the user name and password of the account that should be stored in SSO, as shown in the following figure. This is the account that is used by Excel Services to access the data source. After you have typed the credentials, click OK.  username  note_ddNote:  If the password is left blank when the SSO credentials are Windows credentials, Excel Services will attempt to use Protocol Transitioning on behalf of the end user to connect to the data source. Protocol Transitioning is beyond the scope of this article.  17. You will be returned to the page for managing account information. You can close the browser or click Done to return to the SSO administration home page. |

### Creating a data connection library

The data connection library is a list template in Office SharePoint Server 2007. It can be created almost anywhere a list can be created in Office SharePoint Server 2007.

note_ddNote:

The Report Center site already has a data connection library created by default, and serves as a convenient place to manage all the data connections that are used by reports in that site.

procedure_ddAdd a data connection library to an existing SharePoint site

|  |
| --- |
| 1. From a SharePoint site, click View All Site Content from the left navigation bar for the site, as shown in the following figure.  ViewAllSite  2. Click the Create button near the top of the page, as shown in the following figure.  CreateButton  3. On the next page, in the Libraries section, select Data Connection Library, as shown in the following figure.  DataConnectionLibrary  4. On the next page, enter a name for the data connection library and optional description, as shown in the following figure.  DCLaName  5. Click Create. |

### Trusting a data connection library on Excel Services

Before connection files can be used by Excel Services, the data connection library must be explicitly added to the internal trusted data connection libraries list.

procedure_ddAdd a data connection library to trusted list

|  |
| --- |
| 1. Launch the SSP administration console. For more information, see [Step-by-step server configuration for external data](#DSDOC_section77e6ce086_57b6_4ef2_8117_e7).  2. In the Excel Services Settings section, select Trusted data connection libraries.  3. On the Excel Services Trusted Data Connection Libraries page, enter the URL of the data connection library and enter an optional description, as shown in the following figure.  URLoftheDCL  note_ddNote:  The URL must connect directly to the data connection library, as shown in the previous figure. The URL cannot connect to the forms directory or to the default aspx page. If you copy a link to a data connection library directly from your browser, you must delete any /forms or /default.aspx strings from the URL.  1. Click OK. |

### Exposing the data connection library in the Office client

To make discovery and reuse of connections easier, the data connection libraries can be surfaced in the data connections UI in the Office client (currently displays in Office Excel 2007 and Microsoft Office Visio 2007). This allows users to choose a connection from the data connection library, based on friendly name and description, inline as part of the document authoring experience.

To enable data connection libraries to display directly in the client application, the data connection library must be published from the server to the client computer. The client computer must be associated with that server, or a registry key must be set directly.

#### Publishing the data connection library to the Office client

procedure_ddPublish the data connection library to the Office client

|  |
| --- |
| 1. Launch the SSP administration console. For more information, see [Step-by-step server configuration for external data](#DSDOC_section77e6ce086_57b6_4ef2_8117_e7).  2. In the User Profiles and My Sites section, click Published links to Office client applications, as shown in the following figure.  PublisheLlinksToOfficeClientApplications  3. On the Published Links to Office Client Applications page, click New.  4. Enter the URL to the data connection library.  note_ddNote:  The URL must be directly to the data connection library, as shown in the image and not to the forms directory or the default aspx page. If you copy a link to a data connection library directly from your browser, you must delete any /forms or /default.aspx strings from the URL.  5. Choose Data Connection Library from the Type drop-down list, as shown in the following figure.  DirectlyToTheDCL  6. Click OK.  note_ddNote:  If Audience Targeting is used, only the users that are members of the specified SharePoint audience will receive the link to the data connection library. By default, if Audience Targeting is not used, all users will receive the link to the data connection library if they have permissions to view the data connection library. |

##### Associating the client computer with the server

To enable the client computer to receive the published list of data connection libraries, it must first be associated with the portal server. This can be done by having My Site enabled, and by having a default My Site set.

note_ddNote:

In most real-world deployments, this is already done and in those cases, no action needs to be taken here.

procedure_ddEnable My Site

|  |
| --- |
| 1. Launch the Central Administration console. For more information, see [Step-by-step server configuration for external data](#DSDOC_section77e6ce086_57b6_4ef2_8117_e7).  2. In the top navigation bar, click the Application Management tab.  3. On the Application Management page, in the Application Security section, click Self-service site management, as shown in the following figure.  SelfServiceSiteManagement  4. From the Self-Service Site Management page, select a Web application (the default is acceptable in most deployments), and click On, as shown in the following figure.  OnRadioButton  5. Click OK. |

Setting My Site as the default should be done by the end user who will be reusing connections from a data connection library.

procedure_ddSet My Site as the default

|  |
| --- |
| 1. Navigate to the portal, and click My Site on the top right part of the toolbar, as shown in the following figure.  MySite  2. From the My Site page, select Set as default My Site from the top right of the page, as shown in the following figure.  SetAsDefault  3. Click OK to the dialog box that launches.  note_ddNote:  The default My Site setting can be propagated to other servers for that user via Active Directory. |

#### Setting a registry key to surface a data connection library in the client

This section contains steps that detail how to create a registry key that will cause a data connection library, or any other HTTP or UNC location, to surface in the connection UI.

procedure_ddCreate a registry key to surface a data connection library

|  |
| --- |
| 1. On the taskbar, click Start, and then click Run. Type regedit, and then press ENTER, as shown in the following figure.  regedit  2. Navigate to the folder at HKEY\_CURRENT\_USER\Software\Microsoft\Office\12.0\Common\Server Links\Published.  3. If the Published folder does not exist, you will need to create it. In this case, right-click the Server Links folder and select New Key, as shown I the following figure. Name the Key Published.  NewKey  4. Create a new string value for the Published folder by right-clicking inside the folder and selecting New String value, as shown in the following figure.  NewStringValue  5. Name the string the friendly name of the data connection library.  6. Right-click the string value, and select Modify, as shown in the following figure.  selectModify  7. Enter the HTTP path to the data connection library in the Edit String dialog box, as shown in the following figure.  PathToTheDCL  8. Click OK. |

## Step-by-step workbook configuration for external data

This section covers the common options that need to be configured from the Excel client to allow a workbook to refresh external data when loaded on Excel Services. This section also covers reusing connections from a data connection library, as well as exporting connections to a data connection library.

### Creating a new connection

The simplest way to create a new data connection in an Excel workbook is to use the Data Connection Wizard. This wizard also allows you to configure the authentication options for Excel Services. The Data Connection Wizard produces .odc files, which are linked from the workbook, as described in [Embedded and linked connections](#DSDOC_subsection137e6ce086_57b6_4ef2_811).

procedure_ddCreate a new connection

|  |
| --- |
| 1. In Excel, on the Data tab, in the Get External Data section, select From Other Sources, select From Data Connection Wizard from the drop-down list, as shown in the following figure.  CreatingANewConnection  2. Walk through each screen of the wizard, making appropriate choices for your data source. On the last screen of the wizard, click the Authentication Settings button, as shown in the following figure.  AuthenticationSettingsButton  3. On the Authentication dialog box, select the option button that corresponds to your authentication choice. The types of authentication are described in [Authentication to external data](#DSDOC_section47e6ce086_57b6_4ef2_8117_e7), and are shown in the following figure.  AuthenticationChoice  4. Click OK to close the Authentication dialog box, and then click Finish to end the wizard.  note_ddNote:  This wizard produces an .odc file, and can save this file directly to a data connection library. To do this, choose the browse button on the last screen of the wizard, and type the HTTP path to the data connection library in the corresponding file dialog. When the file is in the data connection library, others can reuse it. |

### Reusing an existing connection from a data connection library

If a data connection library is populated with connection files and is exposed to the Office client, connections from it can be reused directly from within Excel. For more information, see [Exposing the data connection library in the Office client](#DSDOC_subsection97e6ce086_57b6_4ef2_8117).

procedure_ddReuse an existing connection

|  |
| --- |
| 1. From the Excel Data ribbon, select Existing Connections, as shown in the following figure.  ExistingConnections  The DCL folder is shown under the Connection Files on the Network section of the Existing Connections dialog box, as shown in the following exhibit.  ConnectionFiles  2. Each data connection library will have a separate folder. Double-click the folder for a data connection library to see the connections that are stored there, as shown in the following figure.  ChooseTheConnection  3. Select the connection that you want to use, and then click Open.  4. In the Import Data dialog box, select how you want to view your data in Excel, as shown in the following figure.  SetTheServerAuthentication  note_ddNote:  The Table option is not supported in Excel Services. If it is chosen, that workbook will not load in Excel Services. |

### Specifying the server authentication for an existing connection

This section illustrates how to set the server authentication for connections that were previously created in an Excel workbook. For information about creating a new connection, see [Creating a new connection](#DSDOC_subsection107e6ce086_57b6_4ef2_811).

procedure_ddSpecify the server authentication

|  |
| --- |
| 1. From the Excel Data ribbon, in the Connections section, click Connections, as shown in the following figure.  ConnectionsDialog  2. In the Workbook Connections dialog box, which shows all the external data connections that are currently being used by the workbook, select the connection that needs to be changed, and then click Properties, as shown in the following figure.  ConnectionPropertiesDialog  3. In the Connection Properties dialog box, which allows many properties of the connection to be changed, including the refresh on open setting, choose the Definition tab, as shown in the following figure.  DefinitionTab  4. Click the Authentication Settings button.  5. From the Excel Services Authentication dialog box, select the option button that corresponds to the preferred authentication type, as shown in the following figure. For more information about authentication types, see [Authentication to external data](#DSDOC_section47e6ce086_57b6_4ef2_8117_e7).  ExcelServicesAuthenticationSettingsDialog  6. Click OK to close the Excel Services Authentication dialog box, and click OK out of the workbook connections and properties dialogs. |

#### Saving an existing connection to a data connection library

procedure_ddSave an existing connection

|  |
| --- |
| 1. In the Connection Properties dialog box, on the Definition tab, click Export Connection File, as shown in the following figure.  ExportConnectionFile  2. In the File dialog box, enter the HTTP path to the data connection library, and then click Save. When an .odc file is exported in this manner, the workbook connection becomes linked to that .odc file, as described in [Connections and Excel workbooks](#DSDOC_section27e6ce086_57b6_4ef2_8117_e7). |

##### More about the properties on the Definition tab

The Definition tab on the Connection Properties dialog box has other properties that can affect how connections are used and behave on both the client computer and the server. All of these properties are persisted in the .odc file, which is generated by clicking Export Connection File, and will be inherited by any workbook that later uses that .odc file.

These settings are respected in both Excel client and Excel Services. This section contains notes on how two of the most important properties affect connections across client computer and server. For more information about the high-level behavior of both of these settings, see [Connections and Excel workbooks](#DSDOC_section27e6ce086_57b6_4ef2_8117_e7).

 Connection file   This is the path to the connection file that this workbook connection maintains a link to. To change to a different connection file, choose the browse button and enter a path to a new connection file.

note_ddNote:

Changing any settings on the Definition tab of the Connection Properties dialog box will break the link to the connection file because the copy of the connection in the workbook will no longer be an exact replica of the connection file.

 Always use connection file   This specifies whether to use the embedded copy of the connection first, or whether to always use the contents of the linked connection file to refresh data. If this check box is selected, the embedded copy of the connection information is always ignored, regardless of whether the connection file connection is successful.

## Frequently asked questions

### How do I get Microsoft Access data into my workbooks on Excel Services?

Workbooks that refresh data from an Access database are not supported with the features that come with Excel Services. This is because these types of solutions have problems scaling and performing in an enterprise server environment. Although it might be possible to make this work by adding the right provider to the trusted providers list and installing any required Data Source Name (DSN) files on the server, it is not supported.

### How do I use other workbooks as data sources on Excel Services?

This is not supported in this version of Excel Services. Linked workbooks are an unsupported feature, and those workbooks will fail to load on the server. You might consider moving the data from the linked workbooks into a single workbook. An alternate approach is to use a user-defined function (UDF) to fetch data from a different workbook.

### Why don't my Windows authentication connections work even when I have correctly configured Kerberos in my farm?

This is happening either because the user who is viewing the workbook does not have correct permissions on the data source, or because the server's Access Model was configured as a trusted subsystem. In the trusted subsystem mode, Windows authentication style connections fail automatically as the back-end calculation server does not have the full identity (security token) of the user and therefore cannot delegate to the data source.

### If the credentials are not delegated, how can Excel Services make per-user permission checks on files?

Even if the Access Model is a trusted subsystem, Excel Services can still do per-user permissions checks on files stored in Office SharePoint Server 2007. Excel Services is part of Office SharePoint Server 2007, and so it is trusted to do per-user permission checks even when it cannot delegate an end user's identity; however, it does not affect how Excel Services connects to external data.

In these topologies, as described in the previous paragraph, Windows authentication–type connections do not work because the back-end application server cannot delegate the workbook viewer's identity.

### What is the guidance around using local cubes on the server?

Local cubes for SQL Server 2005 Analysis Services are not supported by Excel Services. These local cubes do not scale well in an enterprise production environment because they were not designed to meet the demands of many users refreshing data immediately. It is not recommended to use these with Excel Services.

### How can I have more control over how external data is accessed from the server?

Trusted file locations allow a granular level of control over how workbooks behave on the server, including how they refresh external data. When a user loads a workbook on Excel Services, the workbook trusted location is resolved to the deepest level. For example, if a workbook is loaded from http://server/site/doc%20lib/, and a set of trusted location rules exists for http://server, and a different set exists for http://server/site/doc%20lib, the rules from the latter will be applied. This makes it possible to enable scenarios where a particular set of security restrictions are applied at a very wide, or very granular, level.

For example, the entire portal can be added as a trusted location (http://server or http://).

note_ddNote:

You must select the Include Children check box to allow workbook loading from all subdirectories. You might choose to configure the trusted location settings at this level to always show data warnings, and only allow refresh by using data connection libraries. Workbooks stored in a more secure document library might be enabled to load any data connections (data connection library or embedded). The external data cache time-out values might be extremely high because workbooks in this document library take a long time to refresh data and data is not updated very often.

Administrators are encouraged to add trusted file locations, and change what is allowed for each, in a way that fits their particular security requirements.

### What factors should I consider regarding performance and external data?

There are a number of considerations to take into account when designing external data access from Excel Services.

 Excel Services shares data caches in the middle tier. The cache is shared when the connections are identical, and the credentials used to connect to the data source are the same. This ensures that users have rights to the same data. This means that Excel Services scales better when the same credentials are used by many users to connect to data. SSO group mappings, None where a user name/password are saved in a connection string, or None where the unattended account is used are all good authentication types for these cases. (Although it should be noted that SSO is the best option here from a security point of view.)

 For SQL Server 2005 Analysis Services and later, data caches can be shared even if individual SSO or Windows credentials are used. This is an optimization that only applies to SQL Server 2005 Analysis Services or later, and it only applies if the users are members of the same groups on Analysis Services, and if there are not any cube calculations or security that relies on an individual user's identity.

 Increase external data cache lifetimes where it makes sense. If a workbook takes a particularly long time to refresh data due to the size of a query, consider increasing the data cache timeout for that trusted location.

 Disable interactivity in the dashboard for OLAP PivotTables. When users interact with OLAP-based PivotTables, new queries are issued against the back-end data source for that user's session. In this case, that user will stop sharing the data cache. Consider publishing the workbook so that the view of the data is appropriate for most users, and disabling interactivity where it makes sense to do so.

### How can I secure my data so that it is viewable only from a workbook published to Excel Services?

Excel Services takes advantage of the View Only permission set in Office SharePoint Server 2007. All users who are added to the Viewers group in Office SharePoint Server 2007 get this level of permissions by default. This only applies to files loaded from Office SharePoint Server 2007 when the trusted file location is set to be of type SharePoint.

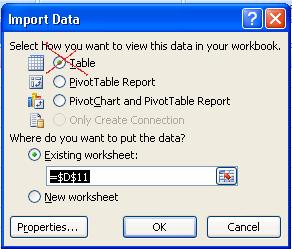
Users who have View Only permissions have the right to load, render, interact, refresh, recalculate, and take snapshots of workbooks that are loaded on Excel Services. These users cannot access the actual file source, or contents, of the workbook directly. This means that they cannot download or save the workbook, open it directly in Excel, or access the file contents through any method other than Excel Services. This is the prescribed way to secure, "one version of the truth" workbooks.

In this case, users can see only the parts of the workbook that are marked as "Viewable on the Server," by the workbook author who uses the Publish to Excel Services feature in Excel client. By publishing the correct parts of the workbook and securing the workbook with View Only permissions, the workbook author can ensure that no data or proprietary information from the workbook is exposed when it should not be.

In cases where users are allowed to download the source of the workbook, and that user does not have direct access to the data source, if the data connection uses SSO or the unattended account to refresh on the server, the user cannot refresh that connection from Excel client. This is because Excel client cannot use the server's unattended account or SSO to refresh connections directly. The workbook author should take care in these cases to remove any cached data from the workbook, or ensure that any cached data in the workbook is allowed to be viewed by all users who might open the workbook in Excel client.

### I followed the instructions in this article, but when I load my workbook on the server I see some unsupported features error talking about Query Tables. How can I fix it?

When authoring a workbook, and bringing the external data into a workbook for the first time, you are presented with an Import Data dialog box, as shown in the following figure, with choices on how to visualize the data.



When you select Table from this dialog box, a Query Table is created. These structures are not supported in Excel Services, and the workbook will not load on the server. To correct this, delete the table from the workbook. Reconnect to data, and select PivotTable Report next time.

A PivotTable can be made to look a lot like a Query Table by using the PivotTable Tools, Design tab, from the ribbon. Try turning off Subtotals, Grand totals, and drill indicators. Then choose Tabular form for the report layout.

Another option, which requires custom code, is to use a UDF to retrieve the data, and return it to the workbook as a table. This can be rendered, loaded, and refreshed on Excel Services. This is beyond the scope of this article.

### I have an ODBC connection, and therefore I do not have an .odc file. How can I use my connection with a data connection library so that it will work on Excel Services?

Excel Services works only with .odc files. If you have a connection in a workbook that you want to save to a data connection library and have work with Excel Services, you will need to export that connection as an .odc file. The Export Connection File command from the Connection Properties dialog box described in can be used to do this as it always exports .odc files.

### How do View Only permissions and .odc files in a data connection library work?

View Only permissions grant users the right to use an Excel file on Excel Services, but not from any other client application — not even Excel. The .odc files work the same way. If a workbook uses an .odc file to refresh data, the server copy of that workbook will correctly refresh for a user with View Only permissions to the .odc file. However, even if the user has permissions to open the workbook in Excel client, the connection will cannot use the .odc file to refresh from Excel client. The user can only make use of the .odc file by refreshing workbooks running on the server that uses the .odc file.

Typically, the user will have the same View Only permission restrictions on the workbook and the .odc file. If users are intended to open the workbook in Excel client but not the .odc file, the embedded connection in the workbook should not expose the content s of the .odc file. In this case, the embedded connection should not be a copy of the .odc file. Ensure the cached data in the workbook is not exposing data from the data source to which the .odc file points.

## See Also

[Excel Services](http://go.microsoft.com/fwlink/?LinkId=78464&clcid=0x409)

[Excel Services Architecture](http://go.microsoft.com/fwlink/?LinkId=78465&clcid=0x409)

[Plan Excel Services security](#DSDOC_a49883a7_de84_4a66_8fa0_7c7d125f23)

[Determine resource requirements to support Excel Services](#DSDOC_fb6928ce_49f8_492a_abff_5bd00ed588)

[Single Sign](http://go.microsoft.com/fwlink/?LinkId=78476&clcid=0x409)

[Implementing a Pluggable SSO Provider](http://go.microsoft.com/fwlink/?LinkId=78479&clcid=0x409)

[Creating Custom Solutions with Excel Services](http://go.microsoft.com/fwlink/?LinkId=78480&clcid=0x409)

[Kerberos Authentication in Windows Server 2003](http://go.microsoft.com/fwlink/?LinkId=78481&clcid=0x409)

# VII Plan search

In this chapter:

 [Chapter overview: Plan search (Office SharePoint Server)](#DSDOC_e8c0fccd_8364_4352_8778_c9c46a668b)

 [Identify your search team (Office SharePoint Server)](#DSDOC_b4b9ceae_3837_4a79_8097_d6381500e4)

 Levels of administration for search

 [Plan to crawl content [Office SharePoint Server]](#DSDOC_82c09ad6_6137_438d_a324_16a7f99e12)

 [Plan the end user search experience [Office SharePoint Server]](#DSDOC_a56532d7_9814_4a0c_a308_f2369eaf30)

 Plan to customize search

# Chapter overview: Plan search (Office SharePoint Server)

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [Why two search services?](#DSDOC_section1e8c0fccd_8364_4352_8778_c9)

 [Plan the search team](#DSDOC_section2e8c0fccd_8364_4352_8778_c9)

 [Plan to crawl content](#DSDOC_section3e8c0fccd_8364_4352_8778_c9)

 [Plan the end-user search experience](#DSDOC_section4e8c0fccd_8364_4352_8778_c9)

Planning search is an important part of planning any deployment of Microsoft Office SharePoint Server 2007. If you devote time to plan how search is implemented, you can save time in the future and can reinforce the effectiveness of other business processes.

Planning carefully for search can prepare you for an initial limited deployment. You can continue to refine your search implementation, such as adding additional crawled content to the content index. Using an effective planning process can help make your search solution more effective, even if you implement the solution in stages or your needs continue to evolve after initial deployment.

You should also plan the following practical aspects of using search features:

 What roles will be performed by the people who will manage the search features.

 Whether you want to customize search Web Parts or the Search Center site (Enterprise edition only).

 Whether you want to use custom search applications.

 Whether you need to include data from external sources.

## Why two search services?

Office SharePoint Server 2007 provides two search services: Office SharePoint Server Search and Windows SharePoint Services Help Search. Each of these services can be used to crawl, index, and query content, and each service uses a separate index.

The Office SharePoint Server Search service is based on the search service that is provided with earlier versions of SharePoint Products & Technologies, but with many improvements. You should use the Office SharePoint Server Search service to crawl and index all content that you want to be searchable (other than the Help system).

note_ddNote:

For the purposes of this planning guide, the Office SharePoint Server Search service is referred to as the Search service.

The Windows SharePoint Services Help Search service is the same service provided by Windows SharePoint Services 3.0, although in Windows SharePoint Services 3.0 it is called the Windows SharePoint Services Search service. Windows SharePoint Services 3.0 uses this service to index site content, index Help content, and serve queries.

As its name implies, in Office SharePoint Server 2007 the purpose of the Windows SharePoint Services Help Search service is to enable searching of the Help system that is built into Office SharePoint Server 2007.

Because the Windows SharePoint Services Help Search service uses an index that is separate from the other search service, users' queries in the Search box for the Help system return hits for only Help content. If you do not want users to be able to search the Help system, you do not need to start this service.

## Plan the search team

You need to identify the search team and assign administration roles to the people on the team. Depending on the size of your organization, some members of the search team might be assigned more than one role. For more information, see [Identify your search team (Office SharePoint Server)](#DSDOC_b4b9ceae_3837_4a79_8097_d6381500e4).

## Plan to crawl content

Before users can search for content, you must make that content available to search queries by crawling the content to build the content index. You plan for crawling by determining where the content is that you want to crawl, what type of content it is, and security credentials for accessing the content, among other things. This section of the guide can help you make the decisions necessary to effectively plan for crawling. It provides a worksheet that you can use to record the choices you make during this part of the planning phase. You can then use your completed worksheet when you deploy search.

For more information, see [Plan to crawl content [Office SharePoint Server]](#DSDOC_82c09ad6_6137_438d_a324_16a7f99e12).

## Plan the end-user search experience

After you plan how to crawl content, you can then plan the end-user search experience. This includes determining what users see when performing queries and what they see in the search results pages. For more information, see [Plan the end user search experience [Office SharePoint Server]](#DSDOC_a56532d7_9814_4a0c_a308_f2369eaf30).

# Identify your search team (Office SharePoint Server)

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [About the search planning team](#DSDOC_section1b4b9ceae_3837_4a79_8097_d6)

 [About the search planning process](#DSDOC_section2b4b9ceae_3837_4a79_8097_d6)

 [Plan the search deployment and operations teams](#DSDOC_section3b4b9ceae_3837_4a79_8097_d6)

 [Worksheet](#DSDOC_section4b4b9ceae_3837_4a79_8097_d6)

## About the search planning team

Before you begin planning the features and deployment of the Office SharePoint Server Search service for Microsoft Office SharePoint Server 2007, you should understand the role of the search planning team. Involve the following administrators in planning for search:

 Shared Services Provider (SSP) administrators, who manage large content sets within a server farm or across multiple farms. SSP administrators understand the high-level content needs of the organization and what information is important for users across their content set.

 Site collection administrators, who manage the specific content needs of a single site collection, often scoped to a division or specific organizational purpose or product line.

 Application administrators, who manage the end-user experience, which includes defining keywords, Best Bets, and scopes. Administrators must plan the end-user search experience at the site collection level, but they can also plan it for individual sites.

 IT administrators, who plan architecture and topology details for one or more server farms in the organization based on the content needs identified by others. Typically, IT administrators are not concerned with content except as it affects IT operations such as availability, reliability, and capacity planning.

## About the search planning process

The search planning process encompasses the following major steps:

1. You identify the content managed by SSP administrators and site collection administrators during content planning, and content needs are reflected in the taxonomy developed for the organization. For more information, see [Determine the information architecture of your site](#DSDOC_7a74c8bf_83a2_4ee1_82e7_c2e9dee789).

2. Site collection administrators and SSP administrators consider the search capabilities they want to implement to meet the content needs, and communicate the required capabilities to IT administrators and application administrators.

3. The high-priority content needs are addressed in IT planning and deployed in a pilot deployment, and then other content needs are met in successive waves of planning.

4. When there is sufficient content, and the search capabilities for that content are available, the initial deployment is made available to the entire organization.

5. Depending on the amount of content and level of planning detail, planning and implementation continue after initial deployment.

## Plan the search deployment and operations teams

To deploy the Office SharePoint Server Search service, each of the types of administrators listed in the previous section is required. To perform regularly scheduled operations, you will need an SSP administrator and a site collection administrator, at a minimum. The same people who are on the search planning team might also be involved in the deployment and operations phases, but this can vary between organizations.

## Worksheet

Use the following worksheet to record information about your search planning team and to record information about other team members who will not be involved in the planning phase but might be involved in the deployment or operations phases:

 [Search team worksheet](http://go.microsoft.com/fwlink/?LinkId=73621&clcid=0x409) (<http://go.microsoft.com/fwlink/?LinkId=73621&clcid=0x409>)

# Plan to crawl content [Office SharePoint Server]

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [About crawling content](#DSDOC_section182c09ad6_6137_438d_a324_16)

 [Plan content sources](#DSDOC_section282c09ad6_6137_438d_a324_16)

 [Plan crawler impact rules](#DSDOC_section382c09ad6_6137_438d_a324_16)

 [Plan crawl rules](#DSDOC_section482c09ad6_6137_438d_a324_16)

 [Plan file-type inclusions and Ifilters](#DSDOC_section582c09ad6_6137_438d_a324_16)

 [Plan search settings that are managed at the farm level](#DSDOC_section882c09ad6_6137_438d_a324_16)

 [Worksheet](#DSDOC_section982c09ad6_6137_438d_a324_16)

Microsoft Office SharePoint Server 2007 includes the ability, not found in previous versions of Microsoft SharePoint Products and Technologies, to crawl and index content on other SharePoint farms, other Web sites, file shares, business data, and so on. This greatly increases the amount of content you make available to search queries, because you can crawl content on other SharePoint farms, Web sites on the Internet, business data stored in a line of business application, and so on.

One way that Office SharePoint Server 2007 is notably different from previous versions is that the service used for crawling and indexing content is part of a shared services provider (SSP) and all content crawled using the SSP is indexed to a single content index. In most organizations, only one SSP is used to crawl and query all content, so these settings apply to all content sources in the organization.

During deployment, you will create one or more SSPs, and then create content sources for each SSP. During planning, on the other hand, it can help to plan content sources first. In the small number of cases where more than one SSP is needed for isolating highly sensitive content, planning content sources can help identify the need for multiple SSPs. For more information about using multiple SSPs, see Plan for search administration.

Careful planning of your initial deployment is essential. We recommend that you use the information in this article to help you make the necessary decisions and gather information about the content you want to crawl and how and when you want to crawl it. At key points in this article we provide a Worksheet action table that recommends you fill out the section of the worksheet that pertains to the section you just read. You can either record your decisions on the worksheet as you work through this article or all at once at the end of this article. Either way, a completed worksheet is a valuable asset to have when you deploy search.

note_ddNote:

This article steps you through the process of planning for search for one content index. If you discover as you plan to crawl your content that you want to use an additional content index, record your planning decisions for each SSP on separate worksheets.

## About crawling content

Before you can use the enterprise search functionality in Office SharePoint Server 2007 to search for content, you must first crawl the content that you want to make available to search queries. Crawling content is the process by which the system accesses and parses content and its properties to build a content index from which search queries can be serviced. SSP administrators create content sources that specify what type of content is crawled, what URLs to crawl, and how deep and when to crawl. After a content source is created, an SSP administrator can use the content source to crawl the content specified in the content source.

note_ddNote:

Crawling content by using a particular content source is sometimes called "crawling the content source."

By default, Office SharePoint Server 2007 adds the URL of the top-level site of each site collection that you create to in the Web application that uses the same Shared Services Provider (SSP) to a content source named Local Office SharePoint Server sites. This is sometimes called the default content source. SSP Administrators can use this content source to crawl and index all content in your Web application.

note_ddNote:

The content defined by the default content source is not crawled automatically. To crawl and index the content you want available for search queries, you must use this default content source or another content source that you create to crawl the content.

SSP administrators can modify the default content source, create additional content sources for crawling other content, or both. For example, they can configure the default content source to also crawl content on a different server farm or they can create a new content source to crawl other content. They can create crawl rules for start addresses that apply to all content sources in the SSP based on what content and data at each start address is relevant to the organization, and configure settings for each content source.

note_ddNote:

A crawl rule is a set of preferences that applies to a specific URL or range of URLs that you can use to include or exclude items you want to crawl and specify the content access account to use when crawling that URL or range.

With previous versions of Microsoft SharePoint Products and Technologies, administrators managed content indexes, which are the underlying collections of all content crawled by content sources. With Office SharePoint Server 2007, this is no longer necessary. The single content index for each SSP is automatically created based on the settings selected for each content source, and content indexes are no longer displayed to administrators.

## Plan content sources

Office SharePoint Server 2007 uses content sources to crawl content in your site collections or on related external sites or business data applications. Other search features filter or modify content after it has been crawled. Effective planning for content sources can help you to build search capability during your initial deployment that enables you to configure and manage content across your organization based on key subsets of content and data, content and data external to your Office SharePoint Server 2007 deployment, or content and data external to your organization.

The system automatically adds the top-level Web address of each site collection that is served by the SSP to the default content source. This is done so that all content served by the SSP is available to search after the initial crawl that uses that content source is performed.

Your information architecture should also suggest additional content sources to create for each of your site collections in each of your Web applications. To manage and schedule crawls independently, you can create content sources for crawling a subset of content throughout the SSP. This is useful to crawl high-priority or quickly changing content more frequently without needing to recrawl all content.

Examples of content for which you might want to plan additional content sources are listed in the following table.

|  |  |
| --- | --- |
| This type of content source | Includes this type of content |
| SharePoint sites |  SharePoint sites from the same farm or different farms   Sites in the Site Directory |
| Web sites |  Other Web content in your organization not found in SharePoint sites   Content on Web sites on the Internet |
| File shares |  Content on file shares within your organization |
| Exchange public folders |  Exchange Server content |
| Business data |  Business data stored in line of business applications |

Each content source can contain one or more start addresses that point to locations of the same content source type that is selected for the content source. For example, you can create a content source that contains URLs for SharePoint sites and another that contains URLs for file shares, but you cannot create a single content source that contains URLs to both SharePoint sites and file shares.

Adding the URL of the top-level site in site collection causes all subsites to be crawled unless you exclude them by using a crawl rule. For more information about crawl rules, see Plan crawl rules.

You can also crawl SharePoint sites that are part of a Microsoft SharePoint Portal Server version 2 or Windows SharePoint Services version 2 site collection. However, the crawler cannot automatically crawl all subsites in a site collection from a previous version of SharePoint Products and Technologies. Therefore, when crawling a previous version SharePoint sites, you must specify the URL of each top-level site and each subsite that you want to crawl.

Whether you group content in a content source or create additional content sources depends largely upon administration considerations. Administrators often make changes that require a full update of a particular content source. Changes to crawl require a full crawl of the affected content source. To make administration easier, organize content sources in such a way that updating content sources, crawl rules, and crawling content is convenient for administrators to do simultaneously with their other planned administration tasks.

Content on file shares and servers outside your server farm should be organized by availability. Examples include mail servers, Web servers that do not contain SharePoint sites, or file servers. If the servers containing content are available at the same time, you are more likely to successfully crawl all the content specified in the content source, with less need to run full updates later.

To summarize, consider the following when planning your content sources:

 A particular content source can be used to crawl only one of the following content types: SharePoint sites, Web sites that are not SharePoint sites, file shares, Exchange public folders, and business data.

 You can specify one or more start addresses (URLs) for each content source, but each URL in a particular content source must be of the same content source type.

 For a particular content source, you can choose how deep to crawl the start addresses. This configuration setting, or in some cases set of configuration settings apply to all start addresses in the content source. The available choices on how deep you can crawl the start addresses differ depending upon the content source type that is selected.

 You can schedule when to perform either a full or incremental crawl for the entire content source. This means you must plan your content sources around your crawl schedules.

 To effectively crawl all the content needed by your organization, use as few content sources as you can.

### Plan default content access account

The default content access account is the account that is used by default when crawling content sources. This account is selected by the SSP administrator during post-setup configuration. The default content access account must have read access to all content that is crawled, or the content will not be crawled and will not be available during search queries. For individual URLs in a content source, you can use crawl rules to specify a different content access account to use when crawling those URLs.

We recommend that you select a default content access account that has the broadest access to most of your crawled content, and only use other content access accounts when security considerations require separate accounts. For each content source you plan, identify the start addresses that cannot be accessed by the default content access account and plan to add content access accounts for those start addresses. Administrators can configure additional content access accounts in crawl rules for the relevant start addresses.

note_ddNote:

Do not use the same domain account for the default content access account that you use for the Application Pool. Doing so will cause minor versions of files (history) in SharePoint sites to be crawled and indexed.

For more information about the planning considerations for content access accounts, see [Plan crawl rules](#DSDOC_section482c09ad6_6137_438d_a324_16).

|  |
| --- |
| Worksheet action |
| Record the content access account that the crawler will use, by default, when crawling content in the Default content access account section of the [Plan to crawl content worksheet](http://go.microsoft.com/fwlink/?LinkID=73748&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73748&clcid=0x409). |

### Plan for external content

Two types of external content can be useful for people in your organization:

 Content within a Web application that uses a different SSP that you want to crawl by using this SSP.

 Internet or extranet content that is not created or controlled by people in your organization.

Whenever possible, use only one SSP to crawl all content for your organization. Typically, if content on a Web application that uses a separate SSP is relevant enough to be included in a content source for your SSP, the Web application should use the same SSP as the Web applications that are crawled using your SSP. However, there are valid reasons to use more than one SSP for crawling content. For example, you might want some content in a separate content index for security reasons or you might want to crawl content in separate geographical regions.

note_ddNote:

You can use one SSP to crawl content on servers in separate geographical regions, but performance can suffer depending upon the bandwidth of your Internet link.

In some cases, you might want to include a subset of content in your organization from a Web application that uses a different SSP. We recommend that you avoid this situation by carefully planning your information architecture, SSPs, and site structure. If you must crawl content on a Web application that uses a different SSP, ensure that the user account used to crawl the content (either the default content access account or a different content access account defined by a crawl rule) has read permission to the content, and try to group the start address in a content source with other content available at similar times, or that is conceptually related.

A common scenario involves content outside the control of your organization that relates to the content on your SharePoint sites. You can add the start addresses for this content to an existing content source or create a new content source for external content. Because availability of external sites varies widely, it is helpful to add separate content sources for different external content. This way they can be crawled at different times than your other content sources. You can then update each set of external content on a crawl schedule that makes sense for the availability of each site.

### Plan content sources for business data

Business data content sources require that the applications hosting the data are first registered in the Business Data Catalog, and the properties mapped to managed properties that are consistent with your search schema. Business data start addresses cannot be combined with start addresses for other content, so you must separately manage business data content sources.

Often, the people who plan for integration of business data into your site collections will not be the same people involved in the overall content planning process. Include business application administrators in your content planning teams so that they can advise you how to integrate their data into your other content and effectively present it on your site collections.

For more information about planning business data search, see [Plan for business data search](#DSDOC_2b7121fc_a1f2_469d_ac1c_7b12283897).

### Plan crawl settings

For each content source, you can select how extensively to crawl the start addresses in that content source. The options available in the properties for each content source vary depending upon the content source type that is selected. The following table describes the crawl settings options for each content source type.

|  |  |
| --- | --- |
| Content source type | Crawl settings options |
| SharePoint sites |  Everything under the hostname for each start address   Only the SharePoint site of each start address |
| Web sites |  Only within the server of each start address   Only the first page of each start address   Custom — specify page depth and server hops. The default setting for this option is unlimited page depths and server hops. |
| File shares |  The folder and all subfolders of each start address   Only the folder of each start address |
| Exchange public folders |  The folder and all subfolders of each start address   Only the folder of each start address |
| Business data |  Crawl entire Business Data Catalog   Crawl selected applications |

The most important factors to consider when planning the crawl settings of content sources are the relevance of the information and the impact to performance.

For best results for SharePoint sites:

 Crawl only the SharePoint site of each start address if the content available on linked sites is not likely to be relevant, and the content on the site itself is relevant.

 Crawl everything under the hostname of each start address if the links on the start address tend to point to relevant content.

For best results for Web sites:

 Crawl only within the server of each start address if the content available on linked sites is not likely to be relevant, and the content on the site itself is relevant.

 Use the custom option to specify the number of pages deep and number of server hops to crawl if you want to limit how deep to crawl the links on the start addresses.

### Plan crawl schedules

SSP administrators can configure the crawl schedules independently for each content source. For each content source, they can specify a time to do full crawls and a separate time to do incremental crawls. It is a requirement that a full crawl is run for a particular content source before incremental crawls can be run.

We recommend that you plan crawl schedules based on the availability, performance, and bandwidth considerations of the servers running the search service and the servers hosting the crawled content.

For best results, plan crawl schedules in the following ways:

 Group start addresses in content sources based on similar availability and with acceptable overall resource usage for the servers that host the content.

 Schedule incremental crawls for each content source during times when the servers that host the content are available but the demand on the resources of the server are low.

 Stagger crawl schedules so that the load on the servers in your farm is distributed over time.

 Schedule full crawls less frequently than incremental crawls.

 Schedule administration changes that require a full crawl to occur shortly before the planned schedule for full crawls.

You can adjust schedules after the initial deployment based on the performance and capacity of servers in the farm and the servers hosting content.

|  |
| --- |
| Worksheet action |
| Record the decisions you make about content sources for your initial deployment in the tables in the Content sources section of the [Plan to crawl content worksheet](http://go.microsoft.com/fwlink/?LinkID=73748&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73748&clcid=0x409). |

### Protocol handlers

All content that is crawled requires the use of a protocol handler to gain access to that content. Office SharePoint Server 2007 provides protocol handlers for all common Internet protocols, such as HTTP, HTTPS, and FTP. However, if you want to crawl content that requires a protocol handler that is not installed with Office SharePoint Server 2007, you must install the third-party or custom protocol handler before you can crawl that content.

The protocols that are supported by the default protocol handlers are: bdc, bdc2, file, http, https, rb, rbs, sps, sps3, sps3s, spsimport, spss, sts, sts2, sts2s, sts3, and sts3s.

|  |
| --- |
| Worksheet action |
| Record the decisions you make about protocol handlers for your initial deployment in the Protocol handlers section of the [Plan to crawl content worksheet](http://go.microsoft.com/fwlink/?LinkID=73748&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73748&clcid=0x409). |

## Plan crawler impact rules

Crawler impact rules are particularly important when crawling external content sources because crawling uses resources on the crawled servers.

Crawler impact rules enable administrators to manage the impact your crawler has on the servers being crawled. For each crawler impact rule, you can specify a single URL or use wildcard characters in the URL path to include a block of URLs to which the rule applies. You can then specify how many simultaneous requests for pages will be made to the specified URL or choose to request only one document at a time and wait a number of seconds that you choose between requests.

The following table shows the wildcard characters that you can use in the site name when adding a rule.

|  |  |
| --- | --- |
| Use | To |
| \* as the site name | Apply the rule to all sites. |
| \*.\* as the site name | Apply the rule to sites with dots in the name. |
| \*.site\_name.com as the site name | Apply the rule to all sites in the site\_name.com domain (for example, \*.adventure-works.com). |
| \*.top-level\_domain\_name (such as \*.com or \*.net) as the site name | Apply the rule to all sites that end with a specific top-level domain name (for example, .com or .net). |
| ? | Replace a single character in a rule. For example, \*.adventure-works?.com will apply to all sites in the domains adventure-works1.com, adventure-works2.com, and so on. |

You can create a crawler impact rule for \*.com that applies to all Internet sites whose addresses end in .com. For example, an administrator of a portal might add a content source for samples.microsoft.com. The rule for \*.com applies to this site unless you add a crawler impact rule specifically for samples.microsoft.com.

For content within your organization that other administrators are crawling, you can coordinate with those administrators to set crawler impact rules based on the performance and capacity of the servers. For most external sites, this coordination is not possible. Requesting too much content on external servers or making requests too frequently can cause administrators of those sites to limit your future access if your crawls are using too many resources or too much bandwidth. Therefore, the best practice is to crawl too little rather than crawl too much. In this way, you can mitigate the risk that you will lose access to crawl the relevant content.

During initial deployment, set the crawler impact rules to make as small an impact on other servers as possible while still crawling enough content frequently enough to ensure the freshness of the crawled content.

During the operations phase, you can adjust crawler impact rules based on your experiences and data from crawl logs.

|  |
| --- |
| Worksheet action |
| Record the decisions you make about crawler impact rules for your initial deployment in the Crawler impact rules section of the [Plan to crawl content worksheet](http://go.microsoft.com/fwlink/?LinkID=73748&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73748&clcid=0x409). . |

## Plan crawl rules

Crawl rules apply to a particular URL or set of URLs represented by wildcards (also referred to as the path affected by the rule). You use crawl rules to do the following things:

 Avoid crawling irrelevant content by excluding one or more URLs from being crawled. This also helps to minimize the use of server resources and network traffic, and to increase the relevance of search results.

 Crawl links on the URL without crawling the URL itself. This option is useful for sites with links of relevant content when the page containing the links contains irrelevant information..

 Enable complex URLs to be crawled. This option crawls URLs that contain complex characters, such as the question mark. Depending upon the site, these URLs might or might not include relevant content. Because complex URLs can often redirect to irrelevant sites, it is a good idea to only enable this option on sites where the content available from complex URLs is known to be relevant.

 Enable content on SharePoint sites to be crawled as HTTP pages. This option enables the index server to crawl SharePoint sites that is behind a firewall or the site being crawled is restricting access to the Web service used by the crawler.

 Specify whether to use the default content access account, a different content access account, or a client certificate to use for crawling the specified URL.

note_ddNote:

Crawl rules apply simultaneously to all content sources.

Often, most of the content for a particular site address is relevant, but a specific subsite or range of sites below a particular site address is not. By selecting a focused combination of URLs for which to create crawl rules that exclude unneeded items, SSP administrators can maximize the relevance of the content in the index while minimizing the impact on crawling performance and the size of content databases. Creating crawl rules to exclude URLs are particularly useful when planning for start addresses for external content, for which the impact on resource usage is not under the control of people in your organization.

When creating a crawl rule, you can use standard wildcard characters in the path (URL). For example:

 http://server1/folder\* contains all Web resources with a URL that starts with http://server1/folder.

 \*://\*.txt includes every document with the txt file extension.

#### Specify a different content access account

Regardless of whether a crawl rule includes or excludes content, administrators have the option of changing the content access account for the rule. The default content access account is used unless another account is specified in a crawl rule. The main reason to use a different content access account for a crawl rule is that the default content access account does not have access to all start addresses. For those start addresses, you can create a crawl rule and specify an account that does have access.

For the initial deployment, we recommend that you use crawl rules to focus crawled content on what is most relevant according to the concepts and business processes that are most relevant to your organization, as identified in the information architecture. Because crawling content consumes resources and bandwidth, it is better to include a smaller amount of content that you know is relevant than a larger amount of content that might be irrelevant. After the initial deployment, you can review the query and crawl logs and adjust content sources and crawl rules to be more relevant and include more content.

note_ddNote:

Do not use the same domain account for a content access account that you use for the Application Pool. Doing so will cause minor versions of files (history) in SharePoint sites to be crawled and indexed.

|  |
| --- |
| Worksheet action |
| Record the decisions you make about crawl rules for your initial deployment in the Crawl rules section of the [Plan to crawl content worksheet](http://go.microsoft.com/fwlink/?LinkID=73748&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73748&clcid=0x409). |

## Plan file-type inclusions and IFilters

Content is only crawled if the relevant file extension is included in the file-type inclusions list and an IFilter is installed on the index server that supports those file types. Several file types are included automatically during initial installation. When you plan for content sources in your initial deployment, it's a good idea to verify if content you want to crawl uses file types that are not included. If so, you will need to add those file types during deployment. On the other hand, if certain file types contain mostly irrelevant content, you can delete the file extension for that file type from the file type inclusions list, which will exclude file names that have that extension from being crawled.

When you add file types, you must also ensure that you have an IFilter that can be used to parse the file type when crawled. Office SharePoint Server 2007 provides several IFilters and several more are available from Microsoft and third-party vendors, and if necessary software developers can create IFilters for new file types.

The following table lists the file name extensions of the file types that are supported by IFilters that are installed by default and are included in the file type inclusions list, by default.

|  |  |  |
| --- | --- | --- |
| File type extension | Default IFilter support | Default file type inclusions |
| ASCX | Yes | Yes |
| ASM | Yes | No |
| ASP | Yes | Yes |
| ASPX | Yes | Yes |
| BAT | Yes | No |
| C | Yes | No |
| CMD | Yes | No |
| CPP | Yes | No |
| CSS | Yes | No |
| CXX | Yes | No |
| DEF | Yes | No |
| DIC | Yes | No |
| DOC | Yes | Yes |
| DOCM | Yes | Yes |
| DOCX | Yes | Yes |
| DOT | Yes | Yes |
| EML | Yes | Yes |
| EXCH | No | Yes |
| H | Yes | No |
| HHC | Yes | No |
| HHT | Yes | No |
| HPP | Yes | No |
| HTA | Yes | No |
| HTM | Yes | Yes |
| HTML | Yes | Yes |
| HTW | Yes | No |
| HTX | Yes | No |
| JHTML | No | Yes |
| JSP | No | Yes |
| LNK | Yes | No |
| MHT | Yes | Yes |
| MHTML | Yes | Yes |
| MPX | Yes | No |
| MSG | Yes | Yes |
| MSPX | No | Yes |
| NSF | No | Yes |
| ODC | Yes | Yes |
| ONE | No | No |
| PHP | No | Yes |
| POT | Yes | No |
| PPS | Yes | No |
| PPT | Yes | Yes |
| PPTM | Yes | Yes |
| PPTX | Yes | Yes |
| PUB | Yes | Yes |
| STM | Yes | No |
| TIF | Yes | Yes |
| TIFF | No | Yes |
| TRF | Yes | No |
| TXT | Yes | Yes |
| URL | No | Yes |
| VDX | No | Yes |
| VSD | Yes | Yes |
| VSS | No | Yes |
| VST | No | Yes |
| VSX | No | Yes |
| VTX | No | Yes |
| XLB | Yes | No |
| XLC | Yes | No |
| XLS | Yes | Yes |
| XLSM | Yes | Yes |
| XLSX | Yes | Yes |
| XLT | Yes | No |
| XML | Yes | Yes |

Note that an IFilter is not provided for the "ONE" file extension used by Microsoft Office OneNote 2007. If you want users to be able to search content in OneNote files, you must install the IFilter for OneNote. This means installing the Microsoft Office OneNote client application on the index server.

note_ddNote:

The Office OneNote 2007 IFilter can crawl both OneNote 2003 and OneNote 2007 files. The Office OneNote 2003 IFilter can crawl OneNote 2003 files only.

For details about enabling and configuring the index server for OneNote files, see Deploy Search.

|  |
| --- |
| Worksheet action |
| Record the decisions you make about file-type inclusions and Ifilters for your initial deployment in the File-type inclusions and IFilters section of the [Plan to crawl content worksheet](http://go.microsoft.com/fwlink/?LinkID=73748&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73748&clcid=0x409). |

## Plan search settings that are managed at the farm level

In addition to the settings that are configured at the SSP level, several settings that are managed at the farm level affect how content is crawled. Consider the following farm-level search settings while planning for crawling:

 Contact e-mail address   Crawling content affects the resources of the servers that are being crawled. Before you can crawl content, you must provide in the configuration settings the e-mail address of the person in your organization whom administrators can contact in the event that the crawl adversely affects their servers. This e-mail address appears in logs for administrators of the servers being crawled so that those administrators can contact someone if the impact of crawling on their performance and bandwidth is too great, or if other issues occur.

The contact e-mail address should belong to a person who has the necessary expertise and availability to quickly respond to requests. Alternatively, you can use a closely monitored distribution-list alias as the contact e-mail address. Regardless of whether the content crawled is stored internally to the organization or not, quick response time is important.

 Proxy server settings   You can choose whether to use a proxy server when crawling content. The proxy server to use depends upon the topology of your Office SharePoint Server 2007 deployment and the architecture of other servers in your organization.

 Time-out settings   The time-out settings are used to limit the time that the search server waits while connecting to other services.

 SSL setting   The Secure Sockets Layer (SSL) setting determines whether the SSL certificate must exactly match to crawl content.

|  |
| --- |
| Worksheet action |
| Record the decisions you make about farm-level search settings for your initial deployment in the Farm-level search settings section of the [Plan to crawl content worksheet](http://go.microsoft.com/fwlink/?LinkID=73748&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73748&clcid=0x409). |

## Worksheet

If you have not already done so, record your planning decisions about content sources and other decisions about crawling content in the following worksheet:

 [Plan to crawl content worksheet](http://go.microsoft.com/fwlink/?LinkID=73748&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73748&clcid=0x409)

If you decide to create only some of the planned content sources and crawl rules during initial deployment and configuration, you can use this worksheet as part of ongoing operations.

# Plan the end user search experience [Office SharePoint Server]

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [Plan properties for search](#DSDOC_section1a56532d7_9814_4a0c_a308_f2)

 [Plan search scopes](#DSDOC_section2a56532d7_9814_4a0c_a308_f2)

 [Plan authoritative pages](#DSDOC_section3a56532d7_9814_4a0c_a308_f2)

 [Plan server name mappings](#DSDOC_section4a56532d7_9814_4a0c_a308_f2)

 [Plan keywords and best bets](#DSDOC_section5a56532d7_9814_4a0c_a308_f2)

 [Plan search-based alerts](#DSDOC_section6a56532d7_9814_4a0c_a308_f2)

Administrators can improve the relevance and presentation of search results by planning the right configuration of administration settings that affect search queries. This includes creating scopes, which is a way to group certain content in index into individually searchable pieces of content, and controlling the way search results are presented. Administrators can also specify what properties and keywords are available to end users for performing search queries. These abilities enable administrators to have a great deal of control of the end user search experience.

While the effectiveness of search queries are constantly evaluated during regular operations of any deployment of SharePoint Products and Technologies, good planning before the initial deployment can create effective search queries from the start and help to reduce future administration costs. Administrators for Shared Services Providers (SSPs) can plan managed properties for search to use across the SSP, relevance settings for specific sites, and the search scopes that users in sites across the SSP use to narrow the content included in each search query. They can also change the presentation of results through server name mappings, and customization of search center sites, the search box, and other search presentation features. Site collection administrators can supplement these plans by planning site-specific search scopes and keywords.

## Plan properties for search

In Office SharePoint Server 2007, the way you organize content strongly influences the effectiveness of search features in your site collections. To effectively deploy Office SharePoint Server 2007, start by understanding the information architecture of your organization, and then apply that understanding to plan managed properties for finding site collection content and business data regardless of file type, and to create search scopes.

The enterprise search functionality of Office SharePoint Server 2007 uses a combination of text and properties about each document to prioritize search results. Good management of properties for search is important for providing relevant search queries. By thinking of search properties as part of an organized information architecture, you can plan to use properties across the Shared Services Provider (SSP) to create a consistent search experience across the content in your organization.

When the content is crawled, the crawler also crawls the properties associated with that content. Examples of crawled properties include the metadata of Office client applications, Web pages, and documents from other applications used by your organization, and the data stored in databases and line of business applications used by your organization.

In previous versions of Microsoft SharePoint Products and Technologies, all of these properties were used when searching for people, documents, or sites. You could reduce property duplication by mapping some properties to other common properties, but many properties confused search results because they weren't relevant. Thus, relevant properties were hard to find amid the many irrelevant properties.

Office SharePoint Server 2007 mitigates this confusion by enabling SSP administrators to create managed properties. They can then map crawled properties, which are the properties that the crawler collects and adds to the property store when crawling content, to managed properties that are used by search queries to prioritize search results across the SSP.

Site collection administrators cannot add or view the list of managed properties, but those managed properties can be used in some administration tasks for the site collection, such as search scopes administration.

You can make the content on your site easier to find by carefully planning your managed properties and how you implement them.

### Plan managed properties based on the information architecture

As part of site planning, you analyze the content and key business processes of your organization, and organize this content and these processes into a taxonomy called an information architecture. There are many ways to do this, and the details of an information architecture and the amount of time that is required to prepare it can vary widely from organization to organization. One practical way to identify key concepts is to examine your existing content and its high-priority metadata. If you have access to a test farm prior to active deployment of Office SharePoint Server 2007, you can crawl your content and see what crawled properties appear, and use those properties to identify part of your information architecture. However, most organizations will benefit from planning an information architecture on paper before staging a deployment, because it can help to focus your planning and identify content and processes that are not as well-organized as they could be.

Knowing the information architecture of your organization can be useful for planning managed properties because every concept in your information architecture can potentially be represented by a managed property. If you identify managed properties for all key concepts in the information architecture, you will have a complete set of managed properties that accurately represents the most important content and business processes in your organization. The key to creating a useful set of managed properties is to determine the most important concepts and find properties in your content that you can map to managed properties that enable users to find relevant content when searching. Be precise when mapping crawled properties to managed properties to maintain performance and increase relevance. Mapping more properties increases the size of content databases, and reduces performance accordingly, so it's a good idea to map properties only when you are highly confident of the relevance of the mapping.

You can represent these concepts in other ways during implementation as well. Some concepts are used to suggest site collection structure and content within site collections. Others are used to create special terms such as keywords to highlight relevant search results.

It is difficult to discover properties of content without first crawling content. Therefore, it is best to wait to plan managed properties until you already have a good idea of the content of each site collection. Then, on a test server, you can crawl all that content so that you have a list of crawled properties to compare against your information architecture when creating managed properties. One thing to realize is that it can be difficult to map properties even after crawling content because it is difficult to identify the content type or application that uses the property. A good practice is to map properties that seem to be related, and then perform relevant searches to see if the expected results appear.

Many of the most useful managed properties are automatically created when Office SharePoint Server 2007 is installed. Use these managed properties as a starting point when planning your other managed properties. Those properties include but are not limited to:

 Author

 Contentclass

 Description

 Container

 Site Name

 Type

 File Size

 Last Modified Date

 URL

 Doc ID

 Title

Keep in mind that for searching using properties to be affective, the crawled properties must first be assigned values. For example, if you have a document that has a property that maps to a managed property called Author, but no value is assigned to that property on that document, then that document will not be displayed in search results when users use perform a search query against the Author property for a particular author.

#### Eliminate redundant and duplicate properties by using property mapping

Some properties are fairly basic and might appear as different properties in different types of content. Examples include the Author and Title properties for documents, or Team or Division properties for people. Adding each Author property as a separate managed property doesn't make sense, because it adds additional managed properties to the database without increasing relevance. The most important thing you can do with these basic properties during planning is to reduce duplication by creating one set of managed properties and mapping the crawled properties with the same meaning to properties in the set of managed properties. In the case of the Author property, you can map each unique appearance of a crawled property for authors with a single Author managed property.

You can map one or more crawled properties to one or more managed properties. You can choose to prioritize multiple crawled properties so that if more than one property is found during crawling, only the value of the highest priority property is used for queries using the managed property or properties. If you don't prioritize crawled properties, values for all crawled properties mapped to the managed property are used for queries, so that the managed property becomes multi-valued. A sensible approach for a single-value property is to choose the most common crawled property as the managed property, and then prioritize mapped properties by how often they occur. It is not always easy to determine which property is crawled most often, but one strategy is to prioritize properties that you know are associated with commonly used applications.

When you map properties with different data types, the data type of the managed property is used by search in most cases.

Be careful when mapping properties that you do not map poorly matched or irrelevant properties. For example, mapping a crawled property that uses the data type Yes/No to a managed property that is assigned the data type Integer might produce inconsistent or unexpected results. Imprecise mappings can actually reduce the relevance of search results. As always, if possible test searches for managed properties before initial deployment, and plan to review usage data for search queries during normal operations to fine tune the properties you have mapped.

#### Add properties to present key concepts in the information architecture

Other crawled properties might clearly map to concepts in the information architecture that are not already captured by existing managed properties. For each concept in your information architecture, ask yourself if there's a crawled property that represents this concept that can be made into a managed property. For every crawled property, ask if there's a place for it in the information architecture. If so, update the information architecture and make the property a managed property. This means creating a managed property using the name of the crawled property and mapping the crawled property to it.

For example, a company might identify customer service as a key business process in its information architecture. Key concepts associated with customer service in the information architecture may include customers, customer service representatives, and customer service regions. There's a line of business application that tracks customer and employee data, and the properties of that data are likely candidates for managed properties after they are registered in the business data catalog and crawled as part of a business data content source. You might also identify crawled properties for applications that should be mapped to these managed properties, for example a customer service representative ID property in a separate data application, or an author property for an application type used exclusively by customer service representatives. A search query that uses that property or a term associated with that property will include search results for all items containing any of the crawled properties mapped to the Customer service representative ID managed property.

Each major business process identified in the information architecture will have a set of associated file types or business data applications that can be used to identify likely managed properties.

Note that although many concepts in the information architecture aren't represented by properties, those concepts are useful during site structure planning and the implementation of other search features. The information architecture can identify managed properties that you overlooked, but just because a concept is listed in the information architecture doesn't mean that there is a managed property for that concept.

### Plan for business data properties

As part of business data search planning, SSP administrators must map the properties of business applications to managed properties. Those properties must be selected as managed properties for business data for an application to appear in search results. The customer service example described previously is an example of mapping business data properties to managed properties used by search. For more information about business data planning, see [Plan for business data search](#DSDOC_2b7121fc_a1f2_469d_ac1c_7b12283897).

### Using properties in queries

By default, for the value of crawled properties to affect a search query, the crawled properties must be mapped to a managed property and the user must perform a search against that managed property. However, SSP administrators can choose to include the values of particular crawled properties to be added to the content index so that they are available to all queries. Including the values of crawled properties may have a negative affect on search relevance and performance.

Administrators planning the initial deployment of Office SharePoint Server 2007 should record the initial set of managed properties planned for the search service for every SSP used in the deployment. Many of these crawled properties can be found by looking at the properties of business data applications, and the properties displayed in applications for content types such as Microsoft Word documents or Excel spreadsheets. If you have access to a test server, you can crawl high-priority content and use the crawled properties that appear to help with planning.

|  |
| --- |
| Worksheet action |
| Fill in the tables in the "Plan managed properties" section of the "Plan the end-user search experience worksheet to record your decisions about crawled and managed properties. |

### Use managed properties in search scopes

Each managed property can be exposed as a property for search scope rules. For more information about planning search scopes, see the Plan search scopes section in this article.

### Plan to integrate properties for new file types using filters

Office SharePoint Server 2007 uses property categories to crawl properties by documents within each category. Property categories include the protocol handler and Ifilter used by search when it indexes content. Before you crawl content, you want to associate the content with the property categories that will most effectively find the crawled properties you need before you create managed properties.

By default, Office SharePoint Server 2007 provides the following property categories:

 Basic

 Business Data

 Internal

 Mail

 Notes

 Office

 People

 SharePoint

 Tiff

 Web

 XML

If you want to add content to your content index that requires different Ifilters or protocol handlers, you can create a new property category for that content. As part of your initial planning process, you should identify what content needs new Ifilters and protocol handlers. This might require custom code, though some Ifilters and protocol handlers will be available.

## Plan search scopes

Search scopes, also referred to as scopes, are filters applied to search results to narrow the results of a search query that is run using the scope. This enables users to perform queries against subsets of content in the content index which improves the relevance of their search results. Scopes can be created at the SSP-level. Scopes created at this level are called shared scopes because they are shared with all site collections that use that SSP. Scopes can also be created at the site collection level which are available only to the site collection on which they were created. Scopes created at this level are called scopes and sometimes called search scopes.

Site collection administrators decide which shared scopes to use and how to display them, and can also create search scopes within a site collection.

When planning search scopes, you look at your information architecture to identify broad content sets that people are likely to want to search. Some of these sets will span the information architecture of site collections, and some will span subsets of information within site collections. You decide whether to implement shared scopes or search scopes based on where content falls within the information architecture.

### Plan shared scopes

The SSP administrator manages shared scopes for all sites that use the same shared services provider. The SSP administrator can also manage search scopes for site collections.

SSP administrators can perform the following tasks:

 Creating and editing shared scopes

 Adding rules to shared scopes

 Deleting shared scopes

 Managing and scheduling compilations of shared scopes.

Shared scopes are visible and available for use by administrators for all site collections that are using the same set of shared services. Shared scopes should be implemented for bodies of content based on concepts in the information architecture, site structure, and content needs planning that are relevant for most sites in the SSP. Content that is only relevant within certain site collections should be left for search scope planning at the site collection level.

For example, a large organization might create a shared scope for content relating to human resources, because human resources is a large division with content relevant to all employees on several SharePoint sites and line of business applications identified during content and site structure planning. The site collection administrator of the human resources site can use that shared scope, and also create additional scopes for the site collection for company policies and new hire information because those are core concepts identified as relevant for the site collection. Those site collection scopes do not make sense as shared scopes, because people searching in other sites are unlikely to want scopes that are so specific.

Site collection administrators make a copy of the shared scopes they want to use in their site collection and then select the display groups in which to include the scope, such as the search box drop-down list and the advanced search page. Note that site collection administrators cannot modify or delete shared scopes, but they can copy a shared scope and then modify the copy.

The following shared search scopes are automatically created for each SSP and are available on the search center, by default:

 People

 All Sites

### Plan search scopes for site collections

For each site collection, a site collection administrator can do the following tasks that are related to search scopes:

 Create, edit, and delete search scopes.

 Copy shared scopes that were created by the SSP administrator.

 Choose how to display search scopes (search dropdown, advanced search, or both).

 Monitor the status of search scopes.

note_ddNote:

SSP administrators can perform all of these administrative tasks that site collection administrators can perform.

During planning, each site collection administrator will want to create search scopes based on the information architecture within the site. They can choose to create new search scopes, make a copy of shared scopes (a copy of a shared scope becomes a search scope), or both. For example, site collection administrators can add search scopes by selecting shared scopes that are useful for people using their site collection, and then supplementing those scopes by creating search scopes for the site collection.

Site collection administrators cannot create or add matching rules to shared scopes directly, though they can copy a shared scope as a search scope and modify the copy.

note_ddNote:

After a shared scope is copied as a search scope, a site collection administrator can perform any of the actions that they can perform on a search scope.

When creating a new search scope, you specify the following:

 Unique title and optionally a description for the scope.

 Display group, sometimes called scope groups. Site collection administrators can assign scopes to display groups to determine where they appear on the site. By default, Office SharePoint Server 2007 provides display groups for the search box drop-down menu and the advanced search page and site collection administrators can assign a particular scope to any number of display groups.

 Results page. You can choose to use the default search results page to display search results when this scope is used or specify a different page. Note that if you choose to use a different page, you must first create that search results page.

No site collection scopes are created, by default, but each site collection has access to the People and All Sites shared scopes.

### Plan display groups

Display groups, sometimes called scope display groups, provide a way to assign one or more scope to a particular search box. Office SharePoint Server 2007 provides two display groups, by default:

 Search Dropdown The All Sites and People scopes are assigned to this display group and it is used by the Search box, by default.

 Advanced Search The All Sites scope is assigned to this display group and it is assigned to the Advanced Search box, by default.

Site collection administrators can:

 Add search scopes to any display group.

 Remove search scopes from any display group.

 Create new display groups and assign the scopes they want to them.

 Assign different display groups to the Search and Advanced Search boxes on the Search Center page.

 Create new search pages using the Search Box and Advanced Search Box Web parts and assign the display group or groups that they want to use.

### Plan search scope rules

One or more search scope rules can be added to a particular search scope to define the extent of the scope.

Each rules is based upon a particular scope rule type, which defines the properties, locations, and sources of content. The following table lists the scope rule types that are available to shared search and search scopes.

|  |  |  |  |
| --- | --- | --- | --- |
| Scope rule type | Shared search scope | Search scope | Tests content by |
| Web address (http://server/site) | Yes | Yes | Location |
| Property Query (Author = John Doe) | Yes | Yes | Single property |
| Content Source | Yes | No | A particular content source |
| All Content | Yes | Yes | All content in the content index. |

These rules affect search results for the search scopes that contain them in one of three ways:

 Include Items matching this rule appear in search results unless another rule removes them. This is equivalent to the OR logical operator.

 Require Items matching other rules must also match this rule to appear in search results. This is equivalent to the AND logical operator.

 Exclude Items matching this rule are excluded from search results even if they match other rules. This is equivalent to the AND NOT logical operator.

Search scopes can contain one or more rules which are applied to all content in the currently selected search scope to determine what is included in search results.

#### Using rules based on location

You can create matching rules based on the location (Web address) of content. Several usage scenarios require rules of this kind, including:

 Searching over a group of document libraries.

 Searching within a set of folders in a single large document repository, as when searching a company archive.

 Searching for content on external sites for a particular subject.

 Searching for content in other servers in your organization.

Each rule contains a single location, defined by a single folder, domain name, or server name. Depending on what set of content you want to make available in a search scope, you would add one or more matching rules until all relevant locations are included in the search scope and all irrelevant locations are excluded. The information architecture and site structure planning will both provide guidance in deciding which locations to include in each search scope.

#### Using rules based on managed properties

Search scope rules can be based on a specific value for a single managed property. Note that the managed property that you want to use in a scope rule must first be created by an SSP administrator. Each item of content is tested against that specific value and included or excluded based on the rule. Rules based on properties can only be queried using the Is exactly operator and not against other hypothetical operators such as Contains.

For example, a sales portal site can create search scopes for each of its sales offices by using the Sales Office managed property and setting the value for the rule in each scope to the value for the relevant office. Because this managed property is based on data from a sales tracking application, the search results will include only business data search results for the sales office for the selected scope.

When you plan the managed properties for your SSP, it is helpful to think about search scopes at the same time. To create a search scope for a certain set of content, you must ensure that there are properties of that content that are mapped to managed properties that can be included in scope rules.

Each managed property in the SSP can be made available as a property for search scope rules, for both shared scopes and site collection scopes. Only the managed properties that specifically have been made available for search scopes can be used in search scope rules.

#### Using rules based on content sources

Only shared search scopes can contain scope rules based on specific content sources. Note that this scope rule type is not available to search scopes at the site collection level. Your content source planning will identify sets of content that are easier to administer when they are on separate content sources.

For each content source that you plan, consider whether the content indexed using that content source is something that would make sense grouped together in a search scope for people using the site collection. If so, you can add a scope rule for that content source.

Also consider if the content source can be divided up into smaller bodies of content that people might want to search for. If so, you can combine scope rules to specify the content source with other scope rule types to create a more narrow scope.

By using rules based on content sources, you can easily enable people in a central site collection for a large organization to search over content on site collections for smaller projects or divisions. To do this, SSP administrators add a matching rule for the relevant content source. That search scope can be shared so that people using any site collection in an SSP can potentially search over content on any other site collection in the SSP. For example, this is useful is a division-wide site collection with a search box menu for the human resources site collection.

For more information about planning for content sources, see [Plan to crawl content [Office SharePoint Server]](#DSDOC_82c09ad6_6137_438d_a324_16a7f99e12).

#### Using rules based on all content

Administrators can create scope rules using the All Content scope rule type, which means that all content in the content index is available to the scope. If you want to create a more narrow scope, you can add additional scope rules to a scope that uses the All Content scope rule type to exclude particular content from the scope.

#### Using multiple rules

Search scopes will often be simple scopes based on a single matching rule. But there are many good reasons to use search scopes with multiple rules. What these reasons have in common is that they seek to create search scopes based around a specific theme or conceptually-related set of content. To do this, you must include several locations, several properties, or a combination of locations and properties that are conceptually related.

Rather than just creating basic one-rule search scopes for every conceivable property or location that might eventually be relevant, it is a better idea to think in terms of broad concepts and use those to create a shorter list of complex search scopes for each site collection. Use complex scopes with multiple rules targeted at specific document libraries, file shares, mail servers, data sources, based on the evaluation of your information architecture.

#### Using exclusion rules

Scope rules that exclude content are created and selected just like any other scope rules used in search scopes. However, you might want to consider their implementation as a separate step. Reasons to exclude content from search results can differ substantially from the reasons to include content.

The All Sites shared search scope can be used as a starting point to include all content in the content index. Then you can add scope rules that exclude content from search results to create search scopes that are broad but do not include a certain set of search results. It is sometimes easier to use a copy of the All Sites shared search scope with exclusion rules than to create a complex search scope containing rules that include every subset of content on the site.

### Example of search scope planning

Contoso Corporation has an IT services division, a customer service division, and a sales and marketing division. Each division has its own site collection, and there's also a central portal site collection for company news and human resources information. The SSP administrator plans to operate the search service using a single SSP for the entire company. This means that all crawled content will be indexed into one content index.

By default, searches in the organization will include content from any division, because that's the default search scope. Because the content for each division is distinct, content on the three division site collections will be crawled using three separate content sources so that IT services, customer service, and sales and marketing information can all be updated on different schedules.

Jacky Chen, the SSP administrator, plans to create separate content sources for each division. She also plans to create a content source for crawling the human resources and company news content that is on the central portal site collection.

By default, all content that has been indexed from all four of the site collections are included in the All Sites shared scope that is available to all site collections. Jacky Chen also creates a shared scope for each divisional site collection and then creates a site scope rule for each of them that includes the appropriate content source for that scope. For example, For example, she creates a scope called Customer Service and creates a scope rule for that scope that includes content from the Customer Service content source.

The site collection administrator for each division decides to include the All Sites shared scope, but none of them plan to use the human resources scope, even though it's a shared scope. That option will only be available from the search drop-down menu in the central portal site collection.

The site collection administrator for each division also plans to make copy of the shared scope that Jackie created for their site collection for each important set of content within their site collections. They then plan to create scope rules for those scopes to target only the content users want to query against when using those scopes.

For example, the site collection administrator for the sales and marketing site collection plans to create search scopes for content related to each product line, based on the managed properties of business data, marketing documents, and other content, and the location of related team sites and document libraries.

Both shared and search scopes are defined by one or more rules concerning properties and document locations. Content can be either included, required, or excluded from search scopes by these rules.

|  |
| --- |
| Worksheet action |
| Fill in the tables in the "Plan scopes" section of the "Plan the end-user search experience worksheet to record your decisions about scopes, scope rules, and display groups. |

## Plan authoritative pages

Authoritative page settings prioritize Web sites and other locations in the content index so that results from those sites are more or less likely to appear at the top of search results. Authoritative page settings are one factor in prioritizing search results, and do not outweigh all other factors such as keywords managed by site collection administrators, managed properties that are managed by the SSP administrator, or the automatic weighting applied to content by the search technology.

A

Authoritative page settings are configured at the SSP level and apply to all queries made using that SSP. SSP administrators can assign sites to one of four authoritative page levels:

 Most authoritative

 Second-level authoritative

 Third-level authoritative

 Sites to demote.

Authoritative Web pages are weighted based on how authoritative they are, with each level receiving proportionate relevance weighting. By default, all top-level pages for Web applications are added as most authoritative. You can move these pages to other authoritative page levels or remove them from authoritative page settings completely.

The less relevant sites are demoted to lower priority with the same amount of weighting as given to third-level authoritative sites.

When planning authoritative page settings, consider the purpose of each site, and review its subsites. Group authoritative sites into the three levels by importance and group the sites that are not likely to be relevant as sites to demote. Demoted sites will typically appear towards the end of the search results after all other relevance weighting factors have been considered.

Good practices to use when planning authoritative page settings include:

 SharePoint sites and business applications central to high-priority business processes will typically be most authoritative.

 Sites that encourage collaboration or action are likely to be more authoritative than sites that are merely informative.

 Secondary business processes are likely to be in the second or third level of authoritative sites.

 External sites will typically be less authoritative, because your organization cannot control the content on those sites.

 You don't need to assign an authoritative page setting to every site. It is a good idea to select relevance for a small number of sites that you know are most authoritative or less relevant, and adjust the authoritative page settings during normal operations based on feedback from users and information in the query logs and crawl logs.

The search results for any site collection can be modified to promote specific content so that it appears more prominently in response to queries that use particular search terms. Although keywords are planned, implemented, and managed at the site collection level, it is a good idea to make sure your planning and implementation is consistent throughout your organization.

|  |
| --- |
| Worksheet action |
| Fill in the table in the "Authoritative pages" section of the "Plan the end-user search experience worksheet to record your decisions authoritative pages. |

## Plan server name mappings

Server name mappings change how the location URL is displayed for each item in search results. Server name mappings are set at the SSP level for all content that is crawled by that SSP, and are applied whenever queries are performed. You might want to use server name mappings in the following scenarios:

 You want to prevent access problems and possible security vulnerabilities caused by links that refer to local addresses by mapping them to addresses on the server. For example,

 You want to obscure complex URLs in search results, so you replace them with a more concise name on the server.

 For security reasons, you want to hide the name of the original source of the content.

Use server name mappings only when you have known access or display problems. For each content source you plan, consider if its start addresses contain local URLs, complex URLs that you would like to simplify for your users, or point to locations that you want to help keep more secure. In most cases, planning for server name mappings prior to the initial deployment will be minimal.

|  |
| --- |
| Worksheet action |
| Fill in the table in the "Authoritative pages" section of the "Plan the end-user search experience worksheet to record your decisions about authoritative pages. |

## Plan keywords and best bets

Keywords are metadata that administrators create at the site collection level to prioritize content during search queries to display high-relevance content more prominently in search results. Each keyword, sometimes called a keyword phrase, is composed of one or more words and optionally any of the following:

 A definition of the keyword that appears in search results

 One or more synonymous search terms

 One or more best bests, which are the URLs that administrators specify as being most relevant for a particular keyword phrase.

note_ddNote:

Although you can create a keyword that does not contain any of the optional information listed above, doing so would not improve the relevance of search results.

Searches using the exact keyword you define or one of its synonyms promote the specific content pre-selected by site collection administrators as more relevant so that they appear at the top of search results.

Keywords are used to highlight or promote search results that the administrator has determined are more relevant for users of each site collection. Keywords appear in a high-confidence Web Part next to search results, and users can click the keyword to view the full definition, synonyms, and Best Bets for that keyword.

Administrators typically update and expand keywords as part of ongoing operations but to promote collaboration for key business content and data related to key business processes, it can be helpful to plan a small set of high-priority keywords before beginning deployment.

### Use information architecture to identify keywords

You can use the information architecture created by your content planning teams to identify high-priority content to associate with keywords. Your information architecture is already a hierarchical list of terms. It is fairly straightforward to take some of those terms and quickly use them to create keywords that you can associate with specific and highly-relevant content.

Relevant content is anything specific that you want people to see first or most prominently when they search using a specific keyword. Examples of relevant content for each major business concept or content area include:

 Documents

 Sites

 People

 Definitions

 Approved or official terms that mean the same thing, but were not included in the search query.

Associating keywords with documents are helpful to encourage people to view the key documents needed to collaborate on key business processes. For example, a business may have a special template for expense reports, and a keyword "expense reports" that promotes that template to the top of search results. Without that keyword, each employee might spend several minutes asking their colleagues for the appropriate URL or browsing the company Web site. With the keyword associated with the URL to the expense report template as a best bet, they can quickly locate the template and enter their expenses.

Keywords for sites are helpful for identifying the location of sites for relevant information in a large organization. For example, "holidays" could be a keyword associated with a Best Bet for the human resources site about paid time off for employees. The keyword helps employees quickly discover when holidays occur so they can plan their work schedules accordingly.

Keywords that help people find other people encourage collaboration between people across the organization who have important knowledge to share, or just about important people in the company. For example, a title such as "CEO" could be a keyword associated with the chief executive officer for a company, or a person's My Site could be a Best Bet for a keyword relating to their organization or area of expertise, such as "chemistry department."

Keywords based on definitions are a good idea for high-priority concepts in each site collection. For each key idea, site collection administrators can create a keyword so that the definition of the keyword appears in the high-confidence Web Part next to the search results. For example, a sales portal devoted to selling a particular line of products might provide definitions for the major items in the product line. These definitions can be used to help sales associates understand their products better, or the definitions can be displayed in search results on a public-facing portal site for customers.

#### Use properties of keywords

Keywords are organized into a keyword list at the site collection level. The following properties of keywords help to highlight content:

 Keyword phrase The keyword phrase is one or more words used in a search query, and it identifies the keyword. For example, a keyword phrase can be a single word, such as "OOF" or a group of words that must be typed in a particular order, such as "out of office". When users type in the keyword phrase, the search results for the keyword appear. When the results appear, the keyword phrase is highlighted in the search results.

 Synonyms Each keyword can have one or more terms identified as synonyms, and the same search results appear for a synonym as appear for the keyword phrase. The keyword phrase displays at the top of search results from any query using one of the synonymous terms. This is useful when several search terms are used for the same underlying concept and content, so that search results are consolidated and not scattered across several search terms. The keyword list including all synonyms is known as a thesaurus. The thesaurus for Office SharePoint Server 2007 is compatible with the thesaurus for SharePoint Portal Server 2003.

 Definition Each keyword can have one or more definitions, and search results for keywords display the definitions next to the keyword phrase, before any other search results. You can also include the title or the URL of the source for the definition, so it's a good idea to identify definition sources during planning. You might even have a separate step during planning to design a glossary of all definitions used by keywords in each site collection.

 Best Bet Best Bets for a keyword are promoted to the top of the high-confidence Web Part next to the search results for queries using that search term, just below the definition for the keyword if there is one. Specific documents, sites, and people with expertise in the concept associated with a search term are common examples of Best Bets. A Best Bet is more than a URL. It is important to consider the title and description of each Best Bet during content planning to increase the relevance and usability of each Best Bet. You can associate up to 25 Best Bets with every keyword in the administration user interface, and many more with the object model, but it is a good idea to not overuse Best Bets. Good content planning and an organized information architecture should help you identify an appropriate number of Best Bets for each keyword that balances number of results with search relevancy.

Note that unlike in previous versions of SharePoint Portal Server, keywords are not affected by security permissions, and all readers on the site collection can see all Best Bets and keywords for that site collection that appear in search results. Users that do not have permissions to see the pages to which a best bet is linked cannot click-through to the page. However, they will see the description of the best bet on the search results page which could expose information that a particular user is not intended to see. Keywords are meant to provide high-priority results for all users. If you want to target content to certain users based on their permissions, you can use audiences and targeted Web Parts in the appropriate places on the site collection.

### Plan keywords

It is important to plan keywords in advance to help ensure consistency of keywords across your organization, even though keywords are implemented at the site collection level. By using a single information architecture to identify your key concepts, associating certain content with certain site collections, and then planning keywords for the information architecture relevant within each site collection, you avoid duplication and confusion of keywords and increase the relevance of search results across your organization.

Keyword Best Bets appear in search results even if the content hasn't been crawled, as long as the person viewing the results has access to the content. This is another reason to plan keywords during initial deployment, so that high-priority content can be available in the early stages of a deployment before all content sources have been crawled. In rare cases where content cannot be crawled because search is missing a relevant IFilter or for any other technical reason, you can use keyword Best Bets to make the content easier to find even though it hasn't been crawled.

As with other parts of the planning process, you will have key people at each level of the organization that plan keywords for their site collections. Those people will use the same overall content plan, adapted for the content on the site collections that they are planning. At each stage of the process, which happens in waves over time, each set of content planners can communicate with each other to keep consistency in the overall plan.

In small organizations, the content planning team is likely to be small and organized around a single site collection, and planning for keywords might be organized by only one or two people. In large organizations, you want to include business planners and administrators at each level to make sure all business needs are addressed, so somewhat larger planning teams are often helpful.

Not all keywords will be planned before deployment. The role of your content planning teams is to identify the high-priority concepts that are most relevant to search queries in your organization, so that search queries are relevant to users from the first day of your deployment. Then they can identify a contact person for each keyword who may or may not be someone on the planning team. After deployment, site collection administrators can expand the keyword list after identifying common search terms in the query logs.

In the planning phase, keyword list managers should consider how keywords match to queries. Keywords must match the complete string of search terms exactly, and must not use special syntax such as + and -. This prevents the return of multiple lists of keywords for the same search query, which streamlines search results. Because of this, you must carefully consider synonyms so that keywords actually match to the relevant content without matching unrelated content.

You must also consider that keywords match across search queries for each site collection, and cannot be excluded by search scopes that narrow the search results. This can affect planning for search scopes, so most content planners and administrators will plan implementation of these features as part of the same process.

The more planning you do before deployment, the less management will be needed during day to day operations.

### Plan keyword management

The details of keyword management are mostly relevant to the daily operations of your site collections, but there are some aspects of administration that are worth considering during planning.

Each search keyword has the following additional but optional properties:

 Contact

 Start, review, and expiration dates

The contact for each keyword is the person who should be contacted when a keyword expires, if it is set to expire. A contact may not be directly responsible for managing keywords. Content planners for each site collection should consider who is going to be managing keywords after initial deployment, and include at least some of those people in the planning process at the site collection level.

The life cycle of keywords is also important to consider. Keywords can be required to go through approval before they affect search results, and can also be set to start or expire after a certain amount of time. The high-priority keywords identified during initial planning are unlikely to be temporary, except for content that is relevant to people using a site collection during the initial deployment. However, part of the planning process is anticipating who will make decisions about keywords in the future. Making those decisions during the planning process can improve the transition to regular operations of the site collection, and promote consistent and efficient use of keywords in the future.

Because the URLs for keywords are associated with the Best Bet, you can use the same Best Bet for more than one keyword. If the Best Bet already exists, you can add it to any keyword without having to enter the properties for the Best Bet again and possibly introduce redundant Best Bets. You can also change the URL and description for that Best Bet for all keywords that use it at the same time. This allows for easy migration of your content to a new site by ensuring users find the content they need. This is particularly useful if you are using a test site during planning and before initial deployment.

By using the object model, you can also import and export keywords between site collections as an Excel spreadsheet, so if some Best Bets apply to other site collections, you can plan once and deploy on all relevant site collections. This also allows keyword managers for a site collection at the divisional or project level to suggest Best Bets for a central site collection in a shared services environment.

For more information about managing keywords, see the Operations Guide for Office SharePoint Server 2007.

|  |
| --- |
| Worksheet action |
| Fill in the table in the "Keywords " section of the "Plan the end-user search experience worksheet to record your decisions about keywords. |

## Plan search-based alerts

An SSP administrator can decide whether search-based alerts will be active for a particular SSP. If active, people using search-based alerts can ask to be alerted when the results of their saved searches have changed. The drawback with allowing search-based alerts is that search-based alerts use resources of mail servers, and they also impact the load on query servers because the queries for each search-based alert run every time a search-based alert is processed. When planning the initial deployment, consider the resources available for alerts and the likelihood that people using your sites will use alerts productively. Search-based alerts are activated, by default.

|  |
| --- |
| Worksheet action |
| Fill in the table in the "Search-based alerts " section of the "Plan the end-user search experience worksheet to record your decisions about search-based alerts. |

# VIII Plan communication

In this chapter:

 [Chapter overview: Plan communication [Office SharePoint Server]](#DSDOC_5c9d5c10_a7a8_43d1_ac36_a6f50f2d0c)

 [Plan presence integration [Office SharePoint Server]](#DSDOC_3f53f3d3_85b8_42e5_8213_afb5eec7e8)

 [Plan incoming e-mail [Office SharePoint Server]](#DSDOC_ca092ed2_4aa2_4c2e_b273_661ca6a76e)

 [Plan outgoing e-mail [Office SharePoint Server]](#DSDOC_75401651_ef01_4348_878e_8a636f0b07)

# Chapter overview: Plan communication [Office SharePoint Server]

Enabling communication is a critical component for creating Web applications in which group members can interact with each other and keep up with changes to information through the use of alerts. The site collection features that are dependent on communications being properly set up include:

 Online presence to allow real-time messaging between group members.

 Alerts to notify group members when things have changed.

 Administrative messages related to requests for site access and other site administration issues.

 Discussion groups.

To make the most effective use of the communications features, planning should include understanding the software requirements. It should also include the privacy and security implications of enabling communication, particularly outside the corporate firewall.

## [[15]](#footnote-16)#Communications components

Communications includes three components: online presence, incoming e-mail, and outgoing e-mail. Plan communication by using the following articles:

 [Plan presence integration [Office SharePoint Server]](#DSDOC_3f53f3d3_85b8_42e5_8213_afb5eec7e8) provides information on how too enable users to see online presence of group members and start instant message conversations from within a site collection.

 [Plan incoming e-mail [Office SharePoint Server]](#DSDOC_ca092ed2_4aa2_4c2e_b273_661ca6a76e) provides information on how to set up e-mail for discussion groups.

 [Plan outgoing e-mail [Office SharePoint Server]](#DSDOC_75401651_ef01_4348_878e_8a636f0b07) provides information on how to use alerts and administrative messages.

# Plan presence integration [Office SharePoint Server]

In this article:

 [About online presence](#DSDOC_section13f53f3d3_85b8_42e5_8213_af)

 [Advantages of incorporating online presence](#DSDOC_section23f53f3d3_85b8_42e5_8213_af)

 [Organizational considerations](#DSDOC_section33f53f3d3_85b8_42e5_8213_af)

 [Software requirements](#DSDOC_section43f53f3d3_85b8_42e5_8213_af)

 [E-mail account requirements](#DSDOC_section53f53f3d3_85b8_42e5_8213_af)

Online presence enables individuals who have access to your site to see who is online and to send instant messages to them. Online presence can be a powerful collaboration tool that helps site members to quickly find out who is available to answer questions.

This article explains what online presence is, how it can be used in an organization, and the software that is required to enable it.

## About online presence

Online presence gives individuals the ability to identify who is online and available to communicate with them at any given moment. Enabling online presence (and installing the required software) adds an online status indicator next to an individual's name wherever their name appears in a site collection. The online status indicator shows whether the individual is offline or is online and available to respond to queries via an instant messaging client. When an individual is online, you can click the online status indicator to send an instant message. This direct access to knowledgeable sources can help team members work more effectively and efficiently.

Wherever a member name appears in a site, the online status indicator menu is available. The online status indicator is integrated with the Active Directory directory service, Microsoft Exchange Server, and MSN Messenger to provide information, such as office location and free/busy status, so it is a useful tool for scheduling meetings and sending e-mail even when an individual is offline.

Online status is rendered by an ActiveX control that is installed with Microsoft Office. The ActiveX control enables online status to be displayed. This control verifies the e-mail address on record for the user and directs a query to the presence server for that client to see if they are online. The ActiveX control does not store online information or e-mail addresses; it simply directs queries from the site to the e-mail address and renders the appropriate status.

Online presence is enabled by default; however, both the software and e-mail account requirements must be met for the functionality to be available to end users.

## Advantages of incorporating online presence

The advantage of enabling presence is in the ability to use it to improve collaboration between group members and increase efficiency in business processes. By integrating instant messaging and presence information in a SharePoint site, group members can see who is online and instantly know whether they are available for a quick question or brief meeting. Individuals can streamline work processes by immediately notifying team members of document or timeline changes or establish group collaborative sessions by using instant messaging.

## Organizational considerations

Because online presence is enabled at the Web application level, it is enabled for all sites and subsites of that virtual server. Therefore, it is critical to ensure that all site collections within the virtual server are willing to share this level of transparency.

While enabling online presence is beneficial in many environments where collaboration is critical, it is important to balance the benefits of increased collaboration among group members with the requirements for security and compliance, particularly in regard to the deployment of an instant messaging client. Planning for presence should include assurance that both internal and external communications to and from the instant messaging client are consistent with company-wide policy for security and compliance with regulatory guidelines and business practices.

For example, in some highly regulated industries, instant messaging conversations must be retained in accordance with record-keeping requirements for electronic communications. Companies that are subject to Sarbanes-Oxley regulation must archive instant messaging conversations as a part of their records-retention requirements.

## Software requirements

Because online status is rendered by Office, Office 2003 or later is required on all client computers. Additionally, one of the following instant messaging clients must be installed on client computers to enable real-time communications:

 Microsoft Windows Messenger version 4.6

 MSN Messenger version 4.6 or later

 Microsoft Office Communicator 2005 or later

If either MSN Messenger or Windows Messenger is installed on the client computer, by default the end user will see online status for their Messenger contacts only. If Office Communicator is installed, the end user will see the online status for all users who have permissions on the site collection.

## E-mail account requirements

To display online status, the presence feature uses a Session Initiation Protocol (SIP) address to communicate with the instant messaging client. If a SIP address is not available, a .NET address (MSN Messenger) or an Exchange Instant Messaging address (Windows Messenger) can be configured on an individual basis. However, only SIP addresses can take advantage of additional presence features, such as the ability to send and receive e-mail and to display free/busy information from the online status indicator.

# Plan incoming e-mail [Office SharePoint Server]

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [About incoming e-mail](#DSDOC_section1ca092ed2_4aa2_4c2e_b273_66)

 [Key decisions for planning incoming e-mail](#DSDOC_section2ca092ed2_4aa2_4c2e_b273_66)

 [Configuration options and settings modes](#DSDOC_section3ca092ed2_4aa2_4c2e_b273_66)

 [Before configuring incoming e-mail](#DSDOC_section4ca092ed2_4aa2_4c2e_b273_66)

 [Plan the Microsoft SharePoint Directory Management service](#DSDOC_section5ca092ed2_4aa2_4c2e_b273_66)

## About incoming e-mail

Incoming e-mail is a feature of Microsoft Office SharePoint Server 2007 that enables SharePoint sites to receive and store e-mail messages and attachments in lists and libraries. This new feature enables teams to store the e-mail that they send to other team members without opening the SharePoint site and uploading the content that was sent in e-mail. This is possible because most types of lists and libraries can be assigned a unique e-mail address.

This article helps server and farm administrators understand the choices they need to make before they deploy the incoming e-mail feature for their organization.

## Key decisions for planning incoming e-mail

There are several key decisions that you can make as you plan for incoming e-mail. These decisions include whether to:

 Accept e-mail from all e-mail servers or only safe e-mail servers.

 Use the directory management service to create distribution lists and contacts from SharePoint sites.

 Specify the folder that you want the system to check for incoming e-mail.

 Specify the e-mail server address that will be displayed in Web pages when users create an incoming e-mail address for a site, list, or group.

Some scenarios — for example, using the directory management service — require one or more IT professionals to implement. Nonetheless, you can still implement a basic incoming e-mail scenario even if your organization does not have an IT staff.

### Basic scenario

If your organization does not have an IT professional staff, you can enable a basic incoming e-mail scenario by installing the Simple Mail Transfer Protocol (SMTP) service on the server running Office SharePoint Server 2007 and enabling incoming e-mail by using the automatic settings mode with all default settings. In this scenario, e-mail is delivered directly to your SMTP server and Office SharePoint Server 2007 periodically checks for e-mail in the default e-mail drop folder that is automatically configured by the SMTP service.

Selecting the automatic settings mode and accepting all the default settings is the easiest way to enable incoming e-mail because all configuration settings are made for you and, therefore, little expertise is required. For most organizations, this configuration is all that is needed.

You enable a basic incoming e-mail scenario in the following steps:

1. The server administrator uses the Windows Components Wizard to install the E-mail Services component on the server that you want to receive incoming e-mail. This installs and starts the SMTP service on that server.

2. The farm administrator enables incoming e-mail by using the automatic settings mode and accepting all the default values.

3. The site collection administrator enables the incoming e-mail feature on the libraries and lists in which they want to store incoming e-mail and assigns each library and list a unique e-mail address in the form address@SMTPserveraddress. For example, sharedfiles@SMTPserver.contoso.com.

When users send e-mail to the address of a list or library, Office SharePoint Server 2007 detects that new e-mail has been delivered and sends it to the appropriate list or library based on the e-mail address.

note_ddNote:

If this basic scenario meets your needs, you can skip the remainder of this article. For more information, see "Configure incoming e-mail" in the Help system.

### Advanced scenarios

For more advanced administrators, additional choices are available, some of which require more expertise to deploy than choosing the basic scenario with all default options. This section describes the following configuration options:

 Safe e-mail server

 E-mail drop folder

 Microsoft SharePoint Directory Management service

 Incoming e-mail server display address

#### Safe e-mail server

You can configure Office SharePoint Server 2007 to accept e-mail from any e-mail server or only e-mail that has been routed through a safe-e-mail server application, such as Microsoft Exchange Server.

This option requires an IT professional to configure the e-mail routing through the safe e-mail server and is available only in automatic mode.

You can derive the following benefits by routing e-mail through a safe e-mail server:

 User authentication   The SMTP service cannot authenticate users who send e-mail to your site, but Exchange Server can. The server administrator can use the SharePoint Central Administration Web site to specify that the system accept e-mail from authenticated users only if the e-mail is sent through Exchange Server.

 Spam filtering    Exchange Server provides spam filtering to eliminate unsolicited commercial e-mail before it is forwarded to its destination — in this case, the server running Office SharePoint Server 2007. Another technique that can reduce spam is to allow members of the team site to archive e-mail only in lists on which you have granted write permissions to members.

 Virus protection   Exchange Server provides virus protection for e-mail routed through it.

|  |
| --- |
| Worksheet action |
| Record your decisions about safe e-mail servers in the Safe e-mail servers section of the Plan incoming e-mail worksheet : |

#### E-mail drop folder

You can specify the location from which Office SharePoint Server 2007 retrieves incoming e-mail. The benefit of using this option is that it enables Office SharePoint Server 2007 to retrieve incoming e-mail from a network share on another server. However, we recommend that you do not do this. This is because Office SharePoint Server 2007 cannot detect configuration changes on the remote e-mail server that is delivering the e-mail to your drop folder. This means that if an administrator configures the e-mail server to no longer deliver e-mail to this folder, Office SharePoint Server 2007 cannot detect that the configuration has changed, and therefore will not be able to retrieve the files from the new location.

You can also use the SMTP service to receive e-mail and specify the folder to which e-mail will be dropped instead of accepting the SMTP service's default setting. This is useful when the default folder location is full or nearly full.

note_ddNote:

When incoming e-mail settings are set to advanced mode, you must ensure that the logon account for the Windows SharePoint Services Timer service has modify permissions on the e-mail drop folder.

|  |
| --- |
| Worksheet action |
| Record your decisions about the e-mail drop folder in the E-mail drop folder section of the Plan incoming e-mail worksheet. |

note_ddNote:

Because this option is only available in advanced mode, you cannot specify an e-mail drop folder and also specify one or more safe e-mail servers.

#### Microsoft SharePoint Directory Management service

The Microsoft SharePoint Directory Management service connects SharePoint sites to your organization's user directory to provide enhanced e-mail features. The benefit of using this service is that it enables users to create and manage e-mail distribution groups from SharePoint sites. This service also creates contacts in your organization's user directory so people can find e-mail-enabled SharePoint lists in their address books.

A typical directory management scenario proceeds in the following steps:

1. A site collection administrator creates a new SharePoint group.

2. The administrator chooses to create a distribution list to associate with that SharePoint group and assigns an e-mail address to that distribution list.

3. Over time, the administrator adds users to and removes users from this SharePoint group. As users are added to and removed from the group, the SharePoint Directory Management service automatically adds and removes them from the distribution list, which is stored in the Active Directory directory service. Because distribution lists are associated with a particular SharePoint group, this distribution list is available to all members of that SharePoint group.

4. Because the SharePoint Directory Management service is used, e-mail addresses are automatically generated for the discussion boards and calendars on team sites, by default, and added to the team distribution list. The e-mail addresses for these two lists will be in the following form, by default: GroupAddress.discussions and GroupAddress.calendar.

5. By including e-mail addresses for discussion boards and calendars in the distribution list, all e-mail and meeting invitations sent to this distribution list will be archived in the team site.

For more information about planning for the SharePoint Directory Management service, see "Planning the Microsoft SharePoint Directory Management service" later in this article.

#### Incoming e-mail server display address

Administrators can specify the e-mail server address that will be displayed in Web pages when users create an incoming e-mail address for a site, list, or group. This setting is often used in conjunction with the Microsoft SharePoint Directory Management service to provide a more friendly e-mail server address for users to type.

|  |
| --- |
| Worksheet action |
| Record your decisions about the incoming e-mail server display address in the Incoming e-mail server display address section of the Plan incoming e-mail worksheet:. |

## Configuration options and settings modes

As a farm administrator, you have two settings modes from which to choose when enabling incoming e-mail: automatic and advanced. As described in the "Basic scenario" section above, you can choose the automatic settings mode with default settings. However, the automatic settings mode has additional options that you can choose.

The following table describes the configuration options and whether they are configured on the Configure Incoming E-Mail Settings page in Central Administration by using the automatic settings mode or the advanced settings mode.

|  |  |  |
| --- | --- | --- |
| Configuration option | Automatic settings mode | Advanced settings mode |
| Safe e-mail servers | Yes | No |
| E-mail drop folder | No | Yes |
| SharePoint Directory management service | Yes | Yes |
| Incoming e-mail server display address | Yes | Yes |

The advanced and automatic settings modes are similar in that they both enable farm administrators to configure the Microsoft SharePoint Directory Management service and the e-mail server address to display in Web pages. These settings modes differ in that the automatic settings mode replaces the ability to choose what e-mail servers to accept e-mail from with the ability to specify the folder to which e-mail is dropped. Office SharePoint Server 2007 uses this e-mail drop folder to detect new e-mail messages.

note_ddNote:

The e-mail drop folder setting is not available in automatic mode, because that mode automatically sets the e-mail drop folder to the folder that is specified by the SMTP service.

## Before configuring incoming e-mail

Before configuring incoming e-mail, perform the following tasks:

 Install the SMTP service on each server on which you want to receive and process incoming e-mail. Alternatively, provide another way for e-mail to be delivered to your e-mail drop folder.

 If you use the SMTP service on the server running Office SharePoint Server 2007, ensure that the server is running the Windows SharePoint Services Web Application service. This enables e-mail that is received on the Web server to be processed by Office SharePoint Server 2007.

For more information about installing the SMTP service, see the Windows Help system.

## Plan the Microsoft SharePoint Directory Management service

You can configure the Microsoft SharePoint Directory Management service by using either the automatic settings mode or the advanced settings mode. You can choose to enable the Microsoft SharePoint Directory Management service on your server or server farm running Office SharePoint Server 2007, or use the Microsoft SharePoint Directory Management service of another farm. One advantage of using the service running on another farm is that Active Directory permissions are managed in a centralized place (that is, on the other farm).

To enable this service on your own server or server farm running Office SharePoint Server 2007, the SharePoint Central Administration application pool account used by Office SharePoint Server 2007 must have write access to the container that you specify in Active Directory. This requires an Active Directory administrator to set up the organizational unit (OU) and the permissions on the OU. The advantage of using the Microsoft SharePoint Directory Management service on a remote farm is that you do not need the help of an Active Directory administrator to create and configure the OU if the OU already exists.

### Directory management service configuration options

When you configure the Microsoft SharePoint Directory Management service to create distribution groups and contacts in Active Directory, you must provide the following information:

 Name of the Active Directory container where new distribution groups and contacts will be created. This must be provided in the following format:

OU=ContainerName, DC=DomainName, DC=TopLevelDomainName

 Name of the SMTP server to use for incoming e-mail (or accept the default SMTP server if one exists). This must be provided in the following format:

Server.subdomain.domain.top-level\_domain

For example, SharePointServer.support.contoso.com

 Whether to accept messages from only authenticated users.

 Whether to allow users to create distribution groups from SharePoint sites. If you choose yes for this option, you can also choose whether users can do any of the following actions:

 Create a new distribution group.

 Change a distribution group's e-mail address.

 Change a distribution group's title and description.

 Delete a distribution group.

When configuring the Microsoft SharePoint Directory Management service to create distribution groups and contacts using a remote Microsoft SharePoint Directory Management service, you must provide the following information:

 The URL of the remote directory management service. For example, http://server:adminport/\_vti\_bin/SharePointEmailWS.asmx.

 The name of the SMTP server to use for incoming e-mail.

 Whether to accept messages from only authenticated users.

 Whether to allow users to create distribution groups from SharePoint sites.

|  |
| --- |
| Worksheet action |
| Record your decisions about the directory management service in the Directory management service section of the Plan incoming e-mail worksheet. |

## Worksheet

Use the following worksheet to record your decisions about incoming e-mail

 Plan incoming e-mail worksheet

# Plan outgoing e-mail [Office SharePoint Server]

In this article:

 [About outgoing e-mail](#DSDOC_section175401651_ef01_4348_878e_8a)

 [General requirements](#DSDOC_section275401651_ef01_4348_878e_8a)

 [Outbound SMTP server](#DSDOC_section375401651_ef01_4348_878e_8a)

 [From and Reply-to addresses](#DSDOC_section475401651_ef01_4348_878e_8a)

 [Character set](#DSDOC_section575401651_ef01_4348_878e_8a)

Outgoing e-mail is the foundation on which site administrators can implement several compelling e-mail notification features. These features help end users track changes and updates to individual site collections and allow site administrators to deliver status messages. These e-mail features include both e-mail alerts and administrative messages.

 Alerts   In a large and growing site collection, users need an efficient way to keep up with updates to lists, libraries, discussions, and other important parts of the site. Setting up alerts provides an effective means to stay on top of changes. For example, if several different groups are dependent on each other for reviewing documents, individuals in each group can set up alerts to be notified whenever there are changes to the documents they are responsible for. Users can specify which areas of the site collection or which documents they want to track and decide how often they want to receive alerts.

note_ddNote:

Users must have at least View permissions to set up alerts.

 Administrative messages   Site administrators might want to receive notices when users request access to a site or when site owners have exceeded their specified storage space. Setting up outgoing e-mail enables site administrators to receive automatic notifications for site administration issues.

This article will help site administrators understand both the uses for integrating outgoing e-mail and the requirements for integrating it into their site collections.

## About outgoing e-mail

Properly configuring outgoing e-mail is a requirement for implementing e-mail alerts and notifications. The outgoing e-mail feature uses an outbound Simple Mail Transfer Protocol (SMTP) service to relay e-mail alerts and notifications.

Outgoing e-mail support can be enabled at both the server farm level (available in the Operations section of Central Administration) and at the Web application level (available in the Application Management section of Central Administration). Therefore, you can specify different settings for a specific Web application. Outgoing e-mail settings at the Web application level override those set up at the server farm level.

## General requirements

The outgoing e-mail settings include several components that must be considered when planning for this feature:

 An SMTP service to relay e-mail alerts and notifications. You will need the DNS name or IP address of the SMTP mail server to use.

 An address to use in the header of an alert message that identifies who the message is from.

 A Reply-to address that is displayed in the To field of a message when a user replies to an alert or notification.

 A character set to use in the body of alert messages.

## Outbound SMTP server

The SMTP service is a component of Internet Information Services (IIS); however, it is not enabled by default with IIS. It can be enabled by using the Add or Remove Programs in Control Panel.

After determining which SMTP server to use, the SMTP server must be configured to allow anonymous access and to allow e-mail messages to be relayed. Additionally, the SMTP server must have Internet access if you want the ability to send messages to external e-mail addresses.

For more information about installing, configuring, and managing the SMTP service, see the Help for Internet Information Services (IIS) Manager (http://go.microsoft.com/fwlink/?LinkId=72343).

note_ddNote:

Only a member of the Farm Administrators group can configure an SMTP server. The user must also be a member of the local Administrators group on the server.

## From and Reply-to addresses

The two e-mail addresses that you can specify when configuring outgoing e-mail settings are the From address and the Reply-to address.

 From address   Alerts and notifications are sent from an administrative account on the server farm. This account is probably not the one you want to be displayed in the From field of an e-mail message. The address that you use does not need to correspond to an actual e-mail account; it can be a simple friendly address that is recognizable to an end user. For example, "Site administrator" might be an appropriate From address.

 Reply-to address   This is the address that will be displayed in the To field of a message if a user replies to an alert or notification. The Reply-to address should also be a monitored account to ensure that end users receive prompt feedback for issues they might have. For example, a Help Desk alias might be an appropriate Reply-to address.

## Character set

When you configure e-mail settings, you will need to specify the character set to use in the body of e-mail messages. A character set is a mapping of characters to their identifying code values. The default character set for outgoing e-mail is Unicode UTF-8, which allows most combination of characters (including bidirectional text) to co-exist in a single document. In most cases, the default setting of UTF-8 works well, although East Asian languages are best rendered with their own character set.

Be aware that if you select a specific language code, the text is less likely to appear correctly in mail readers configured for other languages.

# IX Plan document management

In this chapter:

 [Chapter overview: Plan document management](#DSDOC_cb57d4f7_8353_420b_8a10_d05c9bdf1b)

 [What is document management?](#DSDOC_15e6e3a3_9d35_47af_b287_13aec95d24)

 [Identify document management participants and stakeholders](#DSDOC_e80829b7_48e4_4589_8984_848578f85c)

 [Analyze document usage](#DSDOC_185da9e8_9ed1_4bf1_bfb5_2a5a874f2a)

 [Plan document libraries](#DSDOC_33b67ac7_54c3_42d8_87cd_5d7a00f729)

 [Plan content types [Office SharePoint Server]](#DSDOC_63bb092a_00fe_45ff_a4b8_d8be998d1a)

 [Plan workflows for document management](#DSDOC_34bc3a16_91f6_4c62_ae09_821cb94155)

 [Plan versioning, content approval, and check-outs](#DSDOC_428b488e_2807_4ef0_b942_91cb09d892)

 [Plan Information Rights Management](#DSDOC_073bfc71_7b01_4b77_bdc3_ac018889d5)

 [Plan information management policies](#DSDOC_4de4007d_a45f_419d_9512_824421e143)

 [Plan enterprise content storage](#DSDOC_9994b57f_fef8_44e7_9bf9_ca620ce207)

# Chapter overview: Plan document management

Microsoft Office SharePoint Server 2007 includes document management features that you can use to control the life cycle of documents in your organization — how they are created, reviewed, published, and consumed, and how they are ultimately disposed of or retained. The articles in this chapter will guide you in planning the document management features of your solution based on Office SharePoint Server 2007.

The articles in this chapter include:

 [What is document management?](#DSDOC_15e6e3a3_9d35_47af_b287_13aec95d24) includes an introduction to document management in the enterprise, along with a description of the document management planning process recommended in this planning guide.

 [Identify document management participants and stakeholders](#DSDOC_e80829b7_48e4_4589_8984_848578f85c) describes the creation of a document management planning team.

 [Analyze document usage](#DSDOC_185da9e8_9ed1_4bf1_bfb5_2a5a874f2a) provides guidance on determining the types of documents used in your enterprise and analyzing the stages in the documents' life cycles.

 [Plan document libraries](#DSDOC_33b67ac7_54c3_42d8_87cd_5d7a00f729) describes using document libraries to organize documents in your enterprise.

 [Plan content types [Office SharePoint Server]](#DSDOC_63bb092a_00fe_45ff_a4b8_d8be998d1a) describes planning content types, which are the Office SharePoint Server 2007 mechanism for defining and sharing the attributes of documents, list items, and folders.

 [Plan versioning, content approval, and check-outs](#DSDOC_428b488e_2807_4ef0_b942_91cb09d892) provides guidance on planning content control in Office SharePoint Server 2007, such as by using versioning, check-in and check-out, and approval for publishing content.

 [Plan Information Rights Management](#DSDOC_073bfc71_7b01_4b77_bdc3_ac018889d5) describes how to plan Information Rights Management on documents stored in document libraries so that you can control which actions users can take on documents when they open them from libraries in Office SharePoint Server 2007.

 [Plan workflows for document management](#DSDOC_34bc3a16_91f6_4c62_ae09_821cb94155) describes how to use the Office SharePoint Server 2007 workflow feature to design document-related processes.

 [Plan information management policies](#DSDOC_4de4007d_a45f_419d_9512_824421e143) describes planning and implementing enterprise policies that will help your organization comply with regulatory and legal obligations, in addition to best practices such as auditing documents and retaining them properly

 [Plan enterprise content storage](#DSDOC_9994b57f_fef8_44e7_9bf9_ca620ce207) contains information to help solution planners and designers properly plan and configure a large-scale enterprise content management solution based on Office SharePoint Server 2007 so that it performs well while providing the features needed by site users.

## See Also

[Chapter overview: Plan records management](#DSDOC_271017e8_7f23_4166_9501_140ad2fc55)

# What is document management?

In this article:

 [The elements of a document management system](#DSDOC_section115e6e3a3_9d35_47af_b287_13)

 [The planning process](#DSDOC_section215e6e3a3_9d35_47af_b287_13)

Document management controls the life cycle of documents in your organization — how they are created, reviewed, published, and consumed, and how they are ultimately disposed of or retained. Although the term "management" implies top-down control of information, an effective document management system should reflect the culture of the organization using it. The tools you use for document management should be flexible, allowing you to tightly control documents' life cycles if that fits your enterprise's culture and goals, but also letting you implement a more loosely structured system if that better suits your enterprise.

A well-designed document management system promotes finding and sharing information easily. It organizes content in a logical way, and makes it easy to standardize content creation and presentation across an enterprise. It promotes knowledge management and information mining. It helps your organization meet its legal responsibilities. It provides features at each stage of a document's life cycle, from template creation to document authoring, reviewing, publishing, auditing, and ultimately destroying or archiving.

## The elements of a document management system

An effective document management solution specifies:

 What types of documents and other content can be created within an organization.

 What templates to use for each type of document.

 What metadata to provide for each type of document.

 Where to store documents at each stage of a document's life cycle.

 How to control access to a document at each stage of its life cycle.

 How to move documents within the organization as team members contribute to the documents' creation, review, approval, publication, and disposition.

 What policies to apply to documents so that document-related actions are audited, documents are retained or disposed of properly, and content important to the organization is protected.

 How documents are converted as they transition from one stage to another during their life cycles.

 How documents are treated as corporate records, which must be retained according to legal requirements and corporate guidelines.

Microsoft Office SharePoint Server 2007 includes features that implement all of these aspects of document management. To ensure that information workers can easily take advantage of these capabilities without having to depart from their day-to-day operations and familiar tools, applications in the Microsoft Office 2007 system — such as Microsoft Outlook and Microsoft Word — also include features that support each stage in a document's life cycle.

## The planning process

The document management planning process consists of the following major steps:

1. Identify document management roles   Ensure that your plans incorporate the feedback of your organization's key stakeholders, that you have the right team in place to implement the solution, and that you know who will participate in document management processes. See [Identify document management participants and stakeholders](#DSDOC_e80829b7_48e4_4589_8984_848578f85c) for more information about creating a document management planning team.

2. Analyze document usage   After you identify who works on documents, determine the types of documents they work on and how they will be used. For more information, see [Analyze document usage](#DSDOC_185da9e8_9ed1_4bf1_bfb5_2a5a874f2a).

3. Plan the organization of documents   You can organize documents in libraries, team sites, and portal sites. Office SharePoint Server 2007 offers a range of document organizing and storing features, from specialized sites such as the Records Repository to free-form document libraries for ad-hoc document creation and collaboration. Within a library, you can further organize content into folders and subfolders. For more information, see [Plan document libraries](#DSDOC_33b67ac7_54c3_42d8_87cd_5d7a00f729).

4. Plan how content moves between locations   It may be necessary to move or copy a document from one site or library to another at different stages of its life cycle. For example, the publishing process may include moving a document from a staging site to a public Internet site. If content needs to be converted from one format to another as it moves from site to site, you will also want to plan content conversions. For more information, see "Plan the flow of content" in the topic [Plan document libraries](#DSDOC_33b67ac7_54c3_42d8_87cd_5d7a00f729).

5. Plan content types   Use content types to organize information about types of documents, such as metadata, document templates, policies, and workflow processes. This is an essential step to help you organize your documents and enforce consistency across your organization. For more information, see [Plan content types [Office SharePoint Server]](#DSDOC_63bb092a_00fe_45ff_a4b8_d8be998d1a).

6. Plan content control   You can plan the appropriate degree of control for each content type and storage location. For example, for a document library you can plan to require check-in and check-out and to protect documents from unauthorized distribution by using Information Rights Management. For more information, see [Plan versioning, content approval, and check-outs](#DSDOC_428b488e_2807_4ef0_b942_91cb09d892).

7. Plan workflows   By planning workflows for your organization, you can control and track how documents move from one team member to another as each participant collaborates in a document's life cycle. Office SharePoint Server 2007 includes workflows for common team tasks such as reviewing and approving documents. Office SharePoint Server 2007 also supports creating and installing custom workflows. For more information, see [Plan workflows for document management](#DSDOC_34bc3a16_91f6_4c62_ae09_821cb94155).

8. Plan policies   For each content type, plan information management policies to ensure that documents are properly audited, retained, labeled, and otherwise handled according to your organization's institutional and legal requirements. Office SharePoint Server 2007 includes policies that implement auditing, document retention, labeling, and barcodes (to ensure that printed content can be correlated with corresponding versions in document libraries). For more information, see [Plan information management policies](#DSDOC_4de4007d_a45f_419d_9512_824421e143).

# Identify document management participants and stakeholders

The first step in your document management planning is to determine the stakeholders and participants in your document management solution. You can use a survey to collect this information. For example, your survey might contain the following questions:

1. Who in your organization creates documents?

2. What types of documents do they create?

3. Who reviews documents?

4. Who edits documents?

5. Who uses documents?

6. Who approves the publication of documents?

7. Who designs Web sites used for hosting documents?

8. Who sets guidelines and policies for managing documents?

9. Who manages records in your organization?

10. Who deploys and maintains the servers on which documents are stored?

|  |
| --- |
| Worksheet action |
| Each of these questions can yield multiple answers. Record the information you gather from the survey in the [Document management participants worksheet](http://go.microsoft.com/fwlink/?LinkId=73285&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73285&clcid=0x409), as in the following example. |

|  |  |  |
| --- | --- | --- |
| Position | Types of documents | Role |
| Financial analyst  Technical writer | Equity research note  Financial model  Web page | Author |
| Financial analyst  Manager | Equity research note  Financial model | Reviewer |
| Technical editor | Equity research note  Web page | Editor |
| Customer | Equity research note  Financial model  Web page | Reader |
| Corporate lawyer  Manager | Equity research note  Financial model  Web page | Content approver |
| Server administrator | All | IT specialist |
| Database manager | All | Database specialist |
| Compliance officer | All | Legal specialist |
| Records manager | All | Records manager |
| Site manager | All | Content publisher |
| Site administrator | All | Content auditor |

Identifying content stakeholders can help you ensure that your document management solution is comprehensive, and that you design sites and document libraries that suit your enterprise's content needs and processes.

## Worksheet

[Document management participants worksheet](http://go.microsoft.com/fwlink/?LinkId=73285&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73285&clcid=0x409)

# Analyze document usage

After you identify your content stakeholders, collect information from them that will help you analyze how documents are used in your organization. This is an important part of the planning process because the analysis helps you determine:

 How document libraries are structured.

 Which site templates to use.

 How many sites you will need.

 Which information management policies to apply to the sites.

 Which physical server topology you will need to implement your solution.

The information to collect includes:

 Document type, such as equity research note, employee performance review, internal memo, or product specification.

 Purpose of each document type, such as "provides customers with recommendations about equities along with supporting data."

 Author of each document type (listed as roles, not individuals, such as "Financial Analyst," "Human Resources Specialist," or "Product Manager").

 Format of the document. If the document is transformed from one format to another, record that information.

 Users of each document type, such as "customers" or "team members."

 Other roles that apply to the document's life cycle, such as "technical reviewer" or "copy editor."

 Location of the document, such as "client computer," "Web server," or "file server." Note that this question could have multiple answers, such as when a document is authored on a client computer and then published to a Web server.

 How readers view the document, such as from a Web page or a file share.

|  |
| --- |
| Worksheet action |
| The [Analyze document usage worksheet](http://go.microsoft.com/fwlink/?LinkId=73284&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73284&clcid=0x409) is provided to record your document usage analysis. The following are examples of information that might be collected and recorded in the worksheet from two different organizations in an enterprise. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Type | Purpose | Author | User | Format | Other Roles | Locations |
| Equity research note | Gives premium customers of a financial service guidance on whether to buy or sell one or more stocks | Financial analyst | Customer | DOCX (for authoring); PDF (for publishing) | Reviewer (technical); reviewer (legal); approver; copy editor; records manager; site administrator |  Authoring site   Testing site   Internet   Records repository |

Analysis   The separate authoring and publishing formats require a format conversion. The large number of reviewers requires one or more workflows (business processes implemented on the server). The four sites (authoring, testing, Internet, and records repository) require mechanisms for moving the content from one site to another. The need to archive the content in a corporate records repository and the regulatory implications of publishing equities advice require corporate policies and best practices such as content auditing and retention.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Type | Purpose | Author | User | Format | Other Roles | Locations |
| Employee performance review | Evaluates the performance of an employee — including self-evaluation and manager's evaluation | Information worker; manager | Managers; human resources specialists | .DOC | Reviewer (human resources); reviewer (legal); approver (upper manager); records manager |  Client computer   E-mail server (as attachment)   Corporate Web server   Corporate records repository |

Analysis   Two authors and multiple reviewers require one or more workflows. The document travels from one desktop computer to another as an e-mail attachment, then resides in a corporate Web server (presumably highly locked down) and is archived in a records repository. The sensitive nature of this content requires Information Rights Management (IRM) on the desktops and servers, in addition to corporate policies and best practices (such as auditing) that protect the employee's privacy and the enterprise's legal standing.

## Worksheet

Use the following worksheet to record the information discussed in this article:

 [Analyze document usage worksheet](http://go.microsoft.com/fwlink/?LinkId=73284&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73284&clcid=0x409)

# Plan document libraries

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [Plan document libraries](#DSDOC_section133b67ac7_54c3_42d8_87cd_5d)

 [Plan the flow of content](#DSDOC_section233b67ac7_54c3_42d8_87cd_5d)

 [Promoting document libraries from Office client programs](#DSDOC_section333b67ac7_54c3_42d8_87cd_5d)

Document libraries are collections of files on Microsoft Office SharePoint Server 2007 that you share with other site users. Most Microsoft Office SharePoint Server 2007 document management features are delivered through document libraries. As part of document management planning, you should determine the document libraries that best fit your organization's needs.

When you identify which document libraries best match your organization's needs, you might also determine that you need multiple sites or site collections. For example, if you are authoring content for publication to external customers, you might need one site (and library) in which to author and review content and a separate site, perhaps in a separate Office SharePoint Server 2007 installation, in which to publish your content.

When you plan document libraries over multiple sites, you may also need to plan how content flows from one site to another — by manual processes, workflows, or custom solutions.

## Plan document libraries

The following table lists typical uses of document libraries in Office SharePoint Server 2007.

|  |  |
| --- | --- |
| Library | Purpose |
| Library in a team site | Collaboration; easy sharing of content among peers; content control, such as versioning and moderation; Office SharePoint Server 2007 searching. |
| Library in a portal area | Content that is intended for a wider audience in the organization; similar to a library in a team site, but typically implemented with a more-stringent review and approval process. |
| Library in a Document Center site | A large-scale library useful as an enterprise knowledge base or historical archive; includes features to help users navigate, search, and manage a large number of documents in a deep hierarchy by using a set of specialized Web Parts. |
| Library in a Records Repository | Specialized records management; each library corresponds to a record type, such as contract, that the organization must retain for legal compliance purposes; libraries retain documents, metadata, and associated audits and are meant to be read-only. |
| Library in an Internet site (HTML) | Contains Web pages to incorporate in an Internet or intranet Web site; Office SharePoint Server 2007 supports editing Web pages directly and manages the underlying document libraries for each page automatically. |
| Library in an Internet site (hybrid) | Content available for downloading from a Web site; you can present content from document libraries on an Internet site. |
| Translation management document library | Designed for translating documents, if your enterprise works in multiple languages. It includes a specialized translation workflow and views that show multiple language versions of the same document or all documents in a particular language. |
| Slide library | Supports sharing, managing, and reusing Microsoft Office PowerPoint 2007 slides. |

The following example illustrates how to use the analysis that you completed in [Analyze document usage](#DSDOC_185da9e8_9ed1_4bf1_bfb5_2a5a874f2a) to help you plan document library organization for your enterprise. In this example, Contoso Ltd. delivers content to clients based on market research. The content is created primarily by consultants operating remotely. This is done in a cycle in which:

1. A partner evaluates engagement ideas and requests for proposals.

2. After a contract is established, a project manager assembles a team of consultants and creates an engagement-specific working site in which the results of the research are recorded and the project is completed.

3. When the project is done, the deliverable documents are published to a secured Internet site, where customers have access to them.

4. The team writes best practices documents and case studies based on the project.

5. Knowledge managers collect, organize, and archive the best practices and other documents.

6. Deliverables, contracts, and other records are retained as corporate records.

7. Using the content maintained by the knowledge managers, partners evaluate opportunities and create new proposals.

The following table illustrates a document usage analysis for this scenario.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Documents | Purpose | Author | Users | Format |
| Engagement ideas and requests | Develop new customer engagements | Project leader | Sales manager; project leader | .doc |
| Proposals | Describe a proposed customer engagement | Project leader | Project managers; project team members; customers | .doc |
| Contracts | Commit to a consulting engagement | Lawyer | Project leader; project manager; sales manager; customers | .doc |
| Research results and project deliverable drafts | Generate documents related to the customer engagement | Project leader; project contributor; consultant | Editors; technical reviewers | .doc and other types |
| Deliverable documents | Generate final deliverables, probably converted from .doc format | Project leader | Customers | .pdf |
| Best practices and case study documents | Capture organizational knowledge | Project contributor; consultant; knowledge manager | All team members | Various types |
| Corporate records | Retain some content, such as deliverable documents, as corporate records | All | Corporate records managers; corporate lawyers | All |

This document usage analysis suggests the following conclusions:

 Project leaders need libraries in team sites for storing engagement ideas, engagement requests, and proposal drafts.

 Lawyers need libraries in a portal area for storing contract templates and active contracts.

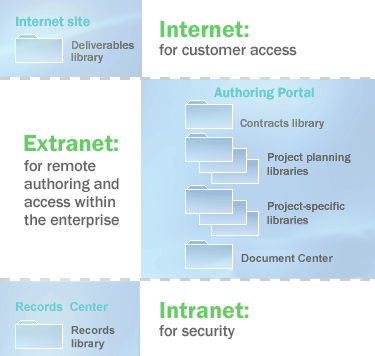
 Project leaders and contributors need libraries in team sites for authoring research results, deliverables, and case studies.

 Customers need libraries in an Internet site for viewing final deliverables.

 All members of the enterprise need access to a Document Center site for viewing best practices and case study documents.

 Corporate records managers and lawyers need access to an enterprise Records Repository to maintain corporate records.

The following figure illustrates how these libraries might be distributed. The sites are hosted in three site collections: an Internet site collection for customer access, an extranet site collection for remote authoring by team members, and an intranet site collection for secure maintenance of the records management site.



|  |
| --- |
| Worksheet action |
| The [Document libraries worksheet](http://go.microsoft.com/fwlink/?LinkId=77248&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=77248&clcid=0x409) is provided to record your library planning decisions. Use this worksheet to list the libraries required for your solution, along with the types of documents they contain. Note that libraries can contain more than one type of document. |

## Plan the flow of content

Content in a document management solution based on Office SharePoint Server 2007 is often dynamic, moving from one site to another as needed to meet document users' needs. When you plan document libraries, therefore, also plan the flow of content from one library or site to another. Office SharePoint Server 2007 includes the following ways to move content, either manually or dynamically:

 You can create custom workflows that copy or move content from one site or library to another. A workflow guides a document through a business process, assigning tasks to participants as their role in the document's life cycle becomes active. A workflow can be designed to move a document from one site or library to another. For information about planning workflows, see [Plan workflows for document management](#DSDOC_34bc3a16_91f6_4c62_ae09_821cb94155).

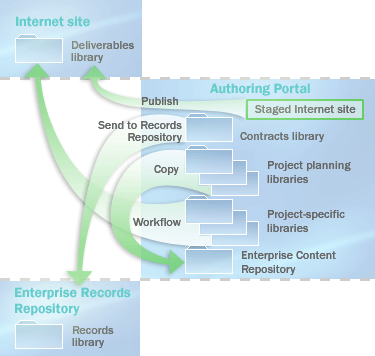
 Authors can copy a document to a library in any site in which they have authoring permissions. The relationship between the source and the destination document is maintained so that the copy can be refreshed as needed.

 Web pages and entire Web sites can be staged and published from one site to another either manually or automatically based on a schedule.

 Content can be sent to the records management site by using the Office SharePoint Server 2007 user interface, by using a workflow, or by using a custom solution based on the Microsoft Windows SharePoint Services 3.0 object model.

 Using Web Folders or Network Places, an author can manually copy or move the contents of a document library from one library or site to another.

Returning to our example, the following figure illustrates how to apply some of these content flow techniques. Note that the Staged Internet site has been added to the Authoring portal site.



 Using publishing features, Web pages are published to the Internet site.

 Using the Copy command, documents are copied to the Document Center site.

 Using a custom workflow, documents are copied to document libraries on the Internet site.

 Using the Send to Records Repository command, contracts are sent to the enterprise Records Repository.

## Promoting document libraries from Office client programs

You can customize the 2007 Office release Open and Save dialog boxes to encourage organization members to use document libraries as storage locations. By adding sites to the My Places bar next to the Open and Save dialog boxes, you can provide one-click access to the locations where users should store their documents. This enables team members to interact with the document libraries as part of the Save experience from 2007 Office release client programs, rather than having to go directly to the server to upload their documents.

To promote using sites in the Open and Save dialog boxes, you can publish them by using a Microsoft Office SharePoint Server 2007 Web service. This service provides a list of sites targeted to specific users based on their roles or the sites that they are members of. A 2007 Office release client program can automatically discover this Web service through the user's My SharePoint Sites. Other server products can also implement this Web service and provide the location of the service to the Office client. After this is configured, 2007 Office release adds an entry to the My Places bar and populates it with the locations defined by the Web service.

Alternatively, administrators can set registry keys to add specific sites to the My Places bar in the Office Open and Save dialog boxes. Registry keys are deployed by using Group Policy and a Microsoft Active Directory directory service template provided in the 2007 Office release Resource Kit.

You can limit the locations that organization members can save to using the Office Save dialog box. For example, you can restrict the ability to save files to desktops and force users to save content in a document library. In 2007 Office release, you can control where users are allowed to browse to save their documents, thereby guiding users to save in approved locations. Note that this does not guarantee that users won't save files to their local computers or other unapproved locations. There are many ways to get files onto a computer, and motivated people can work around most restrictions. However, by limiting access to these locations through the Office Save dialog box, you can dramatically reduce the number of team members who use these unapproved locations.

To restrict the locations available in the Office Save dialog box, use Group Policy to set the appropriate registry keys to enable this setting and define the approved local, network, or server locations. When this setting is enabled, any location not defined in this manner — including standard links to the Desktop and My Network Places — will be removed from the My Places bar.

The list of approved locations can be limited to one or more Office applications. For example, an administrator can restrict save locations in Microsoft Office Access 2007 while allowing other Office applications to save anywhere.

## [[16]](#footnote-17)#See Also

[Plan content types [Office SharePoint Server]](#DSDOC_63bb092a_00fe_45ff_a4b8_d8be998d1a)

# Plan content types [Office SharePoint Server]

In this article:

 [What are content types?](#DSDOC_section163bb092a_00fe_45ff_a4b8_d8)

 [Properties integration with the 2007 Office release](#DSDOC_section263bb092a_00fe_45ff_a4b8_d8)

 [About column templates](#DSDOC_section363bb092a_00fe_45ff_a4b8_d8)

 [About folder content types](#DSDOC_section463bb092a_00fe_45ff_a4b8_d8)

 [Planning document content types](#DSDOC_section563bb092a_00fe_45ff_a4b8_d8)

 [Planning list content types](#DSDOC_section663bb092a_00fe_45ff_a4b8_d8)

 [Planning document conversions](#DSDOC_section763bb092a_00fe_45ff_a4b8_d8)

 [After planning content types: next steps](#DSDOC_section863bb092a_00fe_45ff_a4b8_d8)

 [Worksheets](#DSDOC_section963bb092a_00fe_45ff_a4b8_d8)

This topic describes content types and related features, and provides guidance on planning content types for your solution based on Microsoft Office SharePoint Server 2007.

## What are content types?

A content type defines the attributes of a list item, a document, or a folder. Each content type can specify:

 Properties to associate with items of its type.

 Workflows that can be launched from items of its type.

 Information management policies to associate with items of its type.

 Document templates (for document content types).

 Document conversions to make available (for document content types).

 Custom features.

You can associate a content type with a list or library. When you do this, you are specifying that the list or library can contain items of that content type and that the New command in that list or library will let users create new items of that type.

note_ddNote:

Properties, workflows, policies, and templates can also be associated directly with a list or library. However, doing this limits these associations to the list or library and is not reusable across your solution.

Document libraries and lists can contain multiple content types. For example, a library can contain both the documents and the graphics related to a project. When a list or library contains multiple content types:

 The New command in that list or library lets users create new items of all the associated content types.

 The columns associated with all available content types are displayed.

You define custom content types in a site's content type gallery. A custom content type must be derived, directly or indirectly, from a core content type such as Document or Item. After it is defined in a site, a custom content type is available in that site and in all subsites below that site. To make a content type most broadly available, define it in the content type gallery of the top-level site in a site collection.

For example, if your organization uses a particular contract template, in the content type gallery of the top-level site in a site collection you can create a content type that defines the metadata for that contract, the contract's template, workflows required to review and complete the contract, policies that enforce auditing of actions related to the contract, a retention period for retaining the contract, and labels to insert in printed versions of the contract. Then, any document library in your site collection to which you associate the Contract content type will include all of these features and will enable authors to create new contracts based on the template.

In sites based on Office SharePoint Server 2007, each default list item or library item — such as Contact, Task, or Document — has a corresponding core content type in the site's content type gallery. When planning content types, you can use these core content type definitions as starting points, basing new content types on existing ones as needed or modifying the core types.

Content types are organized into a hierarchy that allows one content type to inherit its characteristics from another content type. This allows classes of documents to share characteristics across an organization, while allowing teams to tailor these characteristics for particular sites or lists.

For example, all customer deliverable documents in an enterprise may require a set of metadata such as account number, project number, and project manager. By creating a top-level Customer Deliverable content type from which all other customer deliverable document types inherit, you ensure that required information such as account numbers and project numbers will be associated with all variants of customer deliverable documents in your organization. Note that, if another required column is added to the top-level Customer Deliverable content type, the content type owner can propagate the changes to all content types that inherit from it, which will add the new column to all customer deliverable documents.

## Properties integration with the 2007 Office release

In the 2007 Microsoft Office system, when a user is editing a document from a Office SharePoint Server 2007 document management server, a Document Information Panel is shown at the top of the document. The Document Information Panel displays an editable form that reflects the document's properties on the server.

Office SharePoint Server 2007 makes it easy to customize the property form for a content type. When you configure a content type, you can start Microsoft Office InfoPath 2007, which generates a default property form based on the properties of the content type. The default form includes the same controls, layout, and schema that 2007 Office release would use if no custom form were defined. You can then customize and deploy the form as you would any other Office InfoPath 2007 InfoPath form. For example, you can add your company logo, fonts, and color scheme to a form; connect it to a custom data source; add conditional logic; and design form features that are available to users based on their roles.

Along with editing properties in the Document Information Panel, authors using Microsoft Office Word 2007 can insert properties defined on the server into their documents. For example, if the document properties include an attorney name, this name can be inserted into the title page, the footer, or anywhere else the name is used in the document. If a new attorney is assigned to a particular case, the Attorney Name property can be updated on the document management server; this updated attorney name will be reflected in every instance of this property that has been inserted into a document.

## About column templates

Each item of metadata associated with a content type is a column, which is a location in a list to store information. Lists or libraries in Office SharePoint Server 2007 are often displayed graphically as columns of information. However, depending on the view associated with the list, the columns can appear in other forms, such as days in a calendar display. In forms associated with a list or library, columns are displayed as fields.

You can define columns for use in multiple content types. To do this, create them in a Column Templates gallery. There is a Column Templates gallery in each site in a site collection. As with content types, columns defined in a site's Column Templates gallery are available in that site and in all of its subsites.

## About folder content types

Folder content types define the metadata associated with a folder in a list or library. When you apply a folder content type to a list or library, the New command in that list or library will include the folder content type, letting users create folders of that type.

You can define views in a list or library that are available only in folders of a particular content type. This is useful when you want a folder to contain a particular type of document and you want views in that folder to only display columns relevant to the document type contained in that folder.

Using the Office SharePoint Server 2007 object model, you can customize the New command for a folder content type so that, when a user creates a new folder of that type, the folder is pre-populated with multiple files and documents based on templates stored on the server. This is useful, for example, for implementing a compound document type that requires multiple files to contribute to a single deliverable document.

## Planning document content types

Plan document content types for your solution by using the Analyze document usage worksheet, which you filled in using the topic [Analyze document usage](#DSDOC_185da9e8_9ed1_4bf1_bfb5_2a5a874f2a). Use the Content type worksheet to record your decisions about each new content type.

Each document content type should inherit its settings directly from the core Document content type or from a content type that is descended from the Document content type. This will ensure that the basic columns for your document types, such as Title and Created By, are present and that you can associate a template with the content type.

The first stage in planning document content types is to review each document type listed in your Analyze document usage worksheet to determine if there is an existing content type available for documents of that type. If a core content type (such as Document) is sufficient, enter the content type name in the Content Type column of the Analyze document usage worksheet.

After reviewing your list of document types to determine which ones can use core content types, plan new document content types using the following steps. For each content type you plan, fill in a separate Plan a content type worksheet.

1. Enter the document type from the Analyze document usage worksheet.

2. Enter the site URL at which the new content type will be defined. Keep in mind that content types are available in the site in which they are defined and in all subsites below that site.

3. Determine the parent content type   Enter the parent content type in the "Parent Content Type" field of the Plan a content type worksheet. This will be either a core content type or a custom content type that you have already planned.

4. Determine the columns   In the "Plan Columns" table of the Plan a content type worksheet, do the following:

a. Enter each column inherited from the parent content type. In the New? column, type No for each entry.

b. For each additional column, enter the name of a pre-defined column or of a column that you will create. Keep in mind that the name of a column is important, because it can communicate the column's purpose. Therefore, even if a column of a type that you need is already defined in the Site Collection Column gallery, you might decide to define a similar column with a more relevant name for your application. Along with the names of the additional columns, enter their types and indicate whether or not they are new.

5. Determine the template   In the Plan Template section of the worksheet, enter the name of the template to associate with this content type along with its type (such as .Docx) and a brief description of the purpose of the template. If the template is not inherited from the parent content type, in the "New?" field, type No.

6. Determine the workflows   Workflows attach business logic to documents and list items in Microsoft Office SharePoint Server 2007. You can associate any available workflow with a content type; the workflow can then be initiated on any document of that content type. For a full discussion of workflow planning, see [Plan workflows for document management](#DSDOC_34bc3a16_91f6_4c62_ae09_821cb94155). After reviewing workflows and determining which workflows are available, enter each workflow to associate with the content type in the "Plan Workflows" table of the Plan a content type worksheet. If the workflow is not inherited from the parent content type, enter that information in the New? column.

7. Determine the policy   A policy is a set of rules for a type of content and is made up of policy features that provide the details of each rule, such as whether or not items of the content type can be printed or which actions on the item should be audited. You can apply a policy to any custom content type. Note that you cannot apply a policy to a core content type. For more information about policy planning, see [Plan information management policies](#DSDOC_4de4007d_a45f_419d_9512_824421e143). After reviewing policies and determining which policy features and policy templates are available, in the Plan a Policy section of the Plan a content type worksheet, do the following:

a. If the parent content type has policy settings, they will apply unchanged in the new content type. This ensures that policies, once set, are enforced in all relevant content types. If the current content type is inheriting its policy settings from its parent type, in the Plan a Policy section of the Plan a content type worksheet, answer Yes to the question, "Is the policy defined in the parent content type? Yes/No."

b. If the current content type is inheriting a policy based on the parent content type, in the "Record the Policy Name" field of the Plan a Policy section, type the name of the policy template. Similarly, if the current content type does not inherit a policy and you want to apply a policy template, in the "Record the Policy Name" field of the Plan a Policy section, type the name of the policy template.

c. If the current content type is inheriting one or more individual policy features from the parent content type, enter each policy feature in the "Feature" table in the Plan a Policy section of the worksheet. Conversely, if the current content type does not inherit a policy and you want to associate policy features with the current content type, enter those policy features in the "Feature" table. Note that you cannot associate both individual policy features and a policy by name to a content type.

8. Determine document conversions   Office SharePoint Server 2007 supports installing document conversion components on the server that transform documents from one format to another. For an overview of document conversions, see [Planning document conversions](#DSDOC_section763bb092a_00fe_45ff_a4b8_d8), below.

You can associate one or more document converters with a content type. For example, if a content type is associated with a template of type .docx, you can associate the From Word Document to Web Page converter that is included in Office SharePoint Server 2007 with the content type. This lets authors write documents of the content type in Microsoft Office Word 2007 and then convert them to Web pages for publication.

note_ddNote:

In the Office SharePoint Server 2007 Central Administration pages, administrators can enable a document converter so that it is available in any document library in a Web application. When a converter is enabled in this way, it is not necessary to associate it with content types in any site in the Web application.

In the Plan Document Conversions section of the Plan a content type worksheet, record each document converter to associate with the content type, specify if the converter is new (and requires installation), and add optional notes.

## Planning list content types

The elements of a list content type include the columns of metadata associated with the content type along with workflows that can run on items of that list content type. Use a list content type to define a type of list item unique to your solution. For example, in a customer call center solution, in which support professionals investigate and resolve customers' technical issues, a list content type could be used to standardize the data for each support incident and to support tracking the incident using a workflow.

|  |
| --- |
| Worksheet action |
| Plan new list content types using the following steps. For each list content type that you plan, fill in a separate Plan a content type worksheet. In the "Document Type" field of the worksheet, enter List.  1. Enter the site URL at which the new content type will be defined. Content types are available in the site in which they are defined and in all subsites below that site.  2. Determine the parent content type   Enter the parent content type in the "Parent Content Type" field of the Plan a content type worksheet. This will be either a core content type or a custom content type that you have already planned.  3. Determine the columns   In the "Plan Columns" table of the Plan a content type worksheet, do the following:  a. Enter each column inherited from the parent content type. In the New? column, type No for each entry.  b. For each additional column, enter the name of a pre-defined column or of a column that you will create. Along with the names of the additional columns, enter their types and indicate whether or not they are new.  4. In the Plan Template section of the worksheet, type None.  5. Determine the workflows   If there is an available workflow that is relevant to the list content type, you can optionally associate it with the content type. The workflow could then be initiated on any list item of that content type. For a full discussion of workflow planning, see [Plan workflows for document management](#DSDOC_34bc3a16_91f6_4c62_ae09_821cb94155). After reviewing workflows and determining which workflows are available, enter each workflow to associate with the content type in the "Plan Workflows" table of the Plan a content type worksheet. If the workflow is not inherited from the parent content type, enter that information in the New? column.  6. In the Plan a Policy section of the worksheet, type None. |

## Planning document conversions

Office SharePoint Server 2007 supports installing document conversion components on the server that transform documents from one format to another. Conversions can be run either from the user interface or programmatically, such as from a custom workflow. The relationship between source documents and their transformed counterparts is maintained. Office SharePoint Server 2007 includes converters that create Web pages from Microsoft Office Word 2007 documents and from Microsoft Office InfoPath 2007 forms.

Along with providing the infrastructure on the server to install and run document converters, Microsoft Office SharePoint Server 2007 includes a load balancer service that you can configure to optimize the use of your server resources. Part of planning document conversions is tuning your server farm to optimally balance the load as documents are transformed.

To be available to users, a converter must be installed on the server farm and then enabled by a server administrator. After a converter is enabled for a server, it is available to run on source documents on that server.

You configure document converters using the following steps:

1. In the document usage analysis that you perform in [Analyze document usage](#DSDOC_185da9e8_9ed1_4bf1_bfb5_2a5a874f2a), identify candidates for document conversion — that is, documents that are written in one format but that should be published or archived in another.

2. For each conversion needed, locate converter programs to implement the needed conversions on your servers.

3. If needed, install the conversion programs on application (middle tier) servers in your farm.

4. Configure the launcher and load balancer services, either on the Web servers or application (middle tier) servers.

5. Identify the points in your document flow at which conversions take place.

6. Identify how conversions will be implemented — either manually or using custom solutions that launch them.

## After planning content types: next steps

After planning document and list content types, here are some suggested next steps:

 If you haven't already done so, in the Content Type column of the Analyze document usage worksheet, record each content type that you planned.

 Sort your "Plan a content type" worksheets by site URL, and identify the new columns to define for each site.

 Identify new templates to design.

 Identify new workflows to plan and install.

 Identify new policy templates to plan and new policy features to plan and install.

## Worksheets

Use the following worksheets to record the information discussed in this article:

 [Analyze document usage worksheet](http://go.microsoft.com/fwlink/?LinkID=73284&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73284&clcid=0x409)

 [Content type worksheet](http://go.microsoft.com/fwlink/?LinkId=73288&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73288&clcid=0x409)

 [Plan a content type](Plan%20a%20content%20type) (http://go.microsoft.com/fwlink/?LinkId=73292&clcid=0x409)

# Plan workflows for document management

Workflows implement business processes on documents, Web pages, forms, and list items in Microsoft Office SharePoint Server 2007. They can be associated with libraries, lists, or content types. For an overview of workflows, see the topic Plan workflows (Office SharePoint Server).

In document management, use workflows to route documents from person to person so they can each complete their document management tasks, such as reviewing documents, approving their publication, or managing their disposition. Also, use custom workflows to move documents from one site or library to another. For example, you can design a workflow to copy a document from one site to another when the document is scheduled to be archived.

Office SharePoint Server 2007 includes workflows that address the following document management needs:

 Collect Feedback — Sends a document for review.

 Approval — Sends a document for approval, often as a prerequisite to publishing it.

 Disposition — Manages document expiration and disposition.

 Collect Signatures — Routes a document for signatures.

 Translation — Manages the translation of a document into one or more languages.

 East Asian Document Approval — Routes a document for approval using stamp signatures and a group-oriented consensus process.

Associate a workflow with a content type when you want to make that workflow available whenever that content type is in use. For example, a purchase order content type could require approval by a manager before completing the transaction. To ensure that the approval workflow is always available when a purchase order is initiated, create a Purchase Order content type and associate the approval workflow with it. Then add the Purchase Order content type to any document libraries in which purchase orders will be stored.

To plan workflows for your document management solution, analyze each document content type you plan to implement and identify the business processes that need to be available to run on content of that type. Then identify the workflows you will need to make available for that content. For more information about planning content types, see the topic [Plan content types [Office SharePoint Server]](#DSDOC_63bb092a_00fe_45ff_a4b8_d8be998d1a).

|  |
| --- |
| Worksheet action |
| In the Plan Workflows section of the [Plan a content type](http://go.microsoft.com/fwlink/?LinkId=73292&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73292&clcid=0x409), enter the name of each workflow and its purpose, and indicate if a new (custom) workflow is needed to implement the process. |

Here is a sample table analyzing workflows for a contract content type:

|  |  |  |
| --- | --- | --- |
| Contract Process | Contract Workflow | New? |
| Review drafts | Collect feedback | No |
| Get manager's and legal counsel's approval | Approval | No |
| Resolve open issues | Issue tracking | No |
| Get signatures | Collect signatures | No |

## Worksheet

Use the following worksheet to record the information discussed in this article:

 [Plan a content type worksheet](http://go.microsoft.com/fwlink/?LinkId=73292&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73292&clcid=0x409)

# Plan versioning, content approval, and check-outs

In this article:

 [Plan versioning](#DSDOC_section1428b488e_2807_4ef0_b942_91)

 [Plan content approval](#DSDOC_section2428b488e_2807_4ef0_b942_91)

 [Plan check-in and check-out](#DSDOC_section3428b488e_2807_4ef0_b942_91)

 [Worksheet](#DSDOC_section4428b488e_2807_4ef0_b942_91)

Microsoft Office SharePoint Server 2007 includes features that can help you control access to content. You configure settings for the content control features discussed in this article in document libraries. To share these settings across libraries in your solution, you can create document library templates that include your content control settings; this ensures that new libraries will reflect your content control decisions.

## Plan versioning

Versioning is the method by which successive iterations of a document are numbered and saved. Office SharePoint Server 2007 has three versioning options:

 None   Specifies that no previous versions of documents are saved. When no versioning is in use, previous versions of documents are not retrievable, and document history is also lost because comments that accompany each iteration of a document are not saved. Use this option on document libraries containing unimportant content or content that will never change.

 Major versions only   Specifies that numbered versions of documents are retained using a simple versioning scheme (such as 1, 2, 3). To control the effect on storage space, you can specify how many previous versions to keep, counting back from the current version.

In major versioning, each time a new version of a document is saved, all users with permissions to the document library will be able to view the content. Use this option when you do not want to differentiate between draft versions of documents and published versions. For example, in a document library that is used by a workgroup in an organization, major versioning is a good choice if everyone on the team needs to be able to view all iterations of each document.

 Major and minor versions   Specifies that numbered versions of documents are retained by using a major and minor versioning scheme (such as 1.0, 1.1, 1.2, 2.0, 2.1). Versions ending with .0 are major versions and versions ending with non-zero extensions are minor versions. Previous major and minor versions of documents are saved along with current versions. To control the effect on storage space, you can specify how many previous major versions to keep, counting back from the current version. You can also specify for how many major versions minor versions should be kept. For example, if you specify that minor versions should be kept for two major versions and the current major version is 4.0, then all minor versions starting at 3.1 will be kept.

In major and minor versioning, any user with read permissions can view major versions of documents. You can specify which users can view minor versions. Typically, grant users who can edit items permissions to view and work with minor versions, and restrict users with read permissions to viewing only major versions.

Use major and minor versioning when you want to differentiate between published content that can be viewed by an audience and draft content that is not yet ready for publication. For example, on a human resources Web site that describes organizational benefits, use major and minor versioning to restrict employees' access to benefits descriptions while the descriptions are being revised.

|  |
| --- |
| Worksheet action |
| In the [Document libraries worksheet](http://go.microsoft.com/fwlink/?LinkID=73306&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73306&clcid=0x409), for each document library listed, specify the versioning scheme to use: none, major, or major and minor. |

## Plan content approval

Content approval is the method by which site members with approver permissions control the publication of content. A document draft awaiting content approval is in the Pending state. When an approver reviews the document and approves the content, it becomes available for viewing by site users with read permissions. A document library owner can enable content approval for a document library and can optionally associate a workflow with the library to run the approval process.

Use content approval to formalize and control the process of making content available to an audience. For example, an enterprise that publishes content as one of its products or services might require a legal review and approval before publishing the content.

The way that documents are submitted for approval varies depending on the versioning settings in the document library:

 None   If no versioning is in use and changes to a document are saved, the document's state becomes Pending. Office SharePoint Server 2007 keeps the previous version of the document so users with read permissions can still view it. After the pending changes have been approved, the new version of the document is made available for viewing by users with read permissions and the previous version is discarded.

If no versioning is in use and a new document is uploaded to the document library, it is added to the library in the Pending state and is not viewable by users with read permissions until it is approved.

 Major versions only   If major versioning is in use and changes to a document are saved, the document's state becomes Pending and the previous major version of the document is made available for viewing by users with read permissions. After the changes to the document are approved, a new major version of the document is created and made available to site users with read permissions, and the previous version is saved to the document's history list.

If major versioning is in use and a new document is uploaded to the document library, it is added to the library in the Pending state and is not viewable by users with read permissions until it is approved as version 1.

 Major and minor versions   If major and minor versioning is in use and changes to a document are saved, the author has the choice of saving a new minor version of the document as a draft or creating a new major version, which changes the document's state to Pending. After the changes to the document are approved, a new major version of the document is created and made available to site users with read permissions. In major and minor versioning, both major and minor versions of documents are kept in a document's history list.

If major and minor versioning is in use and a new document is uploaded to the document library, it can be added to the library in the Draft state as version 0.1, or the author can immediately request approval in which case the document's state becomes Pending.

|  |
| --- |
| Worksheet action |
| In the [Document libraries worksheet](http://go.microsoft.com/fwlink/?LinkID=73306&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73306&clcid=0x409), specify whether or not to require content approval for each document library listed. |

## Plan check-in and check-out

You can require that users check documents in and out of a document library before editing the documents. It is always recommended to do this. The benefits of requiring checking in and out include:

 Better control of when document versions are created. When a document is checked out, the author can save the document without checking it in. Other users of the document library will not be able to see these changes and a new version is not created. A new version (visible to other users) is only created when an author checks in a document. This gives the author more flexibility and control.

 Better capture of metadata. When a document is checked in, the author can write comments that describe the changes made to the document. This promotes creation of an ongoing historical record of the changes made to the document.

If your solution requires that users check documents in and out when editing them, the 2007 Microsoft Office system client programs include features that support these actions. Users can check documents out, undo check-outs, and check documents in from 2007 Office release client programs.

When a document is checked out, it is saved in the user's My Documents folder in a subfolder named "SharePoint Drafts." This folder is displayed in Microsoft Office Outlook 2007. As long as the document is checked out, the user can only save edits to this local folder. When the user is ready to check the document in, the document is saved back to the original server location.

From 2007 Office release client programs, users can optionally choose to leave checked-out documents on the server by changing content editing options.

|  |
| --- |
| Worksheet action |
| In the [Document libraries worksheet](http://go.microsoft.com/fwlink/?LinkID=73306&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73306&clcid=0x409), specify whether or not to require check-in and check-out for each document library listed. |

## Worksheet

Use the following worksheet to help you plan versioning, content approval, and check-outs:

 [Document libraries worksheet](http://go.microsoft.com/fwlink/?LinkID=73306&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73306&clcid=0x409)

## [[17]](#footnote-18)#See Also

[Plan document libraries](#DSDOC_33b67ac7_54c3_42d8_87cd_5d7a00f729)

# Plan Information Rights Management

In this article:

 [Information Rights Management in Office SharePoint Server 2007](#DSDOC_section1073bfc71_7b01_4b77_bdc3_ac)

 [Worksheet](#DSDOC_section2073bfc71_7b01_4b77_bdc3_ac)

Information Rights Management (IRM) enables content creators to control and protect their documents. The contents of rights-managed documents are encrypted and supplied with an issuance license that imposes restrictions on users. These restrictions vary depending on the level of users' permissions. Typical restrictions include making a document read-only, disabling copying of text, not allowing users to save a copy of the document, or preventing users from printing the document. Client applications that read IRM-supported file types use the issuance license inside an IRM-managed document to enforce the restrictions on users who access the document.

## Information Rights Management in Office SharePoint Server 2007

Microsoft Office SharePoint Server 2007 supports using IRM on documents stored in document libraries. Documents that can be rights-managed in Office SharePoint Server 2007 include Microsoft InfoPath forms, Microsoft Word, Microsoft Excel, and Microsoft PowerPoint file formats, in addition to Word, Excel, and PowerPoint Open XML file formats. To add other file types, an administrator must install protectors — programs that control the encryption and decryption of rights-managed documents — for each new type of file.

By using IRM in Office SharePoint Server 2007, you can centrally control which actions users can take on documents when they open them from libraries in Office SharePoint Server 2007. This is in contrast to IRM applied to documents stored on client computers, where the owner of a document can choose which rights to assign to each user of the document. Use IRM on document libraries to control sensitive content that is stored on the server. For example, if you are making a document library available to preview upcoming products to other teams within your enterprise, you could use IRM to prevent the teams from publishing the content to audiences outside your organization.

When IRM is enabled on a document library and a document of a type that can be rights-managed is downloaded from the server to a client application, Office SharePoint Server 2007 encrypts the document and adds an issuance license. When the document is uploaded back to the server, Office SharePoint Server 2007 decrypts the file and stores it in the library in unencrypted form. By only encrypting documents when they are downloaded and decrypting them when they are uploaded, Office SharePoint Server 2007 enables features such as search and indexing to operate as usual on the files in the IRM-protected document library. The IRM permissions that are applied to a document when users upload it from a document library are based upon each user's permissions to the content in the Office SharePoint Server 2007 security settings. The following table describes how Office SharePoint Server 2007 permissions are converted to IRM permissions:

|  |  |
| --- | --- |
| Office SharePoint Server 2007 permissions | IRM permissions |
| Manage Permissions, Manage Web | Full control, as defined by the client. This generally allows a user to read, edit, copy, save, and modify the permissions of rights-managed content. |
| Edit List Items, Manage List, Add and Customize Pages | Edit, copy, and save permissions. You can optionally enable users with these permissions to print documents from the document library. |
| View List Item | Read permissions. A user can read the document, but cannot copy or update its content. You can optionally enable users with view list item permissions to print documents from the document library. |
| Other | No other permissions map to IRM permissions. |

To use IRM in Office SharePoint Server 2007, you must install the Microsoft Windows Rights Management Services Client, version 1, on every front-end Web server in your server farm. In addition, Microsoft Windows Rights Management Services (RMS) for Windows Server 2003, service pack 1.0 or later, must be available on your network. To install the Windows Rights Management Services Client, and for additional information about Microsoft Windows Rights Management Services, visit the [Windows Rights Management Services Technology Center](http://go.microsoft.com/fwlink/?LinkId=73121) (http://go.microsoft.com/fwlink/?LinkId=73121). For a description of the steps needed to configure Microsoft Windows Rights Management Services to allow Office SharePoint Server 2007 to create rights-managed content, see Deployment for Office SharePoint Server 2007.

## Worksheet

For each document library, specify whether or not to require IRM and, if protectors for additional document types are required, note that information in the Require Information Rights Management column. Use the following worksheet to record the information:

 [Document libraries worksheet](http://go.microsoft.com/fwlink/?LinkId=73306&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73306&clcid=0x409)

# Plan information management policies

In this article:

 [About information management policies and policy features](#DSDOC_section14de4007d_a45f_419d_9512_82)

 [About information management policy reporting](#DSDOC_section24de4007d_a45f_419d_9512_82)

 [About information management policy integration with the 2007 Office system applications](#DSDOC_section34de4007d_a45f_419d_9512_82)

 [Policy features available in Office SharePoint Server 2007](#DSDOC_section44de4007d_a45f_419d_9512_82)

 [Plan information management policies](#DSDOC_section54de4007d_a45f_419d_9512_82)

## About information management policies and policy features

An information management policy is a set of rules for a type of content. Each rule in a policy is a policy feature. For example, an Information Management policy feature could specify how long a type of content should be retained, or it could provide document auditing. Information management policies enable you to control who can access your organizational information, what they can do with it, and how long the information should be retained.

note_ddNote:

In this topic, the term "policy" refers to information management policy unless otherwise specified.

Policies can be implemented to help an organization comply with legally mandated requirements, such as the need to retain records. For example, a Human Resources policy, used in an organization to ensure that employee records are handled in accordance with legally recommended guidelines, could include the following policy features:

 Auditing, to record the editing and viewing history of each employee-related document.

 Retention, to ensure that work-in-progress content is not kept for an unnecessarily long period of time.

 Labels, to ensure that physical copies of each document are properly identifiable.

 Print Restrictions, to ensure that sensitive employee-related documents are only printed on secure printers. Note that this is an example of a custom policy that must be implemented using the Office SharePoint Server 2007 object model or acquired from a 3rd-party software vendor.

Policy features are implemented as programs that run on the Office SharePoint Server 2007. They can be enabled and configured by a server administrator and, once enabled, they can be used by site administrators to define policies. Office SharePoint Server 2007 includes five policy features to help you manage your content. By using the Office SharePoint Server 2007 object model, you can design and install custom policy features that meet unique enterprise needs.

A policy feature may use one or more policy resources, which are programs that provide some functionality to a policy feature. For example, a policy resource for a Barcode Generation policy feature could provide the unique barcode value. You can develop custom policy resources and install them to support policy features.

When your organization uses 2007 Microsoft Office system client applications along with Office SharePoint Server 2007, policies are enforced both on the server and in the client applications. This is done transparently; policy features that apply to a document are described in a policy statement associated with the document, and policy-aware applications prevent users from doing tasks that violate the document's policy.

To implement a policy, associate it with content types, libraries, or lists in sites.

note_ddNote:

In the Site Content Type Gallery, you can apply a policy to any custom content type, but you cannot apply a policy directly to a core content type.

You can associate a policy with a library, list, or content type in the following ways:

 Associate policy features with a site collection policy, and then associate that policy with a content type or with a list or library.   The top-level site of a site collection includes a Site Collection Policies gallery where administrators of the top-level site can create new policies. After creating a Site Collection policy, you can export it so that administrators of other site collections can import it into their Site Collection Policy galleries. This enables you to standardize policies across your organization.

When a Site Collection policy is associated with a content type and that content type is associated with a list or library, the owner of the list or library will not be able to modify the Site Collection policy in the list or library. This ensures that policies assigned to a content type are enforced at each level of the site hierarchy.

 Associate a set of policy features directly with a content type, and then add that content type to one or more lists or libraries.   To ensure that a policy created using this method will be used in an entire site collection, associate it with a content type in the top-level site collection's Site Content Type gallery. Then every item in the site collection of that content type, and every item of a content type that inherits from the original content type, will have the policy. When you use this method of associating a policy with a content type, it is harder to reuse the policy in other site collections, because policies created using this method cannot be exported.

note_ddNote:

To more tightly control which policies are in use in a site collection, site collection administrators can disable the ability to set policy features directly on a content type. When setting policy features on a content type is restricted, content type designers can only associate policies from the Site Collection Policies gallery with content types.

 Associate a set of policy features directly with a list or library.   You can only use this method if the list or library does not support multiple content types. This method of creating a policy is only useful for a narrowly defined policy that applies to a single list or library.

note_ddNote:

To more tightly control which policies are in use in a site collection, site collection administrators can disable the ability to set policy features directly on a library. When setting policy features on a library is restricted, content type designers can only associate policies from the Site Collection Policies gallery with libraries.

## About information management policy reporting

To track how policies are being used in each Web application in your solution, you can configure information management policy usage reporting using Microsoft Office SharePoint Server 2007 Central Administration. Information management policy reports help you monitor how well your organization uses policies. Because policies are often implemented to help an organization comply with particular regulations, frequent monitoring of policy usage can help you ensure that your organization is compliant.

Office SharePoint Server 2007 includes a default policy report template in XML-SS format, and you can create a custom report template based on the XML-SS schema. You can specify a schedule for policy reporting and you can generate reports manually.

A policy report is generated for each site collection in a Web application. For each list and library, a report records:

 The number of items using each policy.

 For each policy in use, either based on a Site Collection policy or configured in a content type, a summary of that policy — its description, along with a description of each policy feature.

For more information about creating and deploying a custom Site Collection policy report, see the Deployment for Office SharePoint Server 2007 guide.

## About information management policy integration with the 2007 Office system applications

Office SharePoint Server 2007 information management policies are exposed in 2007 Office release clients. When you configure an information management policy on the server, you can write a policy statement that informs information workers about the policies that are enforced on documents. For example, the policy statement might indicate that a document will expire after a certain period of time, or that it is sensitive information that should not be communicated outside the company. The statement might even provide a contact name if the information worker needs more information about the policy.

The policies that are included in Office SharePoint Server 2007 are exposed to information workers through 2007 Office release client features. For example, when a label is defined as part of a policy, users can insert labels into documents from the Insert menu of most 2007 Office release client applications. If a label is required, users are prompted when saving documents in which a label has not been inserted. Similarly, users will be able to insert barcodes from client applications if that policy feature is part of the document's policy.

Custom policy features can also be integrated in 2007 Office release clients. However, you must implement policy-specific behaviors that you want to be available from 2007 Office release client programs, and you must give users a way to install these behaviors on their client computers via mechanisms such as add-ins to make them available from 2007 Office release client programs. For example, if you implement a custom policy feature that restricts the printers that can be used to print a content type, you must provide a custom add-in for Microsoft Office clients to enforce the restriction from Office client applications.

## Policy features available in Office SharePoint Server 2007

This section describes the five policy features that are included in Office SharePoint Server 2007.

 Expiration   The Expiration policy feature helps dispose of content in a consistent way that can be tracked and managed. You can set content of a specific type to expire on a particular date, or within a calculated amount of time after some document activity (such as creating the document).

 Auditing   The Auditing policy feature logs events and operations performed on documents and list items. You can configure Auditing to log events such as:

 Editing a document or item

 Viewing a document or item

 Checking a document in or out

 Changing the permissions for a document or item

 Deleting a document or item

 Labeling   The Labeling policy feature specifies a label to associate with a type of document or list item. Labels are searchable text areas that Office SharePoint Server 2007 generates based on properties and formatting that you specify. For example, in a law firm, a document related to a legal matter could include a label containing the clients' names, the case number, the attorney assigned to the matter, and so forth. Labels are particularly useful in printed versions of documents as a way to display document properties in printed copy. Along with using labels for documents, you can associate a label with a list item and include that label in views of the list.

 Barcode   The Barcode policy feature enables you to track a document in physical copies by creating a unique identifier value for a document and inserting a barcode image of that value in the document. By default, barcodes are compliant with the common Code 39 standard (ANSI/AIM BC1-1995, Code 39), and you can plug in other barcode providers using the policies object model.

 Form Conversion for Archiving   The Form Conversion for Archiving policy feature generates an image of a completed form, which can later be archived. When you associate Form Conversion for Archiving with a form library, an image is initially generated for each form in the library, and an image is generated each time a new form is added to the library or an existing form is modified.

## Plan information management policies

When planning your solution's policies, first determine organization-wide policy needs, and then design Site Collection policies to meet those needs and distribute those policies for inclusion in all relevant site collections' Site Collection Policy galleries. This might require planning custom policy features. Note that, if your policy requires custom policy features and resources, those features and resources must be installed and enabled on all server farms on which your solution is used. See the Deployment for Office SharePoint Server 2007 guide for more information about deploying and enabling Office SharePoint Server 2007 features and resources.

A typical example of an organization-wide policy is one designed to promote best practices in auditing and expiring product specifications across the divisions of an organization. A single Site Collection policy is designed to be applied to all product specifications so that they are consistently audited and retained. After defining the Site Collection policy and testing it, it is exported and then imported to Site Collection Policy galleries of other site collections in which product specifications are stored. It is then associated with all product specification content types in the various site collections to impose the policy on all product specification documents.

|  |
| --- |
| Worksheet action |
| To help you plan information management policies, use the [Policy worksheet](http://go.microsoft.com/fwlink/?LinkId=73307&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73307&clcid=0x409). Create a separate worksheet for each policy you are planning, and in each worksheet record:   The purpose of the policy, such as "Policy to apply to all product specifications."   The site collection in which the policy is being designed.   The scope at which the policy is being defined. If the policy is to be used across multiple site collections, define it in the Policy Template gallery. Define a policy for a content type if the policy is more narrowly targeted to a single content type in a site collection.   Each policy feature, such as "Expiration" or "Auditing." Optionally enter configuration notes for a policy feature. For example, for Auditing, you could specify which actions to audit, such as "Editing Items." If the feature is custom, list all resources that must be installed for the feature to work.   All content types that the policy will be applied to and list all site collections in which the content types are in use. |

## Worksheet

Use the following worksheet with this article to help plan your deployment:

 [Policy worksheet](http://go.microsoft.com/fwlink/?LinkId=73307&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73307&clcid=0x409))

# Plan enterprise content storage

This article contains information to help solution planners and designers properly plan and configure a large-scale enterprise content management solution based on Microsoft Office SharePoint Server 2007 so that it performs well while providing the features needed by site users. Office SharePoint Server 2007 supports high-capacity document storage; a document library can contain up to 5 million documents. However, depending on how the content is used, the performance of sites containing a very large number of documents can degrade. The prescriptive guidance provided in this article can help you design large-scale content management solutions that scale to the requirements of your enterprise while providing the users of your solution with a well-performing environment in which to create and use documents.

Decisions you make about the capacities of site collections, sites, and libraries in Office SharePoint Server 2007 should take into account not only the physical storage constraints of your Office SharePoint Server 2007 environment but also the content usage and viewing patterns of your users. For example, if users view or query a set of documents in a document library containing thousands of documents, performance can degrade if the site is not configured properly. Or if a service-level agreement requires that content be backed up twice a day, the service might not be satisfactorily performed if the set of content is too large. This article discusses techniques you can use to provide necessary content management functionality while maintaining acceptable performance.

In this topic, four levels of content storage are discussed:

 Site collection

 Site

 Library

 Folder

For each level of storage, this article describes the benefits of organizing content at that level, discusses how performance can decrease as the number of stored documents increases, and provides recommendations for improving performance when high volumes of content are present.

In this article:

 [Typical large-scale content management scenarios](#DSDOC_section19994b57f_fef8_44e7_9bf9_ca)

 [Site collections: content storage benefits and limitations](#DSDOC_section29994b57f_fef8_44e7_9bf9_ca)

 [Sites: content storage benefits and limitations](#DSDOC_section39994b57f_fef8_44e7_9bf9_ca)

 [Libraries: content storage benefits and limitations](#DSDOC_section49994b57f_fef8_44e7_9bf9_ca)

 [Folders: content storage benefits and considerations](#DSDOC_section59994b57f_fef8_44e7_9bf9_ca)

 [Summary of recommendations](#DSDOC_section69994b57f_fef8_44e7_9bf9_ca)

note_ddNote:

Although the examples in this article are primarily relevant for solutions based on Office SharePoint Server 2007, the prescriptive guidance information provided here applies to both Office SharePoint Server 2007 and Microsoft Windows SharePoint Services 3.0.

## Typical large-scale content management scenarios

Typically, large-scale content management scenarios are variants of one of the following scenarios:

 Large-scale authoring environment

 Large-scale content archive

 Extremely large-scale content archive

The scenario descriptions provided here are intended to clarify what we mean by large-scale solutions and to provide examples that hopefully reflect your content management goals.

### Large-scale authoring environment

In a large-scale authoring environment, a site can contain a library in which users actively edit 50,000 or more documents across 500 or more folders. Versioning is enabled, and typically 10 or more previous versions of each document exist. Documents are checked in and out frequently and workflows are used to control their life cycles. Twenty or more content types might be in use. A typical database for this type of site contains approximately 150 gigabytes (GB) of data. (Note that each version of a document is stored separately in the database.) Typically, in a large-scale authoring environment, 80% of site users are authors who have access to major and minor versions of documents, while 20% of site users have read-only permissions and can only view major versions of the content.

A large-scale authoring environment site can be based on the Office SharePoint Server 2007 Document Center site template, which includes a single, large document library and which is optimized for large-scale authoring. See [The Document Center site](#DSDOC_section89994b57f_fef8_44e7_9bf9_ca).

### Large-scale content archive

A large-scale archive is a document repository in which users are either viewing documents or uploading new documents. Little or no authoring takes place in the site. There are two primary large-scale archive scenarios: knowledge base and records management.

In a knowledge base site, there is only a single version of most documents, so the site can scale to easily hold 1,000,000 or more documents. The content is typically stored in a single database as large as 400 GB. In a typical scenario, such as an enterprise's technical support center, 10,000 users might access the content, primarily to read it. A subset of users (3,000–4,000) uploads new content to the site. A knowledge base site can be based on the Document Center site template.

Another type of large-scale archive is a records center, based on the Records Center site template. This site template contains features that you can use to manage the retention and disposition of records (documents that serve as evidence of activities or transactions performed by the organization and that must be retained for some time period). Similar to a knowledge base site, a records center contains a single version of each document and could typically hold 1,000,000 or more documents. Many more users submit content to a records center than view or read it.

### Extremely large-scale content archive

If the user interface of a site is customized to remove resource-intensive user interface operations such as complex viewing queries, an extremely large-scale content archive can be used as a reference library or content repository. An extremely large-scale archive might contain up to 10,000,000 documents distributed across 5,000 or more folders. The database can grow larger than three terabytes (TB).

In an extremely large-scale archive, users (50,000 or more) primarily browse content by searching. Content is submitted by using a custom submission form.

## Site collections: content storage benefits and limitations

A site collection is a set of Web sites that has the same owner and shares administration settings. Each site collection contains a top-level Web site and can contain one or more subsites. A site collection usually has a shared navigation structure.

### Benefits of storing content in the same site collection

The sites in a site collection are usually interrelated by purpose. To maximize your solution's usability, store all related data and content within a single site collection. Benefits of doing this include:

 Content types and columns managed in a site collection can be shared across all sites in the site collection. Conversely, there is no automatic mechanism for propagating content types and column definitions across multiple site collections.

 Information management policies managed in the site collection can be made available to content in all sites in the site collection.

 Office SharePoint Server 2007 automatically updates links to renamed or moved files within a site collection to reflect their new names or locations. Conversely, links to documents in other site collections are not updated.

 If the site collection is on a server running Windows SharePoint Services 3.0, searching can only be done over the content in that site collection. If the site collection is on a server running Office SharePoint Server 2007, content can be searched across multiple site collections.

 Some views in Windows SharePoint Services 3.0 and Office SharePoint Server 2007 list documents from multiple sites within a single site collection (for example, a view enumerating all tasks assigned to a user across a site collection). Also, developers can create cross-site database queries within a site collection, but cross-site queries are not supported across multiple site collections.

 Content quotas and other quotas can only be managed at the site-collection level.

### Limits on storing content in the same site collection

Keep the following limits in mind when planning how to allocate your content across one or more site collections:

 Creating too many subsites of any site in a site collection might affect performance and usability. Limit the number of subsites of any site to 2,000 at most.

 All sites in a site collection share the same back-end resources. In particular, all content in a site collection must be stored in the same content database. Because of this, the performance of database operations — such as backing up and restoring content — will depend on the amount of content across the entire site collection, the size of the database, the speed of the servers hosting the database, and other factors. Depending on the amount of content and the configuration of the database, you might need to segment a site collection into multiple site collections to meet service-level agreements for backing up and restoring, throughput, or other requirements. It is beyond the scope of this article to provide prescriptive guidance about managing the size and performance of databases. For more information about capacity planning, see [Chapter overview: Plan for performance and capacity (Office SharePoint Server)](#DSDOC_8dd52916_f77d_4444_b593_1f7d6f330e).

 Particularly, keep extremely active sites in separate site collections. For example, a knowledge base site on the Internet that allows anonymous browsing could generate a lot of database activity. If other sites use the same database, their performance could be impacted. By putting the knowledge base site in a separate site collection with its own database, you can free up resources for other sites that no longer have to compete with it for database resources.

Note that Windows SharePoint Services 3.0 and Office SharePoint Server 2007 have a number of features that mitigate the need to have your IT department restore content. The Recycle Bin and the Site Collection Recycle Bin provide a double safety mechanism for restoring inadvertently deleted items. Document versioning also provides a safety net for lost documents because their previous versions are available. To further ensure the availability of previous versions, an administrator can remove the delete versions permission from authors' permissions; this can help to guarantee that previous versions of content are available without having to restore them from the database.

## Sites: content storage benefits and limitations

A Web site is the primary means of organizing related content in Office SharePoint Server 2007 and Windows SharePoint Services 3.0.

### Benefits of storing content in the same site

 It is easier to create pages that display views of multiple libraries and lists when they are in the same site.

 The site navigation user interface is optimized to make it easy to find and navigate to libraries within the same site.

 You define and assign permissions to groups at the site level.

 You can define a set of content types and site columns for use in a site.

### The Document Center site

Office SharePoint Server 2007 includes a Document Center site template. Use this template to create a site that is optimized for creating and using large numbers of documents.

To enable document management best practices, sites based on the Document Center site template have recommended document management features enabled by default, including:

 Navigation features to help authors find their content.

 Major/minor versioning enabled.

 Required check-in and check-out of documents.

 Multiple content types enabled.

 A Relevant Documents Web Part that generates a personalized view of documents checked out by, created by, or last modified by the current user. You can configure the Web Part to use more than one criterion.

 An Upcoming Tasks Web Part that generates a personalized view of document-related tasks assigned to the current user.

Column indexing is a technique that helps ensure that a view or query returns a list of items in the recommended range of 2,000 or fewer items. Use the following table to determine the right columns to index for each query that the Relevant Documents Web Part supports:

|  |  |
| --- | --- |
| If you configure the Relevant Documents Web Part to… | Then, in the Shared Documents library, index the following column: |
| Include documents last modified by me | Modified By |
| Include documents created by me | Created By |
| Include documents checked out by me | Checked Out By |

Along with indexing columns to improve the performance of the Relevant Documents Web Part, make sure that the Show items from the entire site collection checkbox is not selected when configuring the Web Part in a large-scale document management environment.

### Limits on storing content in the same site

 More than 2,000 libraries and lists in a single site will degrade performance.

 Usability tests show that having more than 50 lists and libraries in the site's navigation structure makes it more difficult to navigate the content by using the user interface.

## Libraries: content storage benefits and limitations

A document library is a location in a site containing files of one or more content types. Document libraries are designed to manage and store related documents and to let users create new documents of the appropriate types.

### Benefits of storing content in the same library

 It is easier for users to add new documents or find existing documents within a single library.

 Many document management settings — such as permissions, content versioning, and approval — are applied at the library level.

 Views created by using the user interface are bound to a particular library.

 Information management policies, such as content auditing and retention settings, can be applied to a library.

### Limits on storing content in the same library

 The maximum recommended size of a library is 10,000,000 documents.

 To apply unique document management settings to content, such as required checkouts or versioning, the content must be stored in a separate library.

 If multiple content types are used in a library and each content type has one or more columns of metadata that only apply to that content type, views can become confusing. To alleviate this, you can associate each content type with a separate library.

 The performance of views of content degrades when the number of items viewed exceeds 2,000 items. Remedies for this limitation are to organize the content in the library into folders each containing 2,000 or fewer items, or to create views that take advantage of indexed columns to return sets of 2,000 or fewer items (see below for a discussion of using indexed columns in views).

note_ddNote:

All Web page content in a site is stored in a single Pages library in that site, which contains all of that site's Web content pages. The recommended limitation of 2,000 or fewer items per view or query applies to Pages libraries in addition to document libraries.

### Using indexed columns to improve view performance

As mentioned above, the performance of views degrades if the number of items displayed exceeds 2,000 items. A useful technique for limiting the number of items to display in a view is to index a column used in the view, and then to filter the view based on that column so that 2,000 or fewer items are displayed. (An indexed column is one that Office SharePoint Server 2007 maintains a record of to make view-related queries more efficient.)

For example, if it is unlikely that more than 2,000 items in a library will be modified in any seven-day period, you could index the Modified column in a library and then filter a view so that only items changed in the last seven days are displayed. (To do this, specify that the Modified column is less than Today-7.) As another example, if it is likely that each author will create less than 2,000 items, you could index the Created By column and then filter a view so that authors only see the documents they created. (To do this, specify that the Created By column is equal to Me.)

The following types of column types can be indexed and used to filter views:

 Single line of text

 Multiple lines of text

 Number

 Currency

 Choice

 Date and Time

 Lookup

 Yes/No

 Person or Group

 Calculated

Here are other considerations in creating views filtered by indexed columns:

 Only one indexed column can be used in a view.

 Do not create filters using "Or" to provide multiple criteria when using an indexed column to filter a view.

 Using the Item Limit feature to modify a view does not improve the view's performance.

note_ddNote:

If a user tries to create a view that could benefit from using an indexed column, Office SharePoint Server 2007 will display a warning message recommending that approach.

## Folders: content storage benefits and considerations

A folder is a named subdivision of the content in a library similar to folders in a file system. The primary purpose of folders is to organize content to match the expected functionality of the library. For example, if a library is intended to provide product specifications, the set of folders in the library could be named for each feature area in the product or for each team member who writes product specifications.

Folders can be used to enhance library performance. By dividing content across multiple folders, each containing 2,000 or fewer items, views on the folders will perform well. Note that, to take advantage of this, views available within folders must be configured to only show items inside the folders (this feature is available in the default Office SharePoint Server 2007 view-creation interface). Note also that, if folders contain 2,000 or fewer items, views in the folders do not have to be filtered using indexed columns.

## Summary of recommendations

Here is a summary of the recommendations for improving performance at each level of storage when high volumes of content are being stored:

|  |  |
| --- | --- |
| Level | Performance limits |
| Site collection | 2,000 subsites of any site is the recommended limit.  The same content database is used for an entire site collection. This may affect performance in operations such as backup and restore. |
| Site | 2,000 libraries and lists is the recommended limit. |
| Library | 10,000,000 documents is the recommended limit.  2,000 items per view is the recommended limit. |
| Folder | 2,000 items per folder is the recommended limit. |

## [[18]](#footnote-19)#See Also

[Chapter overview: Plan for performance and capacity (Office SharePoint Server)](#DSDOC_8dd52916_f77d_4444_b593_1f7d6f330e)

[Chapter overview: Plan records management](#DSDOC_271017e8_7f23_4166_9501_140ad2fc55)

# X Plan records management

In this chapter:

 [Chapter overview: Plan records management](#DSDOC_271017e8_7f23_4166_9501_140ad2fc55)

 [What is records management?](#DSDOC_1b4765ef_3d28_4082_bb37_5d84e9996c)

 [Identify records management roles (Office SharePoint Server 2007)](#DSDOC_41ee29a8_be9b_4632_adbf_9bc8205809)

 [Develop the file plan (Office SharePoint Server 2007)](#DSDOC_037fb582_6448_4baf_85d4_6e6221f216)

 [Design the Records Center site (Office SharePoint Server 2007)](#DSDOC_03702c06_3e32_409d_ad8c_7e84eae386)

 [Plan how records are collected (Office SharePoint Server 2007)](#DSDOC_f3fae102_5b20_4c9f_9707_ab76c68be9)

 Plan how to retain physical records

 Plan how to retain e-mail messages

# Chapter overview: Plan records management

Microsoft Office SharePoint Server 2007 includes records management features you can use to help your organization meet its regulatory and legal requirements and manage its corporate knowledge.

The articles in this chapter include:

 [What is records management?](#DSDOC_1b4765ef_3d28_4082_bb37_5d84e9996c) reviews the elements of a records management system and provides an overview of records management planning.

 [Identify records management roles (Office SharePoint Server 2007)](#DSDOC_41ee29a8_be9b_4632_adbf_9bc8205809) helps you identify members of your organization with the range of records management–related roles and skills to support planning and implementing a records management solution based on Office SharePoint Server 2007.

 [Develop the file plan (Office SharePoint Server 2007)](#DSDOC_037fb582_6448_4baf_85d4_6e6221f216) provides guidance on determining the types of records in your organization and on creating a file plan to specify retention periods, disposition plans, and other information for each record type.

 [Design the Records Center site (Office SharePoint Server 2007)](#DSDOC_03702c06_3e32_409d_ad8c_7e84eae386) describes how to plan the document libraries, metadata, policies, and other features of a Records Center site, the Office SharePoint Server 2007 site you use to implement your file plan and manage records.

 [Plan how records are collected (Office SharePoint Server 2007)](#DSDOC_f3fae102_5b20_4c9f_9707_ab76c68be9) helps you plan how electronic and hard-copy records in your organization should move to the Records Center site.

## See Also

[Chapter overview: Plan document management](#DSDOC_cb57d4f7_8353_420b_8a10_d05c9bdf1b)

# What is records management?

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [Elements of a records management system](#DSDOC_section11b4765ef_3d28_4082_bb37_5d)

 [Overview of records management planning](#DSDOC_section21b4765ef_3d28_4082_bb37_5d)

## Elements of a records management system

A record is a document or other electronic or physical entity in an organization that serves as evidence of an activity or transaction performed by the organization and that requires retention for some time period. Records management is the process by which an organization:

 Determines what types of information should be considered records.

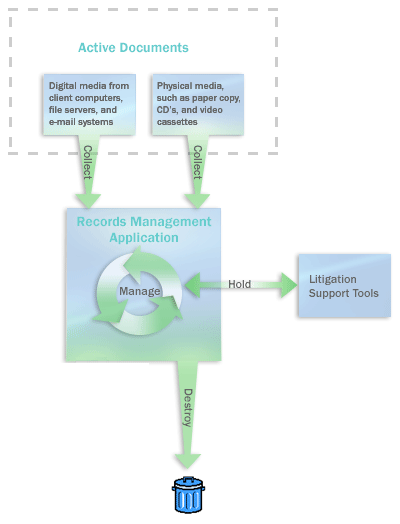
 Determines how active documents that will become records should be handled while they are in use, and determines how they should be collected once they are declared to be records.

 Determines in what manner and for how long each record type should be retained to meet legal, business, or regulatory requirements.

 Researches and implements technological solutions and business processes to help ensure that the organization complies with its records management obligations in a cost-effective and non-intrusive way.

 Performs records-related tasks such as disposing of expired records, or locating and protecting records related to external events such as lawsuits.

Determining which documents and other physical or electronic items in your organization are records is the responsibility of corporate compliance officers, records managers, and lawyers. By carefully categorizing all enterprise content in your organization, they can help you ensure that documents are retained for the appropriate period of time. A well-designed records management system helps protect an organization legally, helps the organization demonstrate compliance with regulatory obligations, and increases organizational efficiency by promoting the disposition of out-of-date items that are not records.



A records management system includes the following elements:

 A content analysis that describes and categorizes content in the enterprise that may become records, provides source locations, and describes how the content will move to the records management application.

 A file plan describing, for each type of record in the enterprise, where they should be retained as records, the policies that apply to them, how they need to be retained, how they should be disposed of, and who is responsible for managing them.

 A compliance requirements document defining the rules that the organization's IT systems must adhere to in order to ensure compliance, along with the methods used to ensure the participation of enterprise team members.

 A method for collecting records that are no longer active from all record sources, such as collaboration servers, file servers, and e-mail systems.

 A method for auditing records while they are active.

 A method for capturing records' metadata and audit histories and retaining them.

 A process for holding records (suspending their disposition) when events such as litigations occur.

 A system for monitoring and reporting on the handling of records to ensure that employees are filing, accessing, and managing them according to defined policies and processes.

Microsoft Office SharePoint Server 2007 includes features that can help organizations implement integrated records management systems and processes. To ensure that information workers can easily participate in your enterprise's records management system, 2007 Microsoft Office system applications, such as Microsoft Office Outlook 2007 and Microsoft Office Word 2007, also include features that support records management practices.

## Overview of records management planning

This topic describes the planning steps you should take to help ensure that the records management system you implement based on Office SharePoint Server 2007 will achieve your organization's records management goals. Here is a preview of the records management planning process:

1. Identify records management roles   Successful records management requires specialized roles, including:

 Records managers and compliance officers to categorize the records in the organization and to run the records management process.

 IT personnel to implement the systems that efficiently support records management.

 Content managers to identify where organizational information is kept and to commit their teams to following records management practices.

2. Analyze organizational content   Before creating a file plan, records managers and content managers survey document usage in the organization to determine which documents and other items may become records.

3. Develop a file plan   After you have analyzed your organizational content and determined retention schedules, fill in the rest of the file plan. File plans differ from organization to organization, but in general they describe the kinds of items the enterprise acknowledges to be records, indicate where they are stored, describe their retention periods, and provide other information such as who is responsible for managing them and what broader category of records they belong to.

4. Develop retention schedules   For each record type, determine when it is no longer active (in use), how long it should be retained after that, and how it should ultimately be disposed of.

5. Evaluate and improve document management practices   Make sure that proper policies are being applied in document repositories. For example, ensure that content is being properly audited, so that adequate audits are retained along with records.

6. Design the records management application   Office SharePoint Server 2007 includes a specialized site template, the Records Repository, which is designed for records management. Based on your file plan, design the site's libraries, content types, policies, and its record series, which defines where in the site record that type should be stored.

7. Plan how content moves to the Records Center site   If you are using Office SharePoint Server 2007 for both your active document management and your records management application, you can create custom workflows to move documents to the Records Repository at the appropriate times. If you are using either Office SharePoint Server 2007 or external document management systems, you can plan and develop interfaces that move content from those systems to the Records Repository, based on the Records Repository's programmable interface.

8. Plan Microsoft Exchange integration   Microsoft Exchange Server "12", along with Office Outlook 2007, includes features designed to facilitate the flow of e-mail into the Records Repository using specialized folders and commands. If you are using Exchange Server "12" as your e-mail server, you can plan how to classify e-mail and move it to the Records Repository.

9. Plan compliance reporting and documentation   To verify that your organization is performing its required records management practices and to communicate these practices, you should document your records management plans and processes. If your enterprise becomes engaged in records-related litigation, you may be required to produce these records management guidelines, implementation plans, and metrics on effectiveness.

## [[19]](#footnote-20)#See Also

[Identify records management roles (Office SharePoint Server 2007)](#DSDOC_41ee29a8_be9b_4632_adbf_9bc8205809)

[Develop the file plan (Office SharePoint Server 2007)](#DSDOC_037fb582_6448_4baf_85d4_6e6221f216)

[Design the Records Center site (Office SharePoint Server 2007)](#DSDOC_03702c06_3e32_409d_ad8c_7e84eae386)

[Plan how records are collected (Office SharePoint Server 2007)](#DSDOC_f3fae102_5b20_4c9f_9707_ab76c68be9)

# Identify records management roles (Office SharePoint Server 2007)

Effective records management requires an organization-wide commitment to planning, implementing, overseeing, and participating in the records management program. To achieve this, members of your organization with a range of records management–related roles and skills must support the effort. As you start planning your records management solution, identify who in your organization will fill the following roles:

 Records managers   Usually members of an organization's legal department. They are skilled in the process of categorizing electronic and physical documents and in deciding which documents should become records. Records managers help determine organizational records management policies and participate in designing the records management solution. They are responsible for researching and writing the file plan and retention schedule, and they participate in writing the compliance requirements document. Records managers also operate the records management system, performing tasks such as putting records on hold during litigation and disposing of records at the end of their retention periods. The participation of records managers is essential to the success of your records management system.

 Compliance officers   Also members of an organization's legal department. In some organizations, this role is filled by records managers. Compliance officers monitor every aspect of enterprise records management to ensure that the organization is closely following relevant regulations and guidelines. They are primarily responsible for writing the compliance requirements document, which describes the enterprise records management methodology, guidelines, and training plans.

 IT professionals   Responsible for deploying, operating, and maintaining the computers and applications that implement the records management solution. They ensure that the records management solution is secure, that it is of the proper scale, that it is reliable, and that it communicates with the document management servers and e-mail servers that supply it with records.

 Site designers   In a records management solution based on Microsoft Office SharePoint Server 2007, they are the experts in creating and configuring Web sites implementing a Records Center site.

 Content managers   Manage teams that produce documents or that handle physical or electronic files that might be records. Their role is to supply leadership in identifying records, in planning processes for their teams that will ensure good records management practices, and in making sure that the information workers on their teams participate in the organizational records management effort.

 Information workers   The participants in the records management system. They create or manage the electronic and hard-copy documents, memos, reports, messages, and other content that could be records. The success of your records management solution depends on the quality of participation by the information workers in your organization.

note_ddNote:

How you design your records management system can have a big impact on how well information workers comply with it. For example, by creating simple processes for retaining records, you will increase participation because information workers will be less likely to see these tasks as impediments to getting their other work done. Also, effective records management training and documentation will increase information workers' active participation.

Your organization might have already filled all of the roles described in this article. If not, you might want to seek experts in records management and compliance. Professional organizations such as the Association of Records Managers and Administrators can be helpful in locating records management professionals in your area.

The initial tasks of the team designing your records management system include analyzing content usage in your organization, analyzing regulatory and other requirements that will affect records management decisions, evaluating hardware and application resources to use to retain records, and planning the best strategy for ensuring information workers' cooperation in managing records. Because this planning touches on so many disciplines in your organization, form a diverse team to plan your records management solution, including all the roles described above.

|  |
| --- |
| Worksheet action |
| Use the [Records management stakeholders and participants worksheet](http://go.microsoft.com/fwlink/?LinkId=73296&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73296&clcid=0x409) to record the name, e-mail address, role, and other contact information for each participant you enlist for the records management planning team. |

## Worksheet

Use the following worksheet to help plan your deployment:

 [Records management stakeholders and participants worksheet](http://go.microsoft.com/fwlink/?LinkId=73296&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73296&clcid=0x409)

# Develop the file plan (Office SharePoint Server 2007)

In this article:

 [About records, active documents, and archived documents](#DSDOC_section1037fb582_6448_4baf_85d4_6e)

 [Determine what is a record](#DSDOC_section2037fb582_6448_4baf_85d4_6e)

 [Complete the file plan](#DSDOC_section3037fb582_6448_4baf_85d4_6e)

The file plan is the primary records management planning document. Although file plans can differ across organizations, they typically:

 Describe the kinds of items the organization acknowledges to be records.

 Describe what broader category of records the items belong to.

 Indicate where records are stored.

 Describe retention periods for records.

 Delineate who is responsible for managing the various types of records.

## About records, active documents, and archived documents

Before you can determine your file plan, you need to understand the differences among records, active documents, and archived documents.

 Records   These are documents or other physical or electronic entities in an organization that serve as evidence of activities or transactions performed by the organization. They must be retained for some time period so they can be produced if needed, such as for regulatory or legal discovery.

When an active document is declared to be a record, it is moved or copied to a protected place such as a physical vault or an electronic records repository, and it is assigned a retention period that specifies how long the organization will keep it. (Note that the retention period could be permanent, meaning that the record would be retained indefinitely.) When a record's retention period is over, it is either disposed of by a records manager or moved to an archive for safekeeping as a document of historical interest.

 Active documents   These are documents in use, such as the e-mail messages in an information worker's inbox, the printed product specifications on someone's desk, the documents in a document library, or the pages on a corporate Web site. It is expected that active documents will change over time, be copied and shared, and generally move about the organization.

Active documents may be declared as records if they serve as evidence of an activity or transaction performed by your organization. For example, if your organization provides a service that includes delivering content to a customer, then that content becomes a record of the delivery of the service and a copy of the document should be retained. Some types of active documents will never become records; for example, you might not classify an e-mail sent among coworkers to agree on where to meet for lunch as a record.

At some point in a document's life cycle, it stops being active. For example, when a deliverable document is presented to a customer, it might no longer be necessary to keep managing this content as an active record. But if the document is a record, it should be saved and protected for some retention period.

 Archived documents   These are documents that are no longer active but are not records (either because they no longer have to be retained or because they were never classified as records). Archived documents are kept by an enterprise for non-legal reasons such as for historical preservation.

## Determine what is a record

Determining which active documents in your organization might be declarable as records requires the collaboration of records managers, lawyers, compliance officers, and content managers. Note that, even if your enterprise is not in a highly regulated industry, there are general laws (such as the Sarbanes-Oxley Act of 2002) that your records managers need to be aware of that might obligate your enterprise to retain records. Along with general business laws, you need to evaluate legal requirements specific to your enterprise.

It is beyond the scope of this article to provide more than general information about how to determine what is a record in your organization. Most likely, your enterprise is already doing some form of records management and has filled most of the records management roles you need, and you might already have a taxonomy of records.

Generally, to determine what are records in your organization:

1. Understand your enterprise's legal obligations and business needs.

2. In a collaborative effort across the divisions of your organization, analyze active document usage.

3. Develop a list of active document types that should become records. For example, you may determine that the following should be retained as records:

 Contracts to rent corporate space.

 Documents related to employees' benefits.

 Documents related to product research and development.

4. Categorize the records.

|  |
| --- |
| Worksheet action |
| This is useful because records in the same category often have the same retention periods and might require equivalent treatment in other ways. You can use the [Record categories worksheet](http://go.microsoft.com/fwlink/?LinkID=73300&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73300&clcid=0x409) to record the results of your research. |

Here is a sample worksheet:

|  |  |  |  |
| --- | --- | --- | --- |
| Records | Record category | Description | Sites |
| Benefit plans, insurance plans, pension plans | Employee Benefit Descriptions | Descriptions of all employee benefit plans. | http://example |
| Payroll timesheets, supplementary payroll information | Payroll Records | Summaries of hours worked, overtime, and salary paid. | http://example |
| Vendor invoices | Invoices | Records of goods or services purchased from vendors. | http://example |
| Product surveys, questionnaires, training manuals, training videos | Training Materials | Provides internal or external training. | http://example |
| Shipping forms, shipping reports | Shipping Records | Documents the shipment of materials. | http://example |
| Press releases, newspaper articles | Press Releases | Public relations information about products and services. | http://example |
| Emergency contact sheets, medical plan enrollment forms, resumes, benefits status reports | Personnel Records | Records of individuals' employment histories and related personnel actions. | http://example |

## Complete the file plan

After determining which documents should be retained as records and creating a set of record categories, complete your file plan by defining retention periods for each record category, indicating how to dispose of records when their retention periods have expired and supplying other information such as the primary records manager for each record type and the media in which the record is stored.

Here is a completed sample file plan:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Records | Description | Media | Record category | Retention | Disposition | Contact |
| 401k plans | Description of employee benefit plan. | Web pages | Employee Benefit Plans | X years | None | Reshma Patel |
| Insurance plans | Description of employee insurance plan. | Print | Employee Benefit Plans | X years | None | Reshma Patel |
| Pension plans | Description of employee pension plan. | Print | Employee Benefit Plans | X years | None | Reshma Patel |
| Payroll timesheets | Summaries of hours worked, overtime, and salaries paid. | Electronic documents | Payroll Records | X years | Destroy | Reshma Patel |
| Supplementary payroll information | Summaries of sick time, vacation time, and other non-salary payroll items. | Electronic documents | Payroll Records | X years | Destroy | Reshma Patel |
| Vendor invoices | Records of goods or services purchased from vendors. | Print | Invoices | X years | Destroy | Eric Lang |
| Product surveys | Customer satisfaction survey. | Web pages | Survey Materials | X years | Archive | Molly Dempsey |
| Questionnaires | Questionnaire to determine customer demographics. | Print | Survey Materials | X years | Archive | Molly Dempsey |
| Training manuals | Hard-copy training content. | Print | Training Materials | X years | Destroy | Molly Dempsey |
| Training videos | Video training content. | Video | Training Materials | X years | Destroy | Molly Dempsey |
| Shipping forms | Configure the shipment of materials. | Print | Shipping Materials | X years | Destroy | Eric Lang |
| Shipping reports | Document the shipment of materials. | Electronic spreadsheets | Shipping Materials | X years | Destroy | Eric Lang |
| Press releases | Releases about products and services. | Electronic documents | Public Relations Information | X years | Archive | Molly Dempsey |
| Newspaper articles | News about products and services. | Print | Public Relations Information | X years | Archive | Molly Dempsey |
| Emergency contact sheets | Employee information. | Electronic documents | Personnel Records | X years | Destroy | Reshma Patel |
| Medical plan enrollment forms | Employees' sign-up forms for health plans. | Electronic documents | Personnel Records | X years | Destroy | Reshma Patel |
| Resumes | Resumes received. | Mixed | Personnel Records | X years | Destroy | Reshma Patel |

note_ddNote:

The above example is a sample and not a recommendation of any particular file plan settings. No retention periods are supplied to reinforce that this is an example and not a recommendation of any records management policy.

## Worksheet

You can use the following worksheet with this article to help plan your deployment:

 [Record categories worksheet](http://go.microsoft.com/fwlink/?LinkID=73300&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73300&clcid=0x409)

# Design the Records Center site (Office SharePoint Server 2007)

In this article:

 [About the Records Center site](#DSDOC_section103702c06_3e32_409d_ad8c_7e)

 [Planning document libraries for records retention](#DSDOC_section203702c06_3e32_409d_ad8c_7e)

 [Planning metadata](#DSDOC_section303702c06_3e32_409d_ad8c_7e)

 [Planning the record routing table](#DSDOC_section403702c06_3e32_409d_ad8c_7e)

 [Planning the site's security](#DSDOC_section503702c06_3e32_409d_ad8c_7e)

To manage records in Microsoft Office SharePoint Server 2007, site designers and records managers plan and implement a Records Center site. This site, based on the Records Center site template, contains features you can use to implement your file plan and manage the records while they are being retained.

Design the Records Center site in four steps:

1. Based on your file plan, plan the document libraries you need to store your records.

2. Plan metadata for each record type, and define columns in the document libraries to contain and display the metadata.

3. For each type of record, plan policies to define retention periods and auditing specifications that help meet your enterprise's regulatory obligations.

4. Based on your analysis of active content that will become records, plan the record routing table, which maps each type of record to the appropriate library in the Records Center site. When a record is sent to the Records Center site, either programmatically or via the user interface, this table is used to determine how to classify the document within the file plan.

## About the Records Center site

The Office SharePoint Server 2007 Records Center site template is designed to implement records management and retention.

By combining standard Office SharePoint Server 2007 features with specialized records management features, the Records Center site provides the following capabilities:

 Record routing   When a document is sent to the Records Center site, either by using a default method such as the Send to Records Center command or by using the programmable interface, the record is routed to the correct document library based on its type. The correlation between incoming record types and their related document libraries is managed in the record routing table, as described later in this article in the section [Planning the record routing table](#DSDOC_section403702c06_3e32_409d_ad8c_7e).

When a record is sent to the Records Center site, other information is sent along with the record itself. This other information includes the record's audit history, which is stored in an XML file, and all of its metadata, which is stored both in an XML file and in columns of metadata in the Records Center site.

 Policy enforcement   Office SharePoint Server 2007 includes the following policy features that are useful for records management:

 Auditing   Logs events and operations performed on documents. In the context of records management, this is useful to record who is viewing and accessing information in the Records Center site.

 Expiration   Specifies how long the record should be retained and provides an action to take when the retention period ends, such as initiating a disposition approval workflow. In the context of records management, the retention period usually starts when the record is stored in the Records Center site.

 Barcodes   Provides each record with a unique barcode graphic and numeric value. The value of the barcode is stored and indexed along with the electronic version of the record. In the context of records management, barcodes are useful for retaining and tracking physical records. When the records in a library have hard-copy versions, barcodes provide a way to correlate the hard-copy versions with their electronic counterparts. See the topic Plan how to retain physical records for a discussion of physical records retention planning.

 Programmable interface   A comprehensive records management solution enables records to flow into the records management system from all sources of records in the organization. The Records Center site's programmable interface provides a method to send a file, its associated metadata, and its audit history to the Records Center site as part of a business process. By using this method, any document management system can be configured to send files to the Records Center site. You can also add modules that extend the classification of incoming records — for example, to classify records based on their metadata values.

In addition to extending the interface for moving records into the Records Center site, you can extend other aspects of the Records Center site. For example, you can design additional policy features that meet your enterprise's unique requirements.

 Hold   The Office SharePoint Server 2007 Records Center site provides a way to suspend a record's expiration policy. It includes a hold feature that lets records managers create named "holds" that protect specified records from expiring and being destroyed. For example, in the event of an internal audit or a litigation, putting the relevant records on hold ensures that those records, which you may be required to produce, will be available until the audit or litigation is complete.

## Planning document libraries for records retention

The easiest approach to planning document libraries for records retention — and the approach recommended in this planning guide — is to create a document library for each type of record in your file plan (see [Develop the file plan (Office SharePoint Server 2007)](#DSDOC_037fb582_6448_4baf_85d4_6e6221f216)). For example, each record in the following sample file plan could be stored in a separate library:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Records | Description | Media | Record category | Retention | Disposition | Contact |
| 401K plan | Description of employee benefit plan. | Web pages | Employee Benefit Plans | X years | None | Reshma Patel |
| Insurance plan | Description of employee insurance plan. | Electronic documents | Employee Benefit Plans | X years | None | Reshma Patel |
| Press releases | Releases about products and services. | Electronic documents | Public Relations Information | X years | Archive | Molly Dempsey |
| Newspaper articles | News about products and services. | Print | Public Relations Information | X years | Archive | Molly Dempsey |

|  |
| --- |
| Worksheet action |
| To help you plan document libraries for records retention, list each record type and assign it to a document library. To record information about the library, such as what policies to apply and what columns of metadata to add to it, use the [Document library for retaining records worksheet](http://go.microsoft.com/fwlink/?LinkId=73298&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73298&clcid=0x409) for each library. |

## Planning metadata

After planning document libraries for records retention, the next step is to determine the metadata to define for each library. There are two categories of metadata to consider:

 Records metadata

 Additional metadata

### Planning records metadata

Records metadata is the metadata that is submitted along with a record when it is sent to the Records Center site. Determining what the optimal metadata for a type of record is depends on that type of record, and it may require discussions among records managers and the managers of the content on the active servers. Once you have determined that adequate metadata is being generated and stored for a record type, you can configure the destination document library for that type of record to retain the metadata along with the record. When a record is sent to the destination document library:

 The names and values of each column of metadata associated with it are saved along with the record in an XML file in a hidden \_properties folder that is created in the destination library.

 The metadata values are copied to matching columns in the destination library.

For each column of metadata for a type of record, define a column in the destination document library that matches the incoming column's name and type. To specify that the column must be submitted along with the record and that it must have a data value associated with it, configure the column in the Office SharePoint Server 2007 user interface to require data. (Do this by selecting the Require that this column contains information option.) For example, if the source records include a "Department" column of type "Single Line of Text," define a column with that name and type in the destination document library.

note_ddNote:

If a record is submitted for retention and required metadata is missing (either because no value is supplied or because the column is missing entirely), the submitter will be prompted for the missing metadata. If the metadata is not provided, the record will not be accepted for retention. If the document is sent programmatically (rather than from the user interface), the file is placed in a temporary holding area, and information is sent back to the calling program that must be handled programmatically to supply the missing column of information before the record is added to the destination library.

|  |
| --- |
| Worksheet action |
| In the [Document library for retaining records worksheet](http://go.microsoft.com/fwlink/?LinkId=73298&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73298&clcid=0x409), record the name and type of each column of records metadata that you want to store along with the record, and specify if the column should be required. |

### Planning additional metadata

Along with displaying columns of metadata associated with retained records, you may want to add other columns of information to display in your records management document libraries. For example, you may want to add a "Records Manager" column to display the name of the person on your team who is responsible for managing the records stored in the document library. Note that, as with columns submitted along with records, if you specify that these additional columns are required, the record submitter will be prompted for the missing metadata and the record will not be accepted unless that metadata is supplied. If you do not want the submitter to be prompted for the values of additional metadata, do not configure the columns to require data.

note_ddNote:

You can define columns for use in multiple document libraries. To do this, you can create them in the Column Templates gallery associated with the Records Center site.

|  |
| --- |
| Worksheet action |
| In the [Document library for retaining records worksheet](http://go.microsoft.com/fwlink/?LinkId=73298&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73298&clcid=0x409), record the name and type of each column of additional metadata that you want to store along with the record, and specify if the column should be required. |

### Planning policies

An information management policy is a set of rules for a type of content. Each rule in a policy is a "policy feature." For example, an information management policy feature could specify how long a type of content should be retained or which actions on the content should be audited. Information management policies enable you to control who can access your organizational information, what they can do with it, and how long to retain it. Policies in a records management system should be configured by records managers to reflect the enterprise's regulatory obligations.

Microsoft Office SharePoint Server 2007 includes the following policy features that are useful for managing records in the Records Center site:

 Auditing, to demonstrate that records are being managed properly.

 Expiration, to control how long records are retained in the Records Center site.

 Barcodes, to track physical records.

Depending on your records management needs, you can also acquire or develop your own records management–related policy features that are not included in Office SharePoint Server 2007, such as policies that digitally sign records or convert them to a fixed format.

There are two recommended options for planning policies for records management:

 If the same policies will apply to multiple record types — for example, because they are in the same record category — create a separate site collection policy for each set of record types. Associate each site collection policy with the relevant document libraries.

|  |
| --- |
| Worksheet action |
|  In the topic [Develop the file plan (Office SharePoint Server 2007)](#DSDOC_037fb582_6448_4baf_85d4_6e6221f216), you determined record categories using the [Record Categories worksheet](http://go.microsoft.com/fwlink/?LinkId=73300&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73300&clcid=0x409). For each record category that requires a policy, create and configure the policy in the Site Collection Policy gallery by adding policy features and configuring them. (For more general information about policies and policy planning, including links to policy planning worksheets, see the topic [Plan information management policies](#DSDOC_4de4007d_a45f_419d_9512_824421e143). |

|  |
| --- |
| Worksheet action |
| In the [Document library for retaining records worksheet](http://go.microsoft.com/fwlink/?LinkId=73298&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73298&clcid=0x409) for a library, record your decisions about policy configuration:   To associate a site collection policy with the document library based on the record category of the content stored in the document library, in the Policy section of the worksheet, record the name of the policy template for that record category.   To associate unique policy features directly with the document library, in the Policy section of the worksheet, enter each policy feature along with configuration notes for that feature. |

## Planning the record routing table

The record routing table is a list in the Records Center site that lists each type of record that might be submitted to the Records Center site and specifies the library in which to store it. When files are submitted to the Records Center site by using the Send to Records Center command or the programmable interface, this list is used to route the incoming file to its proper location.

Each entry in the record routing table is a record series list item specifying:

 The title and description of the record series. The name of a record series indicates a type of item that can be submitted to the Records Center site for the current record series. If files are submitted to the Records Center site from a server based on Office SharePoint Server 2007 or Microsoft Windows SharePoint Services 3.0, the name should match a content type name in the library containing the active record. If the files are submitted from another source, the name should match the type of document that can be submitted from that file source using the programmable interface.

 The location (a document library) in which to save the records for the current record series.

 A list of record types, called aliases. These are other names for the records that can be submitted to the Records Center site for this record series. For example, if your organization has multiple departments that use different names for the same underlying record type (such as "contracts" and "agreements"), you could define aliases for each name used for the same record type.

If the records are submitted to the Records Center site from a server based on Office SharePoint Server 2007 or Windows SharePoint Services 3.0, the aliases will be content types. If the records are coming from another file source, the aliases should match the types that can be specified for that record source in the programmable interface.

One record series in the record routing table should specify the default document library. When a Records Center site receives a file that does not match an alias in the record routing list, the file is moved to the specified default location where it can be manually filed by a records manager. The Records Center site template includes an Unclassified Records document library and record series as the initial default location; it is recommended that you keep this record series as the default.

A good approach to planning your record routing table is:

1. For each document library that you created in your Records Center site, plan to create an entry in the record routing table.

2. Give a record series the same title as the primary type of record to be retained using that record series.

3. Based on your analysis of active documents in your enterprise, obtain a list of all the content types or other record types that could be submitted for the current record series; these should be listed in your file plan, and they will be the aliases for the record series. For example, if, in a human resources Records Center site, you decide to retain all pension plans, insurance plans, and 401k plans in an Employee Benefits Plans document library, you would specify all these record types as aliases in the record series entry for the Employee Benefits Plans document library.

4. Determine which record series should be the default.

|  |
| --- |
| Worksheet action |
| Use the [Records routing table worksheet](http://go.microsoft.com/fwlink/?LinkId=73303&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73303&clcid=0x409) to record your decisions about each record series you plan to create in the record routing table. Note that there should be a record series for each document library in your Records Center site. |

## Planning the site's security

Because it is based on Office SharePoint Server 2007, the Records Center site uses the Office SharePoint Server 2007 authentication and authorization model and its underlying security model. You control the Records Center site's security by controlling who has access to the site and what operations they are permitted to perform on the site. For a full discussion of Office SharePoint Server 2007 security planning, see [Chapter overview: Plan site and content security [Office SharePoint Server]](#DSDOC_85a1866e_2743_4f98_a1ac_9ea61905c6).

Here are some unique considerations for configuring permissions in the Records Center site:

 Create a unique Web application for the Records Center site. This is generally a more secure option, and it can guarantee that the records won't be commingled with active documents in the database used by the site. Also, by using a separate Web application, you can optimize your backup and restoration schedule to meet your records management needs.

 Do not configure the Web application on which the Records Center site is running to use Forms Authentication. Doing this will require that you enable anonymous submissions to the Records Center site, to allow users to submit records using the user interface or the programmable interface.

 For a user or application to submit files to the Records Center site, that user must have Edit Items rights to the files on the document management server and Add Items rights on the Records Center site. To help protect security, create a group on the Records Center site with Create List rights (but not Edit Items rights), and add the particular accounts on other servers that will submit items to the Records Center site to this group.

 If records are being submitted to the Records Center site from sites in other Web applications, the identity under which the shared services application pool is running on the Web applications from which records will be submitted should be added on the Records Center site as a user with Create List rights but not Edit Items rights.

 To be able to manage records, a user of the Records Center site must have Edit Items rights. In general, only give records managers and legal team members Edit Items rights to content on the Records Center site. For sensitive content, you can limit the set of users with Edit Items rights by assigning them rights at the document library, folder, or even list item level. For example, a particularly sensitive document could have a single records manager assigned to manage it.

 Files are put on hold in the Records Center site by creating "holds" in a specialized Holds list. A hold is a list item, and to create a hold, a user must have Add Items rights to the Holds list. Once a hold is created, a user must have Edit Items rights on the item being placed on hold and View Items rights to the Holds list. Because this list might contain very sensitive information, limit the set of users of the Holds list to team members who can create holds and team members who can put items on hold.

## Worksheets

Use the following worksheets with this article to help plan your deployment:

 [Document library for retaining records worksheet](http://go.microsoft.com/fwlink/?LinkId=73298&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73298&clcid=0x409)

 [Record categories worksheet](http://go.microsoft.com/fwlink/?LinkId=73300&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73300&clcid=0x409)

 [Records routing table worksheet](http://go.microsoft.com/fwlink/?LinkId=73303&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73303&clcid=0x409)

# Plan how records are collected (Office SharePoint Server 2007)

In this article:

 [Techniques for moving files into the Records Center site](#DSDOC_section1f3fae102_5b20_4c9f_9707_ab)

 [Completing your plan](#DSDOC_section2f3fae102_5b20_4c9f_9707_ab)

After you develop a file plan and design the Records Center site, plan how active electronic and hard-copy documents in your organization will move to the Records Center site. This article reviews techniques you can use to move content to the Records Center site and suggests a way to plan how items in your file plan will become records.

## Techniques for moving files into the Records Center site

You can use the following techniques for moving files into the Records Center site:

 Manually sending content from a Web site based on Microsoft Office SharePoint Server 2007.

 Using managed e-mail folders in Microsoft Exchange Server "12".

 Using a custom solution based on the Microsoft Windows SharePoint Services 3.0 object model, such as a custom workflow.

### Manually sending content to the Records Center site

If a file is stored in a document library in a Web site based on Office SharePoint Server 2007, an information worker can declare it a record by sending a copy of it to the Records Center site using the Send to Records Center command. When a site collection administrator configures the connection to the Records Center site, this command becomes available on all active documents in the site collection. Along with sending a copy of the document to the Records Center site, the Send to Records Center command sends the document's metadata, its audit history, and its location on the active document server. If additional metadata is required in the Records Center site, the user is prompted to supply it. Although manually sending records to the Records Center site is not a practical large-scale solution, you can use it to supplement other methods of moving content to the Records Center site.

note_ddNote:

When the Send to Records Center command is used to declare a record and send it to the Records Center site, it leaves the active document in its current location. The active document can continue to be used, or it can be deleted if that is appropriate.

### Using managed e-mail folders in Microsoft Exchange Server 2007 to send e-mail and files to the Records Center site

Exchange Server "12" includes policy features similar to those implemented using Office SharePoint Server 2007. In Exchange Server "12", administrators can configure an Exchange folder so that, when a user moves an e-mail message into the folder, the e-mail message is copied to the Records Center site using Simple Mail Transfer Protocol (SMTP).

When an e-mail message copied from Office SharePoint Server 2007 is received in the Records Center site, it is handled like any other file sent to the Records Center site; it is moved to the appropriate document library based on the matching entry in the record routing table. For more information about the record routing table, see [Design the Records Center site (Office SharePoint Server 2007)](#DSDOC_03702c06_3e32_409d_ad8c_7e84eae386).

The policy and records retention features described above are managed e-mail folders features introduced in Exchange Server "12". Using managed e-mail folders, Exchange administrators can define folders that are targeted to specific business purposes, such as Personnel Issues, Product Planning, or Contracts. By assigning policies to these managed folders, administrators can ensure proper expiration of content, configure connections to other servers (such as a Records Center site in Office SharePoint Server 2007), or initiate any custom actions that have been configured in Exchange Server "12". The use of managed e-mail folders can be enforced by rules (such as moving messages into folders based on their subject lines), or the use of the folders can be voluntary, requiring information workers to manually move e-mail into appropriate folders. For a full description of implementing managed e-mail folders and other Exchange Server "12" features, see the Exchange Server "12" Administrator's Guide.

### Using a custom solution to send files to the Records Center site

You can programmatically send files and e-mail messages to the Records Center site from file and e-mail servers, whether or not they are based on Office SharePoint Server 2007 or Exchange Server "12". To do this, develop and install programs that have interfaces to the records management methods implemented in the Windows SharePoint Services 3.0 object model and then integrate those programs into your document or e-mail management processes.

By using the Windows SharePoint Services 3.0 object model, you can determine the list of record types defined in a Records Center site's record routing table, and then submit a file — including its contents, properties, and audit history — to a particular record series. For a full description of programming the Windows SharePoint Services 3.0 object model, see the Office SharePoint Server 2007 [Software Develop](http://go.microsoft.com/fwlink/?LinkId=71218&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=71218&clcid=0x409).

You can use the Windows SharePoint Services 3.0 object model to create a custom workflow that copies files to the Records Center site. A workflow that sends files to the Records Center site can be integrated into your document management system as part of a workflow that guides a document through its life cycle. For document types that have a predictable life cycle, such as expense reports, you could implement a workflow that guides the document through its various stages and, as a final step, sends a copy of the document to the Records Center site. The workflow could be triggered by the creation of a new document.

## Completing your plan

After you [Develop the file plan (Office SharePoint Server 2007)](#DSDOC_037fb582_6448_4baf_85d4_6e6221f216) and review the methods for moving content into the Records Center site, complete your plan by determining how to send each type of record to the Records Center site. The factors to consider include the following:

 Is compliance enforced or voluntary?

 Can you count on the cooperation of information workers in your organization to comply with records management processes? In general, avoid manual processes; however, where they are needed, devise adequate training and monitoring to ensure team compliance.

 Will content be stored on Office SharePoint Server 2007 document management servers?

 Will e-mail be stored on Exchange Server "12" e-mail servers? If e-mail is stored on Exchange Server "12" e-mail servers, you can use built-in mechanisms such as managed e-mail folders to implement the connection to the Records Center site. If e-mail is stored on other e-mail servers, you can use the Windows SharePoint Services 3.0 object model to design and implement custom methods for sending files to the Records Center site.

 Are you retaining physical content? Managing active physical content, such as hard-copy documents or CD-ROMs, and sending it to a records vault for retention (along with tracking the record in a Records Center site) requires unique planning not described in this topic. For example, if no electronic version of a hard-copy document exists, you might need to track the item by using a list and its associated policies and workflows. For a full discussion of strategies and techniques for tracking a physical record, both while it is active and after it is sent to the Records Center site, see the topic Plan how to retain physical records.

The following table illustrates how some records in a file plan will move to a records repository site:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Documents | Description | Media | Source location | Becomes a record... |
| Benefit plan | Description of employee benefit plan. | Web pages | Office SharePoint Server 2007 document library | Using a custom workflow associated with expiration policy |
| Insurance plan | Description of employee insurance plan. | Print | Physical document associated with list item in Office SharePoint Server 2007 | By sending to a physical vault and creating a list item in the Records Center site to track (using a barcode) |
| Payroll timesheets | Summaries of hours worked, overtime, and salaries paid. | Electronic documents | Payroll records server not based on Office SharePoint Server 2007 | Using a custom program |
| Product development files | Specifications of products and associated documents. | Electronic documents | Office SharePoint Server 2007 document library | Using custom workflow associated with expiration policy and manually using Send To Records Center command |
| Product development e-mail | E-mail messages related to product development. | E-mail | Exchange Server "12" managed folders | Manually by moving messages to an Exchange folder connected to the Records Center site |

# XI Plan site and content security

In this chapter:

 [Chapter overview: Plan site and content security [Office SharePoint Server]](#DSDOC_85a1866e_2743_4f98_a1ac_9ea61905c6)

 [Plan site security [Office SharePoint Server]](#DSDOC_681acebc_32c2_4ec7_8961_c3bdce69bb)

 Plan for securing particular document libraries with IRM

 Determining publishing permission levels

 Determine which WRM server to connect to

 [Determine permission levels and groups to use [Office SharePoint Server]](#DSDOC_610a48d4_a805_4c47_8801_a8a912b294)

 [Define custom permission levels [Office SharePoint Server]](#DSDOC_c5dd8b7e_202d_4d33_8535_5c03f88ea1)

 [Choose which security groups to use [Office SharePoint Server]](#DSDOC_1a45c752_a485_439a_a19b_340a5bd7a6)

 [Choose administrators and owners for the administration hierarchy (Office SharePoint Server)](#DSDOC_cf418db1_6212_4cd7_9383_830249c838)

 [Plan for InfoPath Forms Services security [Office SharePoint Server]](#DSDOC_a41ac3e6_eacb_4b2c_b35f_48c5ab6a0e)

# Chapter overview: Plan site and content security [Office SharePoint Server]

There are several elements that make up security for your environment. One of these elements is the permissions that control access to your sites and the content in your sites. A new security model and new security features (such as SharePoint® groups to control membership, and item- and document-level permissions) make it easy to control who has access to what content in your sites. This chapter explains how security for sites and site content works, and it guides you through making choices about site security.

Another element integral to the security of your environment is how you structure security at the Web application level — choosing authentication methods and specifying the encryption methods to use. For more information, see [Chapter overview: Plan for and design security (Office SharePoint Server)](#DSDOC_3df68222_235b_45de_82fa_b89166c5c6).

In this chapter:

 [Plan site security [Office SharePoint Server]](#DSDOC_681acebc_32c2_4ec7_8961_c3bdce69bb) helps you understand the elements of site security and how permissions are assigned, and it helps you choose which levels of site security to use in your site collection or subsite.

 [Determine permission levels and groups to use [Office SharePoint Server]](#DSDOC_610a48d4_a805_4c47_8801_a8a912b294) reviews the available permission levels and groups, and it helps you determine whether you need additional permission levels or groups.

 [Define custom permission levels [Office SharePoint Server]](#DSDOC_c5dd8b7e_202d_4d33_8535_5c03f88ea1) helps you create any custom permission levels you might need.

 [Choose which security groups to use [Office SharePoint Server]](#DSDOC_1a45c752_a485_439a_a19b_340a5bd7a6) helps you determine which Microsoft® Windows® security groups and user accounts to use to grant access to sites, decide whether to use the All Authenticated Users group, and decide whether to allow anonymous access.

 [Choose administrators and owners for the administration hierarchy (Office SharePoint Server)](#DSDOC_cf418db1_6212_4cd7_9383_830249c838) defines the levels of administration from the server level to the subsite level, and it helps you choose the administrators you need for each level.

 [Plan for InfoPath Forms Services security [Office SharePoint Server]](#DSDOC_a41ac3e6_eacb_4b2c_b35f_48c5ab6a0e) helps you plan security for InfoPath® Forms Services.

# Plan site security [Office SharePoint Server]

In this article:

 [About site security elements](#DSDOC_section1681acebc_32c2_4ec7_8961_c3)

 [About assigning permissions](#DSDOC_section2681acebc_32c2_4ec7_8961_c3)

 [About fine-grained permissions and permission inheritance](#DSDOC_section3681acebc_32c2_4ec7_8961_c3)

 [Choose which levels of site security to use](#DSDOC_section4681acebc_32c2_4ec7_8961_c3)

 [Plan for permission inheritance](#DSDOC_section5681acebc_32c2_4ec7_8961_c3)

 [Worksheet](#DSDOC_section6681acebc_32c2_4ec7_8961_c3)

This article addresses planning for access control and authorization at the site collection, site, and subsite levels, and does not address planning for the security of your server or server farm. For more information about planning for other aspects of security, such as authentication methods and encryption, see [Chapter overview: Plan site and content security [Office SharePoint Server]](#DSDOC_85a1866e_2743_4f98_a1ac_9ea61905c6).

Site security is controlled by assigning permissions to users and groups for a specific securable object (such as site, list, or item). When you plan for site security, you need to decide:

 To what degree you want to control permissions for individual securable objects. For example, do you want to control access for the entire site, or do you need specific security settings for a particular list, folder, or item?

 How you want to categorize and manage your users (by using groups). This article covers the essentials of site security and assists you as you determine the securable objects at which to apply specific permissions. For more information about categorizing users into groups, see [Choose which security groups to use [Office SharePoint Server]](#DSDOC_1a45c752_a485_439a_a19b_340a5bd7a6).

note_ddNote:

The way that groups and permissions interact has changed significantly from the previous version. In the previous version, site-level groups were used to contain both users and permissions — that is, when you added a user to a site group, you automatically determined the permissions that the user was granted for a site. In this version, the concepts of groups of users and permissions have been separated: SharePoint groups at the site collection level contain the users, permission levels contain the permissions, and groups have no permissions until they are assigned a permission level for a specific securable object (such as a site, list or library, folder, item, or document).

## About site security elements

Regardless of what type of site you are creating, the security for your site includes the following five elements:

 Individual user permissions   Individual permissions that grant the ability to perform specific actions. For example, the View Items permission grants the user the ability to view items in a list. Farm administrators can control which permissions are available for the server farm by using the User Permissions for Web Application page in Central Administration. (To get to this page, on the Application Management page, under Application Security, click User permissions for Web application.) For information about available permissions, see User permissions and permission levels.

 Permission level   A pre-defined set of permissions that grants users permission to perform related actions. The default permission levels are: Limited Access, Read, Contribute, Design, and Full Control. For example, the Read permission level includes the View Items, Open Items, View Pages, and View Versions permissions (among others), all of which are needed to read documents, items, and pages of a SharePoint site. Permissions can be included in multiple permission levels. Permission levels can be customized by anyone assigned to a permission level that includes the Manage Permissions permission. For information about default permission levels and which permissions are included in them, see User permissions and permission levels.

 User   A person with a user account that can be authenticated through the authentication method used for the server. You can add individual users and directly assign a permission level to each user; users do not have to be part of a group. We recommend that you assign permissions to groups rather than users. Because it is inefficient to directly maintain user accounts, you should only assign permissions on a per-user basis as an exception. For more information about user account types, see User permissions and permission levels.

 Group   A group of users. Can be a Windows security group (such as Department\_A) that you add to the site, or a SharePoint group such as Site Owners, Site Members, or Site Visitors. Each SharePoint group is assigned a default permission level, but the permission level for any group can be changed as needed. Anyone assigned a permission level that includes the Create Groups permission (included in the Full Control permission level by default) can create custom SharePoint groups.

 Securable object   Users or groups are assigned a permission level for a specific securable object: site, list, library, folder, document, or item. By default, permissions for a list, library, folder, document, or item are inherited from the parent site or parent list or library. However, anyone assigned a permission level for a particular securable object that includes the Manage Permissions permission can change the permissions for that securable object. By default, permissions are initially controlled at the site level, with all lists and libraries inheriting the site permissions. Use list-level, folder-level, and item-level permissions to further control which users can view or interact with the site content. You can return to inheriting permissions from a parent list, the site as a whole, or a parent site, at any time.

## About assigning permissions

You can assign a user or group a permission level for a specific securable object (site, list, or item). Individual users or groups can have different permission levels for different securable objects.

note_ddNote:

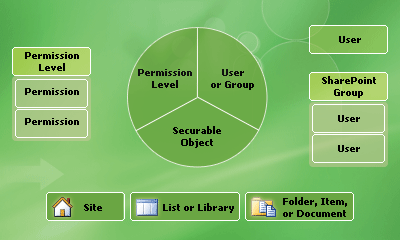
Because it is inefficient to directly maintain user accounts, it is recommended that you use group permissions as much as possible. Particularly if you are using fine-grained permissions (see the following section), you should use groups to avoid having to track individual user accounts. People can move in and out of teams and change responsibilities frequently, and you do not want to have to track all of those changes and continually update the permissions for uniquely secured objects.

 Site administrators and members of the Site Owners group (or users granted Manage Web Site permissions in their permission levels) create groups and assign permission levels for the site as a whole.

 List or library administrators (or users granted Manage Lists permissions in their permission levels) can specify more or less restrictive permissions for their list or library (or a folder within the list or library) by adding or removing users or groups, or by changing the permission levels for users or groups.

 Item or document creators can specify more or less restrictive permissions for an item or document by adding or removing users or groups, or by changing the permission levels for users or groups.

The following diagram illustrates how users and groups are assigned specific permission levels for a particular securable object.



## About fine-grained permissions and permission inheritance

You can use fine-grained permissions (permissions on the list or library, folder, or item or document level) to more precisely control what actions users can take on your site. The following securable objects are available for permission assignments:

 Site   Controls access to the site as a whole.

 List or library   Controls access to a specific list or library.

 Folder   Controls access to a folder's properties (such as the name of the folder).

 Item or document   Controls access to a specific list item or document.

### Permission inheritance and fine-grained permissions

By default, permissions within a site are inherited from the site. However, you can break this inheritance for any securable object at a lower level in the hierarchy by editing the permissions (creating a unique permission assignment) on that securable object. For example, you can edit the permissions for a document library, which breaks the inheritance from the site. However, the inheritance is broken for only the particular securable object for which you assigned permissions; the rest of the site's permissions are unchanged. You can return to inheriting permissions from the parent list or site at any time.

### Permission inheritance and subsites

Web sites are themselves a securable object to which permissions can be assigned. You can configure subsites to inherit permissions from a parent site or create unique permissions for a particular site. Inheriting permissions is the easiest way to manage a group of Web sites. However, if a subsite inherits permissions from its parent, that set of permissions is shared. This means that owners of subsites that inherit permissions from the parent site can edit the permissions of the parent. If you want to change permissions for the subsite alone, you must stop inheriting permissions and then make the change.

Subsites can inherit permissions from a parent site. You can stop inheriting permissions for a subsite by creating unique permissions. This copies the groups, users, and permission levels from the parent site to the subsite, and then breaks the inheritance. If you change from unique permissions to inherited, then users, groups, and permission levels start being inherited, and you lose any users, groups or permission levels that you uniquely defined in the subsite. Permission levels can also be inherited (and they are, by default), such that the Read permission level is the same, no matter what object it is applied to. You can break that inheritance by editing the permission level. For example, you might not want the Read permission level on a particular subsite to include the Create Alerts permission).

## Choose which levels of site security to use

When you create your permission structure, it is important to find the balance between ease of administration, performance, and the need to control specific permissions for individual items. If you use fine-grained permissions extensively, you will spend more time managing the permissions, and users may experience slower performance when they try to access site content. As with any server or Web site, it is also important to follow the principle of least privilege when it comes to authorizing access to the site: Users should have only the permission levels they need to use. Begin by using the standard groups (such as Members, Visitors, and Owners) and controlling permissions at the site level for the easiest administration experience. Make most users members of the Visitors or Members groups. Limit the number of people in the Owners group to only those users whom you want to allow to change the structure of the site or change site settings and appearance. By default, users in the Members group can contribute to the site, adding or removing items or documents, but cannot change the structure of the site or change site settings or appearance. You can create additional SharePoint groups and permission levels if you need more control over the actions that your users can take.

If there are particular lists, libraries, folders, items, or documents that contain sensitive data and must be even more secure, you can grant permissions to a specific group or individual user. Be aware, however, that there is no way to view all of the permissions specific to lists, libraries, folders, items, or documents within a site. This means that it is difficult to quickly ascertain who has permissions on which securable objects and also difficult to reset any fine-grained permissions in bulk.

## Plan for permission inheritance

It is easiest to manage permissions when there is a clear hierarchy of permissions and inherited permissions. It gets more difficult when some lists within a site have fine-grained permissions applied, and when some sites have subsites with unique permissions and some with inherited permissions. As much as possible, arrange sites and subsites, and lists and libraries so they can share most permissions. Separate sensitive data into their own lists, libraries, or subsites.

For example, it's much easier to manage a site that has permission inheritance as illustrated in the following table.

|  |  |  |
| --- | --- | --- |
| Securable object | Description | Unique or inherited permissions |
| SiteA | Group home page | Unique |
| SiteA/SubsiteA | Sensitive group | Unique |
| SiteA/SubsiteA/ListA | Sensitive data | Unique |
| SiteA/SubsiteA/LibraryA | Sensitive documents | Unique |
| SiteA/SubsiteB | Group shared project information | Inherited |
| SiteA/SubsiteB/ListB | Non-sensitive data | Inherited |
| SiteA/SubsiteB/LibraryB | Non-sensitive documents | Inherited |

Comparatively, it is not so easy to manage a site that has permission inheritance as illustrated in the following table.

|  |  |  |
| --- | --- | --- |
| Securable object | Description | Unique or inherited permissions |
| SiteA | Group home page | Unique |
| SiteA/SubsiteA | Sensitive group | Unique |
| SiteA/SubsiteA/ListA | Non-sensitive data | Unique, but same permissions as SiteA |
| SiteA/SubsiteA/LibraryA | Non-sensitive documents, but with one or two sensitive documents | Inherited, with unique permissions at the document level |
| SiteA/SubsiteB | Group shared project information | Inherited |
| SiteA/SubsiteB/ListB | Non-sensitive data, but with one or two sensitive items | Inherited, with unique permissions at the item level |
| SiteA/SubsiteB/LibraryB | Non-sensitive documents, but with a special folder containing sensitive documents | Inherited, with unique permissions at the folder and document level |

## Worksheet

On the Site and content security worksheet (http://go.microsoft.com/fwlink/?LinkId=73135&clcid=0x409), fill in your site hierarchy, and then list the permissions needed at each level of the hierarchy and any permission inheritance.

# Determine permission levels and groups to use [Office SharePoint Server]

In this article:

 [Review available default groups](#DSDOC_section1610a48d4_a805_4c47_8801_a8)

 [Review available permission levels](#DSDOC_section2610a48d4_a805_4c47_8801_a8)

 [Determine whether you need additional permission levels or groups](#DSDOC_section3610a48d4_a805_4c47_8801_a8)

 [Worksheet](#DSDOC_section4610a48d4_a805_4c47_8801_a8)

The most important decision about your site and content security in Microsoft Office SharePoint Server 2007 is to decide how to categorize your users and what permission levels to assign.

There are several default SharePoint groups that are intended to help you categorize your users based on the types of actions they need to perform, but you might have unique requirements or other ways of looking at sets of users. Likewise, there are default permission levels, but they might not always align exactly with the tasks that your groups need to perform.

In this article, you review the default groups and permission levels and decide whether to use them as they are, customize them, or create different groups and permission levels.

## Review available default groups

With SharePoint groups, you manage sets of users rather than individual users. SharePoint groups can be composed of many individual users, can hold a single Windows security group, or can be some combination of the two. SharePoint groups confer no specific rights to the site; they are merely a means to contain a set of users. Depending on the size and complexity of your organization or Web site, you can organize your users into several groups, or just a few.

The default SharePoint groups that are created for sites in Office SharePoint Server 2007 are listed in the following table.

|  |  |
| --- | --- |
| Group name | Default permission level |
| Restricted Readers | Restricted Read to the site (plus Limited Access to specific lists) |
| Style Resource Readers | Read to the Master Page Gallery and Restricted Read to the Style Library. |
| Viewers | View Only |
| Home Visitors | Read |
| Home Members | Contribute |
| Quick Deploy Users | Contribute to the Quick Deploy Items library (plus Limited Access to the rest of the site) |
| Approvers | Approve (plus Limited Access) |
| Designers | Design |
| Hierarchy Managers | Manage Hierarchy (plus Limited Access) |
| Home Owners | Full Control |

note_ddNote:

The Limited Access permission level is used to give groups access to a specific list, document library, item, or document, without giving them access to the entire site. Do not remove this permission level from the groups listed above. If this permission level is removed, the groups might not be able to navigate through the site to get to specific items with which they need to interact.

In addition, the following special users and groups are available for higher-level administration tasks:

 Site collection administrators   You can designate one or more users as primary and secondary site collection administrators. These users are recorded in the database as the contacts for the site collection, have full control of all sites within the site collection, can audit all site content, and receive any administrative alerts (such as verifying whether the site is still in use). Generally, you designate site collection administrators when you create the site, but you can change them as needed by using the Central Administration site or Site Settings pages.

 Farm administrators   Controls which users can manage server and server farm settings. The Farm Administrators group replaces the need for adding users to the Administrators group for the server, or to the SharePoint Administrators group that was used in Windows SharePoint Services version 2.0. Farm administrators have no access to site content by default; they must take ownership of the site to view any content. They do this by adding themselves as site collection administrators, which action is recorded in the audit logs. The Farm Administrators group is used in Central Administration only, and is not available for any sites.

 Administrators   Members of the Administrators group on the local server can perform all farm administrator actions and more, including:

 Installing new products or applications.

 Deploying Web Parts and new features to the global assembly cache.

 Creating new Web applications and new IIS Web sites.

 Starting services.

Like the Farm Administrators group, members of the Administrators group on the local server have no access to site content, by default.

After you identify the groups you need, determine the permission levels to assign to each group on your site.

|  |
| --- |
| Worksheet action |
| Use the [Custom permission levels and groups worksheet](http://go.microsoft.com/fwlink/?LinkId=73134&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73134&clcid=0x409) to record any groups you need to create. |

## Review available permission levels

The ability to view, change, or manage a particular site is determined by the permission level that you assign to a user or group. This permission level controls all permissions for the site and for any subsites, lists, document libraries, folders, and items or documents that inherit the site's permissions. Without the appropriate permission levels, your users might not be able to perform their tasks, or they might be able to perform tasks that you did not intend them to perform.

By default, the following permission levels are available:

 Limited Access   Includes permissions that allow users to view specific lists, document libraries, list items, folders, or documents when given permissions.

 Read   Includes permissions that allow users to view items on the site pages.

 Contribute   Includes permissions that allow users to add or change items on the site pages or in lists and document libraries.

 Design   Includes permissions that allow users to change the layout of site pages by using the browser or Microsoft Office SharePoint Designer 2007.

 Approve   Includes permissions to edit and approve pages, list items, and documents.

 Manage Hierarchy   Includes permissions to sites and edit pages, list items, and documents.

 Restricted Read   Includes permissions to view pages and documents, but not historical versions or user rights information.

 Full Control   Includes all permissions.

For more information about permissions that are included in the default permission levels, see User permissions and permission levels.

## Determine whether you need additional permission levels or groups

The default groups and permission levels are designed to provide a general framework for permissions, covering a wide range of organization types and roles within those organizations. However, they might not map exactly to how your users are organized or to the variety of tasks that your users perform on your sites. If the default groups and permission levels do not suit your organization, you can create custom groups, change the permissions included in specific permission levels, or create custom permission levels.

### Do you need custom groups?

The decision to create custom groups is fairly straightforward and has little impact on your site's security. Essentially, you should create custom groups instead of using the default groups if any of the following applies:

 You have more (or fewer) user roles within your organization than are apparent in the default groups. For example, if in addition to Approvers, Designers, and Hierarchy Managers, you have a set of people who are tasked with publishing content to the site, you might want to create a Publishers group.

 There are well-known names for unique roles within your organization that perform very different tasks in the sites. For example, if you are creating a public site to sell your organization's products, you might want to create a Customers group that replaces Visitors or Viewers.

 You want to preserve a one-to-one relationship between Windows security groups and the SharePoint groups. (For example, your organization has a security group for Web Site Managers, and you want to use that name as a group name for easy identification when managing the site).

 You prefer other group names.

### Do you need custom permission levels?

The decision to customize permission levels is less straightforward than the decision to customize SharePoint groups. If you customize the permissions assigned to a particular permission level, you must keep track of that change, verify that it works for all groups and sites affected by that change, and ensure that the change does not negatively affect your security or your server capacity or performance.

For example, regarding security, if you customize the Contribute permission level to include the Create Subsites permission that is typically part of the Full Control permission level, members of the Contributors group can create and own subsites, and can potentially invite malicious users to their subsites or post unapproved content. Or, regarding capacity, if you customize the Read permission level to include the Create Alerts permission that is typically part of the Contribute permission level, all members of the Home Visitors group can create alerts, which might overload your servers.

You should customize the default permission levels if either of the following applies:

 A default permission level includes all permissions except one that your users need to do their jobs, and you want to add that permission.

 A default permission level includes a permission that your users do not need.

note_ddNote:

You should not customize the default permission levels if your organization has security or other concerns about a particular permission and wants to make that permission unavailable for all users assigned to the permission level or levels that include that permission. In this case, you should turn off this permission for all Web applications in your server farm, rather than change all of the permission levels. To manage permissions for a Web application, in Central Administration, on the Application Management page, in the Application Security section, click User permissions for Web application.

If you need to make several changes to a particular permission level, it is better to create a custom permission level that includes all of the permissions you need.

You might want to create additional permission levels if any of the following applies:

 You want to exclude several permissions from a particular permission level.

 You want to define a unique set of permissions for a new permission level.

To create a permission level, you can copy an existing permission level and then make changes, or you can create a permission level and then select the permissions that you want to include.

note_ddNote:

Some permissions are dependent on other permissions. If you clear a permission that another permission depends on, the other permission is also cleared.

|  |
| --- |
| Worksheet action |
| Use the [Custom permission levels and groups worksheet](http://go.microsoft.com/fwlink/?LinkId=73134&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73134&clcid=0x409) to record any permission levels you want to customize or create. |

## Worksheet

Use the following worksheet to determine permission levels and groups to use:

 [Custom permission levels and groups worksheet](http://go.microsoft.com/fwlink/?LinkId=73134&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73134&clcid=0x409)

# Define custom permission levels [Office SharePoint Server]

In this article:

 [Customize an existing permission level](#DSDOC_section1c5dd8b7e_202d_4d33_8535_5c)

 [Copy an existing permission level](#DSDOC_section2c5dd8b7e_202d_4d33_8535_5c)

 [Create a permission level](#DSDOC_section3c5dd8b7e_202d_4d33_8535_5c)

After you have determined that you need custom permission levels and you have decided what permissions to include in the new permission level, you can create a custom permission level. Permission levels can be created for a site or site collection. You can create a custom permission level by using any of the three procedures in this article.

## Customize an existing permission level

If the custom permission level that you want is nearly identical to an existing default permission level and you don't need to use the default permission level, you can customize the default permission level to include or exclude permissions that you do or do not need.

1. On the Site Settings page, under Users and Permissions, click Advanced permissions.

2. On the toolbar, click Settings, and then click Permission Levels.

3. In the list of permission levels, click the name of the permission level you want to customize.

4. In the list of or permissions, select or clear the check boxes to add permissions to or remove permissions from the permission level.

5. Click Submit.

## Copy an existing permission level

If the custom permission level that you want is similar to an existing default permission level, and you need to use both the default permission level and your custom permission level, you can copy the default permission level, and then modify the copy and save it as a new permission level.

1. On the Site Settings page, under Users and Permissions, click Advanced permissions.

2. On the toolbar, click Settings, and then click Permission Levels.

3. In the list of permission levels, click the name of the permission level you want to copy.

4. At the bottom of the page, click Copy Permission Level.

5. On the Copy Permission Level page, in the Name box, type a name for the new permission level.

6. In the Description box, type a description for the new permission level.

7. In the list of permissions, select or clear the check boxes to add permissions to or remove permissions from the permission level.

8. Click Create.

## Create a permission level

If there is no permission level similar to the one you need, you can create one and include just the permissions that you need.

1. On the Site Settings page, under Users and Permissions, click Advanced permissions.

2. On the toolbar, click Settings, and then click Permission Levels.

3. On the toolbar, click Add a Permission Level.

4. On the Add a Permission Level page, in the Name box, type a name for the new permission level.

5. In the Description box, type a description for the new permission level.

6. In the list of permissions, select the check boxes to add permissions to the permission level.

7. Click Create.

# Choose which security groups to use [Office SharePoint Server]

In this article:

 [Determine which Windows security groups and accounts to use for granting access to sites](#DSDOC_section11a45c752_a485_439a_a19b_34)

 [Decide whether to use all authenticated users](#DSDOC_section21a45c752_a485_439a_a19b_34)

 [Decide whether to allow access to anonymous users](#DSDOC_section31a45c752_a485_439a_a19b_34)

 [Worksheet](#DSDOC_section41a45c752_a485_439a_a19b_34)

For easier user management, we recommend that you assign site permissions to groups rather than to individual users. In the Microsoft Active Directory directory service, the following two types of groups are commonly used to organize users:

 Distribution group   A group that is only used for e-mail distribution and that is not security-enabled. Distribution groups cannot be listed in discretionary access control lists (DACLs) used to define permissions on resources and objects.

 Security group   A group that can be listed in discretionary access control lists (DACLs) used to define permissions on resources and objects. A security group can also be used as an e-mail entity.

You can use security groups to control permissions for your site by directly adding the security group and granting the entire group permissions. You cannot use distribution groups in this way; however, you can expand a distribution list and add the individual users to a SharePoint group. If you use this method, you must manage the process of keeping the SharePoint group synchronized with the distribution group. If you use security groups, you do not need to manage the individual users in the SharePoint application. Because you included the security group itself and not the individual members of the group, Active Directory manages the users for you.

## Determine which Windows security groups and accounts to use for granting access to sites

Each organization sets up its Windows security groups differently. For easiest permission management, security groups should be:

 Large and stable enough that you aren't constantly adding additional groups to your SharePoint sites.

 Small enough that you can assign appropriate permissions.

For example, a security group called "all users in building 2" is probably not small enough to assign permissions, unless it happens that all users in building 2 have the same job function, such as accounts receivable clerks. This is rarely the case, so you should look for a smaller set of users, such as "accounts receivable" or some other smaller, highly-related group.

## Decide whether to use all authenticated users

If you want all users within your domain to be able to view content on your site, consider granting access to all authenticated users (the Domain Users Windows security group). This special group allows all members of your domain to access a Web site (at the permission level you choose), without your having to enable anonymous access.

## Decide whether to allow access to anonymous users

You can enable anonymous access to allow users to view pages anonymously. Most Internet Web sites allow anonymous viewing of the site, but might ask for authentication when someone wants to edit the site or buy an item on a shopping site. Anonymous access must be granted at the Web application level at the time that the Web application is created. If anonymous access is allowed for the Web application, then site administrators can decide whether to:

 Grant anonymous access to a site.

 Grant anonymous access only to lists and libraries.

 Block anonymous access to a site altogether.

Anonymous access relies on the anonymous user account on the Web server. This account is created and maintained by Microsoft Internet Information Services (IIS), not your SharePoint site. By default in IIS, the anonymous user account is IUSR\_ ComputerName. When you enable anonymous access, you are in effect granting that account access to the SharePoint site. Allowing access to a site, or to lists and libraries, grants the View Items permission to the anonymous user account. Even with the View Items permission, however, there are restrictions to what anonymous users can do. Anonymous users cannot:

 Use the Microsoft Office SharePoint Designer remote procedure call (RPC); in other words, they cannot open sites for editing in Office SharePoint Designer. They can also not use DAV (the Web Folders protocol in Windows); in other words, they cannot view the site in My Network Places.

 Upload or edit documents in document libraries, including wiki libraries.

important_ddImportant:

To create more secure sites, lists, or libraries, do not enable anonymous access. Enabling anonymous access allows users to contribute to lists, discussions, and surveys, possibly using up server disk space and other resources. Further, it allows anonymous users to discover site information, including user e-mail addresses and any content posted to lists, and libraries, and discussions.

You can also set permission policies for the anonymous user for different zones (Internet, Extranet, Intranet, Other), if you have the same Web application serving content in those different zones. The policies are described in the following list:

 None   No policy. This is the default option. No additional permission restrictions or additions are applied to site anonymous users.

 Read   Anonymous users can read content, unless the site administrator turns off anonymous access.

 Deny Write   Anonymous users cannot write content, even if the site administrator specifically attempts to grant the anonymous user account that permission.

 Deny All   Anonymous users cannot have any access, even if site administrators specifically attempt to grant the anonymous user account access to their sites.

## Worksheet

On the Site and content security worksheet (http://go.microsoft.com/fwlink/?LinkId=73135&clcid=0x409), list the security groups that you will use and the permission levels they will need at each level of your site hierarchy.

# Choose administrators and owners for the administration hierarchy (Office SharePoint Server)

In this article:

 [Levels of administration](#DSDOC_section1cf418db1_6212_4cd7_9383_83)

 [Worksheet](#DSDOC_section2cf418db1_6212_4cd7_9383_83)

Administration of Microsoft Office SharePoint Server 2007 occurs at many levels, such as on the server farm as a whole, on shared services, and on individual sites. Many people can be involved in managing Office SharePoint Server 2007.

## Levels of administration

Most levels of the server and site hierarchy have a corresponding administration group. Although the Web application level does not have a unique administrator group, farm administrators and service administrators have control over the Web applications within their scope. Members of the Farm Administrators group and members of the Administrators group on the local server can define a policy to grant individual users permissions at the Web application level. For more information about policy, see "Policy for Web applications" in the [Logical architecture elements](#DSDOC_aaed3a01_f4dc_4353_abda_0beced2080) article.

The groups of users who have administrative permissions at different levels are described in the following list:

 Server or server farm level

 Farm Administrators group   Members of the Farm Administrators group have permissions to and responsibility for all servers in the server farm. Members can perform all administrative tasks in Central Administration for the server or server farm. Members of this group can also perform command-line operations. This group does not have access to individual sites or their content. However, members can take ownership of a specific site collection if need be (for example, if the administrator of a site leaves the organization and a new administrator must be added).

 Administrators group   Members of the Administrators group on the local server can perform all farm administrator actions and more, including installing new products or applications, deploying Web Parts and new features to the global assembly cache, creating new Web applications and new Internet Information Services (IIS) Web sites, and starting services. Like farm administrators, members of this group on the local server have no access to site content, by default.

note_ddNote:

Farm administrators and administrators can also take ownership of specific site collections, if needed. To take ownership, they can add themselves as the site collection administrator by using the Site Collection Administrators page in Central Administration.

 Shared services level

 SSP administrators   Can control which services are included in a Shared Services Provider (SSP) and configure settings for those services.

 Service administrators   Can configure settings for a specific service within an SSP. For example, the service administrator for the Search service on Service1 can configure search settings for Service1.

 Site level

 Site collection administrators   Have the Full Control permission level on all Web sites within a site collection. This means that they have access to content in all sites in that site collection, even if they do not have explicit permissions on that site.

 Site owners   By default, members of the Owners group for a site have the Full Control permission level on that site. They can perform administration tasks for the site, and for any list or library within that site.

|  |
| --- |
| Worksheet action |
| Use the [Administrators and owners worksheet](http://go.microsoft.com/fwlink/?LinkId=73126&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73126&clcid=0x409) to record which administrators to assign to each level. Refer to your site hierarchy diagram to be sure you assign owners for each site collection, top-level Web site, and subsite that you are planning. |

## Worksheet

Use the following worksheet to choose administrators and owners for the administration hierarchy:

 [Administrators and owners worksheet](http://go.microsoft.com/fwlink/?LinkId=73126&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73126&clcid=0x409)

# Plan for InfoPath Forms Services security [Office SharePoint Server]

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# XII Plan for site creation and maintenance

In this chapter:

 [Chapter overview: Plan for site creation and maintenance [Office SharePoint Server]](#DSDOC_58d809cc_8e03_4075_9050_638c976840)

 [Plan process for creating sites [Office SharePoint Server]](#DSDOC_f7b617fc_cc45_41bf_bb71_f3d49ed4a5)

 [Plan for site maintenance and management [Office SharePoint Server]](#DSDOC_4fdf96bd_813f_4499_b7d2_958b7bce00)

# Chapter overview: Plan for site creation and maintenance [Office SharePoint Server]

If you plan on having more than a few site collections in your Microsoft Office SharePoint Server 2007 environment, you need to be sure that you have a plan for site creation and maintenance. Without such a plan, it is difficult to control or track when SharePoint sites are created, whether sites are still active, and when you can safely remove inactive sites. Before you deploy and make sites available to users, you need to answer questions such as:

 Do you want to tightly control site creation or to allow many users to create sites?

 At which level in the site hierarchy should additional sites be created?

 How do you find and remove unused sites in your environment?

The articles and worksheets in this chapter help you design and record a plan for site creation and maintenance. This will help you be prepared to manage growth in your environment.

Plan for site creation and maintenance by using the following articles:

 [Plan process for creating sites [Office SharePoint Server]](#DSDOC_f7b617fc_cc45_41bf_bb71_f3d49ed4a5) helps you determine which type of site creation process will fit your organization, and which method to use to implement that process.

 [Plan for site maintenance and management [Office SharePoint Server]](#DSDOC_4fdf96bd_813f_4499_b7d2_958b7bce00) helps you to plan for maintaining your SharePoint sites from the beginning to ensure your sites stay current, useful, and usable.

# Plan process for creating sites [Office SharePoint Server]

In this article:

 [Determine who can create sites and a method for site creation](#DSDOC_section1f7b617fc_cc45_41bf_bb71_f3)

 [Plan for Self-Service Site Management](#DSDOC_section2f7b617fc_cc45_41bf_bb71_f3)

 [Plan for custom site creation processes](#DSDOC_section3f7b617fc_cc45_41bf_bb71_f3)

 [Worksheet](#DSDOC_section4f7b617fc_cc45_41bf_bb71_f3)

Some organizations need to maintain tight control over who can create sites, or when sites are created. Other organizations can allow users more access and freedom to create sites when needed. This article helps you determine which type of site creation process will fit your organization, and which method to use to implement that process.

## Determine who can create sites and a method for site creation

By default, new site collections (and therefore new top-level Web sites) can only be created by using Central Administration, which means that they can only be created by members of the Farm Administrators group. This behavior might suit your organization if you want your environment to be tightly controlled and managed, with only a few people allowed to add top-level sites. However, the default top-level site creation method might not suit your organization if you have any of the following requirements:

 You want users to be able to easily create informal, perhaps even disposable, top-level sites, such as for short-term projects.

 You want to create an informal space for team, group, or community interaction.

 You are hosting top-level sites (either internally or externally) and want the process for requesting and receiving a top-level site to be as quick and low cost as possible.

There are several ways to allow users to create their own sites, while still maintaining some control over your environment. Consider which of the following methods will work best for your organization.

 Self-Service Site Management   In Central Administration, you can turn on Self-Service Site Management to allow users to create site collections under the /sites path (or other path you specify) within a particular Web application. This method is best used when you want to allow groups or communities to create sites. This method also works well if you are hosting sites and want to allow users to create sites without waiting for a complicated process. The sign-up page for Self-Service Site Management can be customized or replaced with a page that includes all of the information you might need to integrate with a billing system or to track custom metadata about the site at creation time. This method does not work well when large numbers of users need access to multiple sites. Because Self-Service Site Management creates site collections, which have separate permissions, users need to be added uniquely to different site collections. If you use subsites instead, the users can be inherited from the parent site in the site collection.

 Subsites of existing sites   Limit users to creating subsites of existing sites, rather than new site collections and top-level sites. Any user who has the Full Control or Hierarchy Manager permission level on an existing site can create a subsite. This method is the most limited, because you still control how many site collections there are. Because the sites are always subsites of other sites, they can either be easy to organize (if there are just a few) or very difficult to organize and browse (for example, if everyone in your organization wants a subsite and they create them at different levels in the site collection's hierarchy, the site collection can soon become very difficult to navigate).

note_ddNote:

If you do not want users to have this capability, you can remove the Create Subsites right from the Full Control and Hierarchy Manager permission levels, either at the site collection or Web application level.

 Personal sites   Allow users to create personal sites (also known as My Sites). Personal sites are site collections stored under the /personal path of the Web application. Personal sites are created for individual users, so they are not the appropriate method to use if you are trying to create sites for groups or communities. For more information about personal sites, see [Plan My Sites](#DSDOC_4edf74cf_8808_4277_ba10_b1f925d7c4).

note_ddNote:

Keep in mind that none of these methods can control how much space each site takes up in your content databases. To control site sizes, you should use quotas and set a size limit for site collections. You cannot set individual size limits for subsites. For more information, see [Plan for site maintenance and management [Office SharePoint Server]](#DSDOC_4fdf96bd_813f_4499_b7d2_958b7bce00).

## Plan for Self-Service Site Management

Self-Service Site Management allows users to create and manage their own top-level Web sites automatically. When you turn on Self-Service Site Management for a Web application, users can create their own top-level Web sites under a specific path (by default, the /sites path). When turned on, this capability advertises itself with an announcement added to the top-level site at the root path of the Web application, so any users who have permission to view that announcement can follow the link.

note_ddNote:

If you want to use a path other than /sites for Self-Service Site Management, you must add the path as a wildcard inclusion. For more information, see [Plan for collaboration sites](#DSDOC_437a9043_e55b_4b52_b578_dd3fdee340).

This capability can obviously affect the security for your Web server. Self-Service Site Management is disabled by default — you must turn on the feature to use it. You enable Self-Service Site Management for a single Web application at a time. If you want to use it on all Web applications in your server farm, you must enable it for every Web application individually.

If you enable Self-Service Site Management, you should consider the following:

 Generally you should require a secondary site collection administrator. Administrative alerts, such as those for when quotas are exceeded, or checking for unused Web sites, go to the primary and secondary administrators. Having more than one contact reduces administrator involvement with these sites.

 Define a storage quota and set it as the default quota for the Web application.

 Review the number of sites allowed per content database. Combined with quotas, this will help you limit the size of the databases in your system.

 Enable unused Web site notifications, so that sites that are forgotten or no longer of value can be identified.

Because Self-Service Site Management creates new top-level Web sites on an existing Web application, any new sites automatically conform to the Web application's default quota settings, unused Web site notification settings, and other administrative policies.

|  |
| --- |
| Worksheet action |
| Use the [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) to record your decisions about using Self-Service Site Management. |

## Plan for custom site creation processes

You can, of course, create your own process for site creation by using a custom form to request a site that integrates with a back-end billing system to charge a customer's credit card or a corporate cost center. If you have a complicated system or process that you want to include as part of site creation, you should create a custom application to call the site creation interface and perform any other tasks you require. However, if you simply want to add a few custom fields to the site creation page (for example, to track which department in your company is requesting a particular site), you should consider using Self-Service Site Management and customize the sign-up page to include the information that you need. You can customize the scsignup.aspx page in the site definition to include the metadata that you need without having to develop an entire application.

|  |
| --- |
| Worksheet action |
| Use the [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) to plan your site creation process. |

For more information about building custom applications or editing pages in a site definition, see the [Office SharePoint Server 2007: Software Development Kit](http://go.microsoft.com/fwlink/?LinkId=72208) (http://go.microsoft.com/fwlink/?LinkId=72208).

## Worksheet

Use the following worksheet to plan the process for creating sites:

 [Site creation worksheet](http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73138&clcid=0x409)

# Plan for site maintenance and management [Office SharePoint Server]

In this article:

 [Plan for site maintenance](#DSDOC_section14fdf96bd_813f_4499_b7d2_95)

 [Plan for managing site collections](#DSDOC_section24fdf96bd_813f_4499_b7d2_95)

 [Worksheet](#DSDOC_section34fdf96bd_813f_4499_b7d2_95)

All Web sites, particularly sites that have more than one author, get cluttered. Periodic review and cleanup can help keep your site functioning well, whether your site is large or small. If you build a plan for maintaining your site or sites from the beginning, you can ensure that they stay current, useful, and usable.

## Plan for site maintenance

Your site maintenance plan will be different than that for any other environment, and it will contain different elements. Site maintenance is different for sites managed by an IT department than it is for user-created sites and managed sites. However, some best practices for a site maintenance plan include:

 Ask users what they want in IT-managed sites. Perform periodic surveys to determine what your users need from the site.

 Use usage logs and reports to find out which areas of the site are being used, and then correlate that with user surveys to find out what can be improved.

 Archive obsolete content or sites. However, if you are going to archive or delete obsolete content or sites, be sure that users understand that plan, and that you perform these actions only at predictable times. For example, publish a schedule of when you are going to archive content or delete unused sites.

 Periodically review site permissions. For example, review the permissions quarterly to remove permissions for any users who have left the group or project.

 Select a reasonable time interval for your maintenance activities. For example, if you plan to conduct periodic user surveys, do not conduct them more than twice a year (and preferably, no more than once a year).

 Create a plan for regular backups of site content. Determine or discover how often backups will be made, and the process for restoring content when necessary. For more information about planning for backup and restore, see [Plan for backup and restore [Office SharePoint Server]](#DSDOC_054c3d6d_a0d3_448a_864b_93db6283d7).

Start now, during your planning process, to create a plan for site maintenance. Record your plan, including how often to tune up the site and archive content. Get your plan reviewed by members of your team and representatives of your user base. This way, you can identify any concerns that users might have now, determine how best to address these concerns, and have a plan for site maintenance in place by the time your site goes live.

|  |
| --- |
| Worksheet action |
| Use the [Site maintenance worksheet](http://go.microsoft.com/fwlink/?LinkID=73146&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73146&clcid=0x409) to create a site maintenance plan. |

## Plan for managing site collections

One part of your site maintenance plan should be a plan for how to manage the size and number of site collections in your environment. This is most important if you are allowing Self-Service Site Management. Most organizations want to be able to predict and control how much growth they can expect from sites because of the impact that they can have on database resources. For example, if a particular content database contains 100 sites, and one of those sites is taking up more than 50 percent of the space, then that site might need to be in its own content database. This will ensure that you preserve some room for additional growth, while maintaining the ability to back up and restore the databases.

Two methods for managing site collections are:

 Site collection quotas   Use this method to control how large site collections can become.

 Site use confirmation and deletion   Use this method to monitor and remove unused site collections.

### Plan site collection quotas

Use quotas to track and limit site storage. You can send a warning e-mail message to site owners when site storage reaches a particular size (in megabytes), and then lock the site to further content when site storage reaches a maximum size. When you perform your database and server capacity planning, determine what size limits (if any) you want to enforce. To take the best advantage of quotas:

 Create different quota templates for different site types. For example, you might want different quotas for different divisions, or for different customer types, or for different paths (perhaps sites under the /sites path only get 100 MB per site collection, whereas sites under the /vip path can take up to 300 MB per site collection). Whenever you create a site collection from Central Administration, you can specify on which quota template it is based. Note that sites created by using Self-Service Site Management use the default quota for the Web application.

 Give enough room for reasonable growth in sites. Depending on what each site is used for, storage space needs can vary dramatically. Sites are designed to grow over time as they are used. A quota limit of 50 MB is unlikely to be enough storage space to start with for most sites, and is unlikely to be anywhere near enough for a site that has a long life.

 Allow for reasonable notice between the warning e-mail message and locking the site for exceeding its quota. For example, do not set the warning limit to 80 MB and the site storage limit to 85 MB. If users are in the middle of uploading several large files, they will not be happy if blocked from completing that task with very little notice.

|  |
| --- |
| Worksheet action |
| Use the [Site maintenance worksheet](http://go.microsoft.com/fwlink/?LinkID=73146&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73146&clcid=0x409) to record your decisions about using site collection quotas. |

### Plan site use confirmation and deletion

You need to plan how to handle sites that become inactive after a project has ended, or sites that users created just to test out some ideas, and then abandoned. Site use confirmation and deletion can help you keep your environment cleaner, by helping you identify when sites are no longer needed. This feature works by automatically sending an e-mail message to site owners to see if they consider their site active. If the owner does not respond to the e-mail message (after a specified number of messages over a specified length of time), the site can be deleted.

To plan for site use confirmation and deletion, decide:

 How long you want to wait before checking to see if a site is inactive. The default length of time for team or project sites is 90 days after site creation, but you should probably give owners longer than that. For a test or personal site, 90 days is probably too long. Usually a site that was created, was actively used, and is now ready to be deleted or archived, took at least six months and probably a few years to complete that life cycle. Reminders every six months are valuable for those situations.

 How often you want to send an e-mail message to site owners to see if their sites are inactive. After the first e-mail message, if the site administrator does not respond, you can continue with additional notices at daily, weekly, or monthly intervals.

 Whether you want to automatically delete unused sites. If the site administrator does not respond to multiple e-mail messages, do you want to go ahead and delete the site automatically? It is recommended that you make a backup first. You can do so by making sure that regular backups are performed and you can use the [Office SharePoint Server 2007: Software Development Kit](http://go.microsoft.com/fwlink/?LinkID=72208&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=72208&clcid=0x409) to customize this functionality so that it automatically makes a backup of the site before deletion, but this is not default behavior.

 If you are going to automatically delete unused sites, how many e-mail messages will you send to site owners before you do so. By default, four weekly notices are sent before site deletion, but you can increase or decrease this number to suit your needs.

|  |
| --- |
| Worksheet action |
| Use the [Site maintenance worksheet](http://go.microsoft.com/fwlink/?LinkID=73146&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73146&clcid=0x409) to record your decisions about site use confirmation and deletion. |

## Worksheet

Use the following worksheet to plan for site maintenance and management:

 [Site maintenance worksheet](http://go.microsoft.com/fwlink/?LinkID=73146&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73146&clcid=0x409)

# XIII Plan for system requirements

Insert introduction here.

## Subhead

Insert section body here.

### Subhead

Insert section body here.

# Determine hardware and software requirements (Office SharePoint Server)

In this article:

 [About hardware and software requirements](#DSDOC_section14d88c402_24f2_449b_86a6_6e)

 [Stand-alone installation](#DSDOC_section24d88c402_24f2_449b_86a6_6e)

 [Server farm installation](#DSDOC_section34d88c402_24f2_449b_86a6_6e)

This article describes the hardware and software requirements for installing Microsoft Office SharePoint Server 2007.

## About hardware and software requirements

An installation of Office SharePoint Server 2007 can range from a single computer (stand-alone installation) to many computers (server farm). The requirements for your installation will depend on the availability and scale requirements for your solution. This article describes the minimum and recommended hardware requirements based on whether you are deploying a stand-alone installation or a server farm. This article also lists the software prerequisites for installing Office SharePoint Server 2007.

This article does not provide guidance about choosing a farm topology or hardware based on availability requirements or performance and capacity requirements. For more information about designing your solution to address these requirements, see [Plan for availability (Office SharePoint Server)](#DSDOC_9ccfb27f_ecba_4b7d_b9a0_88fac71478).

The hardware and software requirements described in this article apply to both x32-bit–based and x64-bit–based systems.

note_ddNote:

Itanium-based systems are not supported.

## Stand-alone installation

You can install Office SharePoint Server 2007 on a single computer by using either of the following methods:

 By selecting Basic.

 By selecting Advanced, and then selecting Stand-alone in Office SharePoint Server 2007 Setup.

### Hardware requirements

The following table lists the minimum and recommended hardware requirements for deploying Office SharePoint Server 2007, including the deployment of Microsoft SQL Server 2005 Express Edition, for a stand-alone installation.

|  |  |  |
| --- | --- | --- |
| Component | Minimum | Recommended |
| Processor | 2.5 gigahertz (GHz) | Dual processors that are each 3 GHz or faster |
| RAM | 1 gigabyte (GB) | 2 GB |
| Disk | NTFS file system–formatted partition with a minimum of 3 GB of free space | NTFS file system–formatted partition with 3 GB of free space plus adequate free space for your Web sites |
| Drive | DVD drive | DVD drive or the source copied to a local or network-accessible drive |
| Display | 1024 × 768 | 1024 × 768 or higher resolution monitor |
| Network | 56 kilobits per second (Kbps) connection between client computers and server | 56 Kbps or faster connection between client computers and server |

### Software requirements

Because Office SharePoint Server 2007 is built on Microsoft Windows SharePoint Services 3.0, the requirements that apply to Windows SharePoint Services 3.0 also apply to Office SharePoint Server 2007.

note_ddNote:

Because the Office SharePoint Server 2007 installation and configuration wizard marshals many components, if you uninstall Office SharePoint Server 2007, and then later install Office SharePoint Server 2007 on the same computer, the Setup program could fail when creating the configuration database, which would cause the entire installation process to fail. You can prevent this failure by deleting the existing configuration database or by using the psconfig command to create a new configuration database.

2007 Microsoft Office system uses a common installer, and the features that are available in your Office SharePoint Server 2007 installation depend on the product identification (PID) key that you specify during installation. This means that even with the same installation source, if you specify a different PID key (for example, a PID key for a different Office SharePoint Server 2007 edition), a different feature set will be available for installation.

#### Database

When you perform a Basic installation, SQL Server 2005 Express Edition is automatically installed. When you perform an Advanced installation on a stand-alone computer that already has Microsoft SQL Server installed, ensure that the computer meets the hardware and software requirements for a database server. For more information, see [Database server](#DSDOC_subsection14d88c402_24f2_449b_86a6) later in this article.

Because of Windows licensing restrictions, if you are using Windows Server 2003, Web Edition in a single server environment, you can only perform a Basic installation. This is because the full SQL Server editions cannot be installed on Windows Server 2003, Web Edition. However, you can install SQL Server 2005 Express Edition or SQL Server 2000 Desktop Engine (Windows) (WMSDE).

#### Operating system

Office SharePoint Server 2007 runs on Windows Server 2003 with SP1 or later. We recommend that you apply all critical updates. You can use the following Windows Server 2003 editions:

 Windows Server 2003, Standard Edition

 Windows Server 2003, Enterprise Edition

 Windows Server 2003, Datacenter Edition

 Windows Server 2003, Web Edition

Because of Windows licensing restrictions, if you are using Windows Server 2003, Web Edition in a single server environment, you can only perform a Basic installation. This is because the full SQL Server editions cannot be installed on Windows Server 2003, Web Edition. However, you can install SQL Server 2005 Express Edition or SQL Server 2000 Desktop Engine (Windows) (WMSDE).

Office SharePoint Server 2007 administration functions require Microsoft Internet Explorer 6.0 with the most recent service packs or Internet Explorer 7.0.

#### Windows components

After you have installed the operating system and applied all critical updates, you must configure the computer to be a Web server by enabling Internet Information Services (IIS) 6.0, including:

 Common files

 WWW

 Simple Mail Transfer Protocol (SMTP)

You must configure the server to use IIS 6.0 worker process isolation mode. This is the default setting in new installations. However, if you have upgraded from IIS 5.0 on Windows Server 2000, Run WWW in IIS 5.0 isolation mode is enabled, and you must change this setting to use IIS 6.0 worker process isolation mode.

To enable e-mail notifications, you need to configure incoming and outgoing e-mail settings. To configure sending e-mail alerts and notifications, you must specify an SMTP e-mail server. To configure your installation so that your SharePoint sites can accept and archive incoming e-mail, you must install the IIS SMTP service.

#### Microsoft .NET Framework 3.0

Before installing Office SharePoint Server 2007, you must install the Microsoft .NET Framework 3.0 and then ensure that ASP.NET 2.0 is enabled.

To enable ASP.NET v2.0.50727, open the Web service extension in the IIS snap-in on the Microsoft Management Console (MMC). If ASP.NET 2.0 is installed on the computer before IIS is enabled, you must enable ASP.NET 2.0 by running the command aspnet\_regiis -i.

## Server farm installation

The primary difference between a single server and a server farm topology is that you can use one or more computers to host the following server roles:

 Application server

 Front-end Web server

 Database server

This section describes the minimum and recommended system requirements for each server role. If you install more than one role on a single computer, ensure that the computer meets the minimum requirements for all server roles.

### Application server

#### Hardware requirements

The following table lists the minimum and recommended hardware requirements for deploying an Office SharePoint Server 2007 application server.

|  |  |  |
| --- | --- | --- |
| Component | Minimum | Recommended |
| Processor | 2.5 GHz | Dual processors that are each faster than 2.5 GHz |
| RAM | 2 GB | 4 GB |
| Disk | NTFS file system–formatted partition with a minimum of 3 GB of free space | NTFS file system–formatted partition with 3 GB of free space plus adequate free space for your data storage requirements |
| Drive | DVD drive | DVD drive or the source copied to a local or network-accessible drive |
| Display | 1024 × 768 | 1024 × 768 or higher resolution monitor |
| Network |  56 Kbps connection between client computers and server   For connections between computers in your server farm, 100 megabits per second (Mbps) connection |  56 Kbps or faster connection between client computers and server   For connections between computers in your server farm, 1 gigabit per second (Gbps) connection |

#### Software requirements

Because Office SharePoint Server 2007 is built on Windows SharePoint Services 3.0, the requirements that apply to Windows SharePoint Services 3.0 also apply to Office SharePoint Server 2007.

We recommend that you install Office SharePoint Server 2007 on a computer that has a new installation of Windows Server 2003 with SP1 or later and all critical updates.

2007 Microsoft Office system uses a common installer, and the features that are available in your Office SharePoint Server 2007 installation depend on the PID that you specify during installation. This means that even with the same installation source, if you specify a different PID key (for example, a PID key for a different Office SharePoint Server 2007 edition), a different feature set will be available for installation.

##### Operating system

Office SharePoint Server 2007 runs on Windows Server 2003 with SP1 or later. We recommend that you apply all critical updates. You can use the following Windows Server 2003 editions:

 Windows Server 2003, Standard Edition

 Windows Server 2003, Enterprise Edition

 Windows Server 2003, Datacenter Edition

 Windows Server 2003, Web Edition

Office SharePoint Server 2007 administration functions require Internet Explorer 6.0 with the most recent service packs or Internet Explorer 7.0.

##### Windows components

After you have installed the operating system and applied all critical updates, you must configure the computer to be a Web server by enabling IIS 6.0, including:

 Common files

 WWW

 SMTP

You must configure the server to use IIS 6.0 worker process isolation mode. This is the default setting in new installations. However, if you have upgraded from IIS 5.0 on Windows Server 2000, Run WWW in IIS 5.0 isolation mode is enabled, and you must change this setting to use IIS 6.0 worker process isolation mode.

To enable e-mail notifications, you need to configure incoming and outgoing e-mail settings. To configure sending e-mail alerts and notifications, you must specify an SMTP e-mail server. To configure your installation so that your SharePoint sites can accept and archive incoming e-mail, you must install the IIS SMTP service.

##### Microsoft .NET Framework 3.0

After you have configured the server as a Web server, you must install the Microsoft .NET Framework 3.0 and then ensure that ASP.NET 2.0 is enabled.

To enable ASP.NET v2.0.50727, open the Web service extension in the IIS snap-in on the MMC. If ASP.NET 2.0 is installed on the computer before IIS is enabled, you must enable ASP.NET 2.0 by running the command aspnet\_regiis -i.

### Front-end Web server

#### Hardware requirements

The following table lists the minimum and recommended hardware requirements for deploying an Office SharePoint Server 2007 front-end Web server.

|  |  |  |
| --- | --- | --- |
| Component | Minimum | Recommended |
| Processor | 2.5 GHz | Dual processors that are each 3 GHz or faster |
| RAM | 2 GB | More than 2 GB |
| Disk | NTFS file system–formatted partition with a minimum of 3 GB of free space | NTFS file system–formatted partition with 3 GB of free space plus adequate free space for your data storage requirements |
| Drive | DVD drive | DVD drive or the source copied to a local or network-accessible drive |
| Display | 1024 × 768 | 1024 × 768 or higher resolution monitor |
| Network |  56 Kbps connection between client computers and server   For connections between computers in your server farm, 100 Mbps connection |  56 Kbps or faster connection between client computers and server   For connections between computers in your server farm, 1 Gbps connection |

#### Software requirements

Because a front-end Web server is a subset of an application server, all features on a front-end Web server are available on an application server. The software requirements for the front-end Web server are the same as the software requirements for the application server before you add specific resources to meet the demands that you forecast as a result of your capacity planning phase.

### Database server

The computer that hosts the database server role must have SQL Server 2000 with SP3a or later or Microsoft SQL Server 2005 SP1 or later. Some advanced features required SQL Server 2005 Analysis Services SP1 or later. For information about the hardware and software required to deploy a database server, see [SQL Server 2005 System Requirements](http://go.microsoft.com/fwlink/?LinkID=75010&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=75010&clcid=0x409).

Because of Windows licensing restrictions, if you are using Windows Server 2003, Web Edition in a single server environment, you can only perform a Basic installation. This is because the full SQL Server editions cannot be installed on Windows Server 2003, Web Edition. However, you can install SQL Server 2005 Express Edition or SQL Server 2000 Desktop Engine (Windows) (WMSDE).

# Plan browser support (Office SharePoint Server)

In this article:

 [About browser support](#DSDOC_section1ff6c5b8c_59bd_4079_8f0b_de)

 [Levels of browser support](#DSDOC_section2ff6c5b8c_59bd_4079_8f0b_de)

## About browser support

Microsoft Office SharePoint Server 2007 supports several Web browsers that are commonly used. However, there are certain browsers that might cause some Office SharePoint Server 2007 functionality to be downgraded, limited, or available only through alternative code. In some cases, functionality might be unavailable for noncritical administrative tasks.

As part of planning your deployment of Office SharePoint Server 2007, we recommend that you review the browsers used in your organization to ensure optimal performance with Office SharePoint Server 2007.

## Levels of browser support

Web browser support is divided into two levels: level 1 and level 2. Although administrative tasks on SharePoint sites are optimized for level 1 browsers, Office SharePoint Server 2007 also provides rendering support for other browsers that are commonly used. To ensure that you have complete access to all the functionality, we recommend that you use a level 1 browser for administrative tasks.

### Level 1 Web browsers

Level 1 Web browsers take advantage of advanced features provided by ActiveX controls and provide the most complete user experience. Level 1 browsers offer full functionality on all SharePoint sites, including the Central Administration Web site. Level 1 browsers are listed in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| Browser | Windows | Linux/Unix | Macintosh OSX |
| Microsoft Internet Explorer 6.x (32-bit) | X |  |  |
| Windows Internet Explorer 7.x (32-bit) | X |  |  |

### Level 2 Web browsers

Level 2 Web browsers provide basic functionality, so that users can both read and write in SharePoint sites and perform site administration. However, because ActiveX controls are supported only in level 1 browsers and due to the functionality differences within different browsers, a different user experience might be provided and there could be some variances from the user experience from the level 1 browsers. Level 2 browsers are listed in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| Browser | Windows | Linux/Unix | Macintosh OSX |
| Firefox 1.5 | X | X | X |
| Mozilla 1.7 | X |  |  |
| Netscape Navigator 7.2 |  | X |  |
| Netscape Navigator 8.1 | X |  |  |
| Safari 2.0 |  |  | X |

If a browser is not listed in either level 1 or level 2, it is not supported. For example, older browsers — such as Internet Explorer 5.01, Internet Explorer 5.5x, Internet Explorer for Macintosh, and versions of third-party Web browsers that are earlier than the ones listed as level 2 browsers — are not supported.

# XIV Design server farms and topologies

In this chapter:

 [Chapter overview: Design server farms and topologies [Office SharePoint Server]](#DSDOC_b474b3dd_b1e3_4d3e_a83c_bc4a6ec4e0)

 Plan server farms

 [Design extranet farm topology [Office SharePoint Server]](#DSDOC_fce67a2a_9a1e_41c2_b0e8_9422c9d5d8)

 [Plan for geographically distributed sites](#DSDOC_72f6f297_1cf0_4dde_98d9_7ec7e79a9d)

 [Design content deployment topology](#DSDOC_1d6d6040_6cbb_4685_a40e_1e9086d426)

 [Design document conversions topology](#DSDOC_f7d7b652_10cc_4c99_8c05_0cc4341d4d)

 [Chart the farms within and across your networks](#DSDOC_ece85813_f5b2_419a_b5f4_fcade5a3e7)

 Chart relationships between farms

 [Plan for availability (Office SharePoint Server)](#DSDOC_9ccfb27f_ecba_4b7d_b9a0_88fac71478)

 [Determine hardware and software requirements (Office SharePoint Server)](#DSDOC_4d88c402_24f2_449b_86a6_6e7afcfec0)

 [Plan browser support (Office SharePoint Server)](#DSDOC_ff6c5b8c_59bd_4079_8f0b_de4f8b4e0a)

# Chapter overview: Design server farms and topologies [Office SharePoint Server]

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

In this article:



# Design extranet farm topology [Office SharePoint Server]

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Design content deployment topology

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

Content deployment copies content from a source Microsoft Office SharePoint Server 2007 site collection to a destination site collection, either based on a schedule or manually. This article describes elements of topologies designed for content deployment and illustrates typical content deployment topologies. For an overview of content deployment using Office SharePoint Server 2007, see [Plan content deployment](#DSDOC_edcdacca_8013_460e_95a0_d2b83b6cc7).

In this article:

 [Elements of content deployment topologies](#DSDOC_section11d6d6040_6cbb_4685_a40e_1e)

 [Typical content deployment topologies](#DSDOC_section21d6d6040_6cbb_4685_a40e_1e)

## Elements of content deployment topologies

Most content deployment topologies include two or more server farms, to separate the authoring environment from the production environment. A server farm used in content deployment can have one of the following purposes:

 Authoring   The farm contains the site collection that is used by the content-creating team to write the content.

 Production   The farm contains the site collection that presents the content to its intended audience, and it usually has tightened security.

 Staging   The farm contains a site collection that is a copy of the production site collection, so that the content can be reviewed and tested before it is published.

On any farm that exports content, you must specify a single front-end server as the export server. Similarly, on any farm that imports content, you must specify a single front-end server as the import server.

Content deployment packages are implemented as cabinet (CAB) files divided, by default, into 10-MB chunks, which are collected in a temporary location on the export server. After all the CAB files have been created and moved to the temporary directory on the export server, the content deployment job is initiated. After all the CAB files are received on the import server, the deployed content is copied to the destination Web sites.

Both the export and the import front-end servers must have sufficient disk space to hold the full set of CAB files for the largest content deployment job that could run. CAB files are removed from the temporary directory on the export server after all of them have been successfully sent to the destination farm. CAB files are removed from the temporary directory on the import server after the site content has been successfully deployed to the destination sites.

## Typical content deployment topologies

This section illustrates common content deployment topologies.

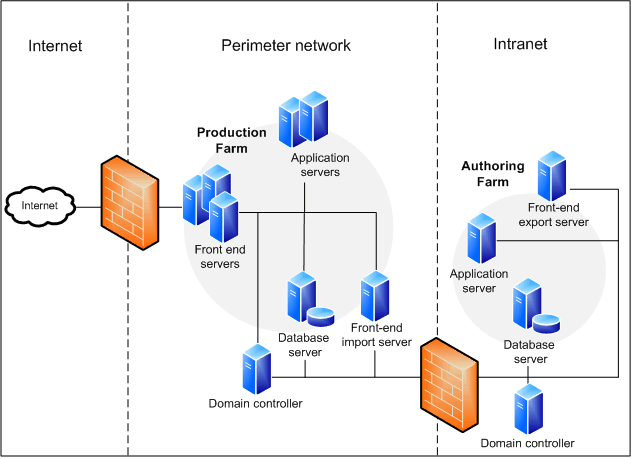
### Standard Internet site topology

The standard Internet site topology is typical of topologies used to publish an Internet site, such as a corporation's Internet presence site or a news organization's online news site. It includes two server farms: one to host the production site collection, and the other to host the authoring site collection along with other sites used by the authoring team. Users of the production server farm belong to a separate Active Directory® directory service domain, and some production farm users may be anonymous.

One front-end Web server in the production farm must be configured to import content from the authoring farm. Optionally, this server can be used to only import content.

The authoring server farm contains the site collection used to author the site's content. A front-end Web server in the authoring farm must be configured to export content from the authoring site collection to the production farm.

Often in this topology, the production farm is hosted in a perimeter network protected by outer and inner firewalls to increase security. For more information about deploying a perimeter configuration, see [Design extranet farm topology [Office SharePoint Server]](#DSDOC_fce67a2a_9a1e_41c2_b0e8_9422c9d5d8).



Variations on this topology include:

 Single authoring farm publishing to multiple production farms   In this variation, multiple farms are deployed in the perimeter network. Each production farm may have the same content, or sites may vary from farm to farm. This topology can be configured in multiple ways:

 The authoring farm can deploy to all of the production farms.

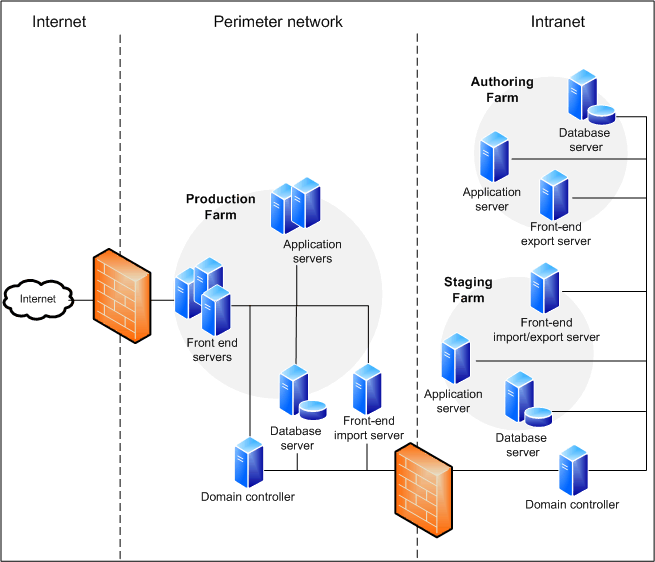
 The authoring farm can deploy to one production farm; by using content deployment, that production farm can then deploy to the other production farms.

 Multiple authoring farms publishing to a single production farm   Different authoring teams, each working on their own authoring farm, may work on separate site collections that are published to a single production farm.

### Three-stage topology

In some solutions, a three-stage topology is deployed, including an authoring farm, a staging farm, and a production farm. The staging farm is used to test or review the content before it is published to the production farm.

In a three-stage content deployment topology, the authoring farm deploys to the staging farm, so a front-end Web server in the authoring farm must be configured to export content. A front-end server in the staging farm must be configured to import and export content. A front-end server in the production farm must be configured to import content from the staging farm.



### Single-farm topology

Content deployment can be configured within a single server farm. In this topology, authors work in one site collection and deploy to a duplicate publishing site collection on the same farm. The site collections are in separate Web applications, and they use separate databases on the same computer running Microsoft® SQL Server™. Security is managed by granting users permissions to the content rather than by using separate Active Directory domains.

## [[20]](#footnote-21)#See Also

[Plan content deployment](#DSDOC_edcdacca_8013_460e_95a0_d2b83b6cc7)

# Plan for geographically distributed sites

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Design document conversions topology

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

In this article:

 [About document conversions](#DSDOC_section1f7d7b652_10cc_4c99_8c05_0c)

 [Typical document conversion topologies](#DSDOC_section2f7d7b652_10cc_4c99_8c05_0c)

 [Configuring document conversions in a server farm](#DSDOC_section3f7d7b652_10cc_4c99_8c05_0c)

 [Planning topologies for document conversions](#DSDOC_section4f7d7b652_10cc_4c99_8c05_0c)

Microsoft Office SharePoint Server 2007 supports installing document converters on the server that let users transform documents from one format to another. Conversions can be run either from the user interface or programmatically, such as from a custom workflow. The relationship between a source document and its transformed counterpart is maintained.

Along with providing the infrastructure on the server to install and run document converters, Office SharePoint Server 2007 includes a Document Conversions Load Balancer Service that you can configure to optimize the use of your server resources. Deploying document conversions includes tuning your server farm to optimally balance the load as documents are transformed.

## About document conversions

A document converter is a program that takes a document of one file type and generates a copy of that file in another file type. Office SharePoint Server 2007 includes converters for transforming documents into Web pages. For example, Office SharePoint Server 2007 includes the From Word Document to Web Page converter that transforms documents based on Microsoft Office Word 2007 into Web pages. Office SharePoint Server 2007 also includes an extensible framework for you to enable your own custom document converters. For details about creating and deploying custom converters, see the Office SharePoint Server 2007 [Software Development Kit](http://go.microsoft.com/fwlink/?LinkId=71218&clcid=0x409).

You can make a document converter available to users in two ways:

 Make it available from all document libraries on the server.

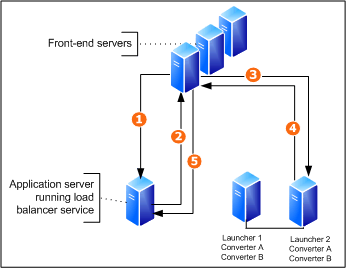
 Associate it with a content type and then associate that content type with a document library. Users can then convert documents of that content type by using the Convert Document command. For more information about content types, see [Plan content types [Office SharePoint Server]](#DSDOC_63bb092a_00fe_45ff_a4b8_d8be998d1a).

Document conversions can be resource-intensive. Because of this, two services are included in Office SharePoint Server 2007 to help manage document conversion performance:

 Document Conversions Launcher Service schedules and initiates the document conversions on a server. When Office SharePoint Server 2007 passes it a document conversion request, the Document Conversions Launcher Service calls the appropriate document converter. In most server farm configurations, the Document Conversions Launcher Service and the converter programs that it starts should be installed on an application server. Each application server can only have a single Document Conversions Launcher Service enabled.

 Document Conversions Load Balancer Service balances document conversion requests from across the server farm. When it receives a converter request from Office SharePoint Server 2007, the Document Conversions Load Balancer Service returns a Uniform Resource Identifier (URI) pointing to the appropriate Document Conversions Launcher Service. An application server can only have a single Document Conversions Load Balancer Service enabled.

The following graphic illustrates how these two services work:



1. A user or service requests a conversion of type "A." The Web application asks the Document Conversions Load Balancer Service for an available launcher.

2. The Document Conversions Load Balancer Service returns a URI for the most available Document Conversions Launcher Service.

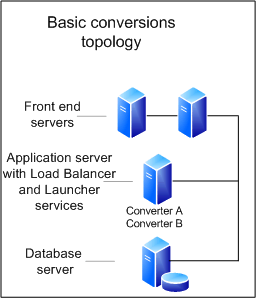
3. The Web application sends the conversion request to the available Document Conversions Launcher Service.

4. The Document Conversions Launcher Service runs Converter A and notifies the Web application when the conversion is done.

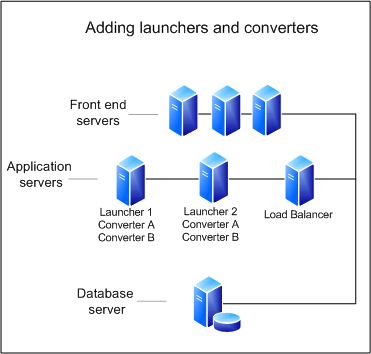
5. The Web application notifies the Document Conversions Load Balancer Service that the conversion is complete, making it available for new requests.

## Typical document conversion topologies

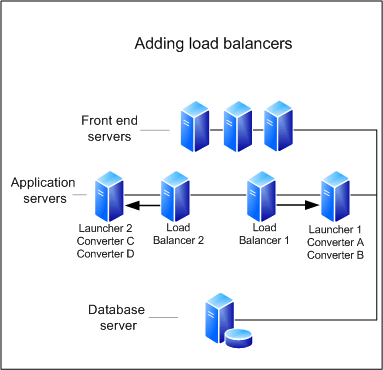
In the most basic document conversions topology, a single application server contains both the Document Conversions Launcher Service and the Document Conversions Load Balancer Service, along with the document conversion programs:



If the performance limits of a single application server are exceeded, better performance can be achieved by using multiple application servers to host identically configured instances of the Launcher Service and its associated document converter programs. A Load Balancer Service can be configured to balance document conversions across multiple application servers, each running the Document Conversions Launcher Service, if each of the application servers running the Document Conversions Launcher Service has the same set of document conversion programs installed:



Each Office SharePoint Server 2007 Web application can only point to one Document Conversions Load Balancer Service. If two Web applications require separate document converters, then two application servers will be required, one for each Document Conversions Load Balancer Service. In the following example, each Web application has a dedicated pair of application servers, one running the Load Balancer Service and the other running the Launcher Service and document conversion programs:



## Configuring document conversions in a server farm

Configuring the document conversions services on a server farm requires manual steps described in this section.

1. On each application server running the Load Balancer Service, determine the port on which the Load Balancer Service is running. To do this, use the regedit command on the application server running the Load Balancer Service, and search for the following key:

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Office Server\12.0\LoadBalancerSettings]

2. Configure the Document Conversions Launcher Service by using the registry. Search for the following key:

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Office Server\12.0\LauncherSettings]

a. On each application server running the Document Conversions Launcher Service, set the value of the entry LoadBalancerUrl to the URL of the relevant Load Balancer Service by using the following syntax: http://[Load Balancer Server]:[Load Balancer port]/HTMLTrLoadBalancer. For example, "http://SampleServer:8093/HTMLTrLoadBalancer" sets the URL of the Load Balancer Service running on the server Http://sampleserver.

note_ddNote:

The Load Balancer Service port number is the value you determined in the previous step. If your farm has multiple application servers running the Load Balancer Service, make sure that you use the port number of the correct Load Balancer Service.

b. Set the value of the entry Port to the port number that the Launcher Service will open for incoming conversion requests. The default port is 8082.

3. If the application server running the Load Balancer Service or the Launcher Service has multiple IP addresses (for example, if the server has two or more network cards), specify the correct IP address for document conversion communications.

note_ddNote:

If a server with multiple IP addresses is running the Load Balancer Service or the Launcher Service, you may see an error message in the Unified Logging Service (ULS) log with the value 6062 or 0000, the event category "Load Balancer Service" or "Launcher Service," and the description string "Found n valid ip addresses for this machine. Choosing this one: nnn.nnn.nnn.nnn"

To specify the correct IP address for document conversion communications, edit the .config file of the Load Balancer Service or the Launcher Service executable program, and provide an IP address mask to exclude all IP addresses except the one used by the Load Balancer Service or the Launcher Service:

a. Use the PING command-line utility from a server running the Launcher Service to determine the IP address of the server running the Load Balancer Service. For example:

Ping servername

Similarly, use the PING utility to determine the IP address of a server running the Launcher Service.

b. Open the .config file for the Load Balancer Service or the Launcher Service executable program; it is located in the same folder as the service's executable program. For example, if the Launcher Service executable program is in C:\Program Files\Microsoft Office Server\12.0\Bin\Microsoft.Office.Server.Conversions.Launcher.exe, then the .config file would be C:\Program Files\Microsoft Office Server\12.0\Bin\Microsoft.Office.Server.Conversions.Launcher.exe.config.

c. In the .config file, update the value of the keyIPExclude entry. The value of this entry is a regular expression that is compared against all IP addresses. Any values that match the key are excluded as the IP address to use to communicate with the Load Balancer Service or the Launcher Service. You should set an IP address mask that filters out all others except the correct one. For instance, if your server had 1.1.1.1, 1.1.1.2, and 1.1.1.3 as valid IP addresses and you wanted to use 1.1.1.3, you would use the following:

keyIPExclude value= (1\.1\.1\.1)|(1\.1\.1\.2)

Note that the keyIPExclude key works for IPv4 and IPv6. For information on creating regular expressions, see [http://go.microsoft.com/fwlink/?LinkId=79218& c lcid=0x409](http://go.microsoft.com/fwlink/?LinkId=79218&clcid=0x409).

d. After changing the .config file for the Launcher Service or the Load Balancer Service, restart the service. On the Start menu, click Administrative Tools, and then click Services. Locate the Office Document Conversions Launcher Service or the Office Document Conversions Load Balancer Service and, from the shortcut menu, stop and then restart the service.

## Planning topologies for document conversions

Use the [Microsoft® Office SharePoint® Server 2007 Document Conversions Topology Worksheet](http://officebeta.iponet.net/search/redir.aspx?AssetID=AM102118391033) to record your document conversions topology decisions:

In the Load Balancer Service section of the worksheet, for each application server that will run the Load Balancer Service:

1. Record the URL of the application server.

2. Record the IP address of the application server.

3. Record the port number on which the Load Balancer Service is running.

In the Launcher Service section of the worksheet, for each application server that will run the Launcher Service:

1. Record the URL of the application server.

2. Record the names of the document conversion programs that will run on the server.

3. Record the URL of the application server running the Load Balancer Service for this Launcher application server.

4. Record the IP address of the application server.

5. Record the port number on which the Launcher Service is running.

## Worksheet

[Microsoft Office SharePoint Server 2007 Document Conversions Topology Worksheet](http://officebeta.iponet.net/search/redir.aspx?AssetID=AM102118391033) (http://officebeta.iponet.net/search/redir.aspx?AssetID=AM102118391033)

# Chart the farms within and across your networks

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Plan for availability (Office SharePoint Server)

This article describes the availability options for the server roles included in a Microsoft Office SharePoint Server 2007 farm. After reading this article, you will be able to identify and record the availability options that are appropriate for your environment.

In this article:

 [About availability](#DSDOC_section19ccfb27f_ecba_4b7d_b9a0_88)

 [Define server redundancy requirements](#DSDOC_section29ccfb27f_ecba_4b7d_b9a0_88)

 [Plan for a minimum level of availability](#DSDOC_section39ccfb27f_ecba_4b7d_b9a0_88)

 [Plan front-end Web server availability](#DSDOC_section49ccfb27f_ecba_4b7d_b9a0_88)

 [Plan application server availability](#DSDOC_section59ccfb27f_ecba_4b7d_b9a0_88)

 [Plan database availability](#DSDOC_section69ccfb27f_ecba_4b7d_b9a0_88)

 [Select a baseline topology](#DSDOC_section79ccfb27f_ecba_4b7d_b9a0_88)

## About availability

Availability management is concerned with the ability of a system to respond predictably to requests. The availability of a service relies on the health of a number of components, including the network and the server computers that are hosting the service. Sever computer dependencies such as network cards, power supplies, and hard disk drives can all affect the availability of your service. This article focuses on the availability options for the server roles included in a Office SharePoint Server 2007 server farm. This article does not address the availability of other components.

One of the most common measures of availability is number of nines. This translates into the percentage of time that a given system is active and working. For example, a system with a 99.999 uptime percentage is said to have five nines of availability. The following table correlates the number of nines to calendar time equivalents.

|  |  |  |  |
| --- | --- | --- | --- |
| Acceptable uptime percentage | Downtime per day | Downtime per month | Downtime per year |
| 95 | 72.00 minutes | 36 hours | 18.26 days |
| 99 | 14.40 minutes | 7 hours | 3.65 days |
| 99.9 | 86.40 seconds | 43 minutes | 8.77 hours |
| 99.99 | 8.64 seconds | 4 minutes | 52.60 minutes |
| 99.999 | 0.86 seconds | 26 seconds | 5.26 minutes |

Office SharePoint Server 2007 supports scalable server farms for high availability and performance. Typically, availability is the first consideration in determining the number of server computers to start with. After factoring in availability requirements, performance and capacity planning also play a role in determining both the number of servers and the size or capacity of the server computers in a server farm. Adding server computers to meet these goals also increases the overall availability of your service.

The purpose of this article is to help you determine the minimum requirements to allow your deployment to achieve your goals for uptime and address your tolerance of downtime. After achieving minimum availability in your design, subsequent articles will guide you through the process of optimizing the server topology and hardware requirements to achieve performance and capacity goals.

## Define server redundancy requirements

By the end of this section, you will be able to decide if you need to build minimum availability into your server deployment topology by deploying redundant servers (three or more servers), or if it makes sense for your organization to plan for a limited server deployment that has no redundant servers. If you have already identified high availability as a requirement for your deployment, you do not need to read this section. Instead, go directly to "Plan for minimum availability" later in this article.

For many organizations, the high availability requirements of a solution drive the initial deployment design. These organizations rely on providing user access to services and information. If a service fails or is down for a period of time, the consequence to the business can be detrimental. Such organizations have a low tolerance for downtime and will likely define their uptime goal as a more important criterion than the cost of additional servers required to build availability into the design.

By contrast, some organizations can tolerate a certain amount of downtime. Downtime for a short period of time is an inconvenience for these organizations but it is not detrimental to the business. Such organizations might be willing to accept the risk of unplanned downtime as an acceptable trade-off for the reduced cost of implementing fewer servers.

To gauge your organization’s tolerance of downtime, answer the following questions.

|  |  |  |
| --- | --- | --- |
| Question | Yes | No |
| Is your availability requirement 99% or greater? |  |  |
| If the service becomes unavailable, will employees of your organization be unable to reasonably perform their expected job responsibilities? |  |  |
| If the service becomes unavailable, will business and customer transactions be halted, leading to loss of business and customers? |  |  |

If you answered yes to any of these questions, your organization's tolerance of downtime is low enough to require that a minimum level of availability be built into the server farm topology.

If you are still unsure, consider the cost of downtime relative to the cost of implementing additional servers. First, estimate the cost of downtime to your organization for a typical server failure:

1. Estimate the cost per hour that your company will incur if the service is unavailable. This cost can include lost customer sales (not necessarily delayed customer sales), lost productivity of employees, and the cost of IT services required to bring the service back up.

2. Estimate how long it typically takes (in business hours) to resolve server hardware issues in your organization. It might be useful to review hardware and software supplier maintenance contracts to obtain this figure.

3. Multiply the cost of downtime (per hour) by the number of hours typically required to resolve server hardware issues. This final number is an estimation of the cost of downtime to your organization for a typical server failure.

Next, estimate the cost of purchasing and maintaining a server in your organization:

1. How much does your organization typically spend purchasing a server computer?

2. How much does your organization typically spend maintaining a server computer on a yearly basis? You can estimate this value by dividing the relevant IT budget by the number of servers currently supported.

3. Add these two numbers. This is the estimated cost to your organization for each additional server you add to your server farm.

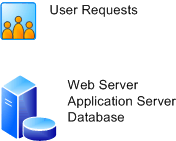
You can additionally add the cost of licensing and maintaining software on these servers if you want to estimate the total cost of ownership per server computer.

By evaluating these two numbers, you can gauge the cost to mitigate the risk of downtime to your organization. If the cost of a single hardware failure is greater than the cost of introducing additional servers into your organization, you can reasonably justify the expense of building availability into your server topology. The next step in the planning process is to build redundancy into the server farm design. Go to "Plan for a minimum level of availability" later in this article.

If, on the other hand, the cost of introducing two or three additional servers into your organization greatly exceeds the estimated cost of downtime for a typical server failure, you can reasonably justify a limited server deployment that is not designed for availability. If so, ensure that this decision is reflected in any service documentation that you produce. However, your goals for performance and capacity might indicate that additional server computers are necessary.

## Plan for a limited server deployment

If you do not need to build availability into your server deployment, the starting point for your server topology is one or two servers. For a limited-use purpose, you can deploy a single server.



Limited-use purposes include the following:

 Installing Office SharePoint Server 2007 for evaluation purposes.

 Deploying only Microsoft Windows SharePoint Services 3.0.

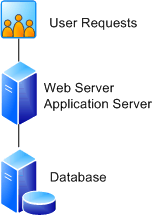
 Deploying a subset of the Office SharePoint Server 2007 features.

 Deploying Office SharePoint Server 2007 for a limited purpose (such as for a single department) or for a limited number of users.

The recommended starting point for most Office SharePoint Server 2007 deployments is at least two server computers:

 Server 1: Front-end Web server and application server computer

 Server 2: Dedicated SQL Server computer



|  |
| --- |
| Worksheet action |
| On the [Availability plan worksheet](http://go.microsoft.com/fwlink/?LinkID=73333&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73333&clcid=0x409), do the following:  **** Indicate that redundancy is not required.  **** Select the most appropriate server topology to use as a starting point for your deployment (either one server or two servers) and copy and paste this topology into the worksheet.  **** In the Notes section, indicate which application server roles you plan to deploy. |

After you complete the worksheet, go to the following article to complete the next planning step: [Chapter overview: Plan for performance and capacity (Office SharePoint Server)](#DSDOC_8dd52916_f77d_4444_b593_1f7d6f330e). The completion of this planning step will determine the total number of servers recommended for your server deployment plan. You do not need to read the rest of this article.

## Plan for a minimum level of availability

To deploy a high-availability solution, you must deploy a server farm. By using a server farm, you mitigate against the effects of unexpected downtime as well as downtime that is related to ongoing maintenance, such as operating system updates.

There are several different server topologies that can be used as a baseline. Each of these topologies builds in a level of server redundancy. This section provides an overview of these server farms.

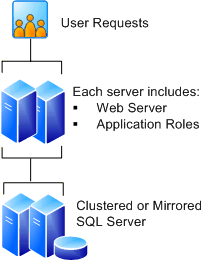
### Four-server farm

The smallest server farm that builds in availability consists of four servers:

 Servers one and two: Web servers and query role installed on both computers. Additional application server roles, such as Excel Calculation Services, can be installed on one or both servers.

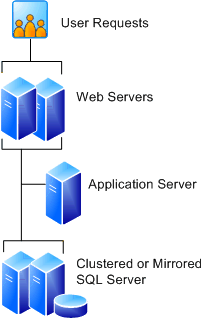
 Servers three and four: clustered or mirrored database server.

The caveat with this farm size, however, is the choice of where to deploy the index server role. If the index role is installed on the same server computer as the query role, the index role no longer propagates content indexes to external query servers. Consequently, if you install the index server role to one of the Web servers, you lose the ability to host the query role on both Web servers. You can install the index role on the database server, achieving availability of the query role on the Web servers. However, the performance of the database server will be affected.



### Five-server farm

The most common highly available server farm topology introduces a middle tier and consists of five server computers.

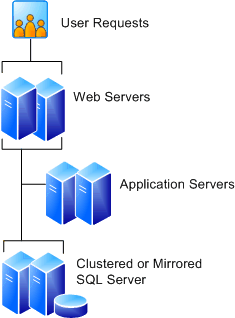


Given this topology, you can install all application server roles on the dedicated application server. This design optimizes the performance of the front-end Web server computers by enabling you to offload one or more application server roles to the middle tier.

The primary planning decision to make with this topology is where to install application server roles. The index server role should remain on the dedicated application server. However, your decision about where to install additional application server roles depends on whether you want to optimize the server farm for performance or for availability. If redundancy of application server roles is a priority, you can install application server roles that are designed to be redundant (Excel Calculation Services, query, and Microsoft Office Project Server 2007) on the two front-end Web server computers. To optimize for performance, consider moving first the Excel Services role to the application server and next the query role. The planning choices that you make after reading “Plan application server availability” later in this article will determine which option is most appropriate for your environment.

### Six-server farm

For maximum redundancy with a minimum number of servers, deploy an additional application server to the middle tier for load balancing application server roles that are designed to be redundant. This server farm topology consists of six servers. The query role is installed to the Web servers to achieve redundancy.



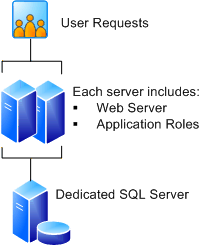
If you plan on deploying the Excel Calculation Services application server role or the Office Project Server 2007 application role to the farm and availability of these services is a priority, this is the recommended starting point. This topology protects these server roles from direct user connections and optimizes the performance of the overall farm when compared to smaller farms.

### Three-server farm

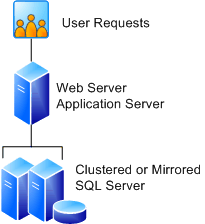
There is another alternative for deploying fewer servers. With a three server farm, you must choose which of the server roles to make redundant: either the Web server role or the database server role.

By adding the third server to the Web tier, you achieve redundancy of the Web server role. The query and index roles can either be installed on the same Web server or they can be separated onto different Web servers. The query role cannot be installed to both Web servers to achieve redundancy.

Although availability is limited, this topology increases the overall performance of the small farm. Use this topology when performance is more important than data redundancy.



By adding a third server to the database tier, you can help ensure availability of critical data. Plan to use this small-farm topology when availability of your data is critical but temporary loss of user access is acceptable.



### Choosing a baseline server farm topology

Each of the server farm topologies described earlier in this article represents a baseline starting point for designing your deployment. The starting point that best suits your organization depends on which server roles you require redundancy for and also which application server roles you plan to use.

The rest of this article describes the redundancy options for each of the server roles. Use the Availability plan worksheet to record your decisions for each of these roles. By the time you are finished with this article, you will be able to identify the baseline topology that can deliver the availability that your organization requires. This is the topology that you will use as a baseline when you start planning for capacity and performance.

## Plan front-end Web server availability

Use this section to:

 Determine if your organization requires redundancy built into the Web tier.

 Plan which Web server load balancing technology to implement.

Most organizations require redundancy at the Web tier. There are a small number of scenarios in which a three-server farm with one server running the Web server role makes sense. To determine if your organization requires redundancy at the Web tier, answer the following questions.

|  |  |  |
| --- | --- | --- |
| Question | Yes | No |
| Is your overall availability requirement below 99%? |  |  |
| Is the availability of your data critical? |  |  |
| Can your organization tolerate temporary loss of access to the data? |  |  |

If you answered Yes to all of these questions, your organization can likely use a single Web server in exchange for adding an additional database server to achieve data availability. In this case, go to the next section, “Plan application server availability.”

If you answered No to any of the questions, Web server redundancy is important to your deployment design. In this case, plan to implement at least two Web servers.

The next step is to plan which load balancing technology to implement. Windows SharePoint Services 3.0 supports two methods of load balancing:

 Software, such as Network Load Balancing (NLB) services in the Microsoft Windows Server 2003 operating system. NLB runs on the front-end Web servers, and uses TCP/IP to route requests. Because NLB (and other software load balancing solutions) runs on the front-end Web servers, it uses the front-end Web system resources, reducing the resources you can use for serving Web pages. However, the impact on system resources is not great, and a software solution can handle up to 32 front-end Web servers.

 Hardware, such as a router or switch box. Load balancing hardware uses your network to direct Web site traffic between your front-end Web servers. Load balancing hardware is more expensive to set up than software, but does not affect your front-end Web server resources. Windows SharePoint Services 3.0 can be used with any load balancing hardware.

Although not recommended, there is a third method of load balancing: round-robin load balancing with Domain Name System (DNS). Round-robin DNS load balancing can use significant resources on the front-end Web servers, is slower than load-balancing software or hardware, and is not recommended for use with Windows SharePoint Services 3.0. Also, round-robin DNS load balancing does not take session load into account when routing a user to a server, which can lead to a server being overloaded.

The Office SharePoint Server 2007 deployment guide includes instructions for configuring NLB in Windows Server 2003. If you choose to implement a different technology for load balancing, factor this into your planning and deployment process.

|  |
| --- |
| Worksheet action |
| In the Web server role section of the [Availability plan worksheet](http://go.microsoft.com/fwlink/?LinkID=73333&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73333&clcid=0x409), indicate the availability choices for the front-end Web server tier. |

## Plan application server availability

Which baseline server topology you choose depends on your requirements for redundancy of application server roles. This section describes the application server roles relative to their availability options.

Application server roles for Office SharePoint Server 2007 fall into two categories:

 Roles that can be redundant

 Roles that cannot be redundant

### Roles that can be redundant

These application server roles can be deployed to multiple servers. The code that is deployed to each server is identical and the application server roles do not store any data. In other words, each instance of these server roles remains identical. If one of the server computers fails, no saved data is lost. The Web servers automatically load balance requests to these server roles across the available application server computers.

The following application server roles can be deployed redundantly:

 Query   The query role can be deployed to any number of application server computers or it can be deployed across Web servers. There is one limitation, however. If the query role is deployed to the same server that hosts the index role, the query role cannot be deployed to any other server computers. This is because the index role recognizes that the query role is on the same server and, consequently, does not attempt to propagate the index. In some scenarios, you can optimize the throughput of your server farm by deploying the query role across your Web servers, even if you have introduced a middle tier for dedicated application servers. For example, if more than 50% of the content requests coming into the server farm are requests for static content, performance is potentially optimized by hosting the query role on the Web servers. This is because the query role caches the content that it serves, making it readily available for subsequent requests. The query role is unique in this sense.

 Excel Calculation Services The Excel Calculation Services role performs Excel calculations on Excel workbooks that are stored in the content databases. This application server role is unique in that it stores session-state information throughout the duration of a user session. When a user opens a workbook, the Web server role continues to route the user requests to the same Excel Calculation Services server until the workbook is closed and the user finishes the session. The Excel Calculation Services role can be a resource-intensive role. In some scenarios, you can optimize the performance of your farm by deploying this role across all Web servers.

 Office Project Server 2007 Although Office Project Server 2007 is not included with Office SharePoint Server 2007, it is built on the Windows SharePoint Services 3.0 platform and can be deployed to a Windows SharePoint Services 3.0 or Office SharePoint Server 2007 farm. The Office Project Server 2007 application role serves requests for Office Project Server 2007 services and data to the Microsoft Office Project Web Access servers.

### Roles that cannot be redundant

Application server roles that cannot be redundant include index and Windows SharePoint Services 3.0 search. These application server roles can be deployed to multiple servers; however, the multiple servers are not redundant. These server roles are configured to crawl content and generate content indexes. If you deploy these roles to multiple servers, each server crawls different content.

 Windows SharePoint Services 3.0 The Windows SharePoint Services 3.0 search application role is an option if you are not using Office SharePoint Server 2007 query and indexing. The Windows SharePoint Services 3.0 search application role includes both the search and indexing components. These components cannot be divided. Additionally, Windows SharePoint Services 3.0 search is required to provide full text search of Help. Consequently, you can consider deploying this application server role to a Office SharePoint Server 2007 farm to achieve this functionality (even if Office SharePoint Server 2007 search is deployed).

 Office SharePoint Server 2007 In Office SharePoint Server 2007, the index role is associated with a Shared Services Provider (SSP). The index role builds one index per SSP. One index server can be associated with multiple SSPs. However, indexes across SSPs cannot be combined. You can deploy multiple index servers to improve capacity. In this case, each index server is associated with different SSPs. Unlike the Windows SharePoint Services 3.0 search role, content indexes produced by the Office SharePoint Server 2007 index role are continuously propagated to all servers that host the query role in a farm. Consequently, the output of the Office SharePoint Server 2007 index server role (that is, the index) is considered redundant if the query role is deployed to more than one server computer.

If you are deploying a Office SharePoint Server 2007 farm, we recommend that you use the Office SharePoint Server 2007 query server and index server roles. This allows you to scale the query component out, achieving redundancy of the content indexes. Because the primary reason for deploying multiple Office SharePoint Server 2007 index servers or Windows SharePoint Services 3.0 search servers is to scale for capacity or performance, subsequent planning articles will help you decide if multiple servers are recommended for your deployment.

The following chart indicates which application server roles can be deployed redundantly and which roles can be deployed to multiple servers but are not redundant.

|  |  |
| --- | --- |
| Application server role | Multiple servers hosting this role are redundant |
| Query | Yes |
| Excel Calculation Services | Yes |
| Office Project Server 2007 | Yes |
| Index | No |
| Windows SharePoint Services 3.0 search | No |

### Evaluating the risks of application server failures

This section summarizes the expected consequences of a single application server failure. In other words, if you deploy an application server role to just one server and the server fails, what are the potential consequences? Understanding the potential consequences will help you prioritize the allocation of servers in your farm. The following table lists application server roles and describes the consequences of downtime for each.

|  |  |
| --- | --- |
| Application server role | Consequences of downtime |
| Query | Users will not be able to issue full-text queries. Users can still browse through sites and access content exposed through the sites. If your application depends on users or customers being able to find content by searching, plan to deploy the query server role to multiple servers. In a five-server farm, this can easily be accomplished by deploying the query role to the two Web server computers. |
| Excel Calculation Services | Server-side rendering of Excel and business intelligence data will not be available. Spreadsheets cannot be loaded, recalculated, refreshed, or retrieved by Excel Calculation Services. Scorecards and features that use the Excel Web Renderer are not available.  Users will still be able to open spreadsheets from SharePoint libraries by using the Excel client application. However, if users don’t have permission to open files in the client, they will not be able to view those files until the Excel Calculation Services role is back online. |
| Office Project Server 2007 services | Office Project Server 2007 applications are not available. Project Workspaces will be available from within the content Web application; however, Office Project Web Access and all related features are not accessible. Also, third-party integration with the Project Server Interface will not be available. The Office Project Server 2007 Reporting database remains available. |
| Index | Query servers will continue to use existing content indexes until the index service is restored and new or updated indexes are generated. Consequently, search results will not include new or changed content while the index role is unavailable. |
| Windows SharePoint Services 3.0 search | Search is unavailable. The amount of time required to restore the search capability depends on if existing content indexes can be restored or if new indexes must be generated by re-crawling the content. |

The general redundancy recommendation is to plan to install an application server role to at least two application server computers if:

 Your solution is primarily based on the features provided by the application server.

 Your availability requirement for the features provided by the server role is 99 percent or greater.

If your organization can tolerate temporary loss of this functionality for the amount of time it takes your IT team to deploy an application server role to a different server or to restore service to the existing server, consider deploying the role to a single application server.

|  |
| --- |
| Worksheet action |
| In the application server roles section of the [Availability plan worksheet](http://go.microsoft.com/fwlink/?LinkID=73333&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73333&clcid=0x409), indicate which application server roles you plan to deploy. For server roles that can be redundant, indicate if your organization requires redundancy of the role. |

## Plan database availability

Use this section to help you determine if redundancy of the database server role is a requirement for your solution. Subsequent planning topics will help you decide which database availability technology is most appropriate for your environment. For more information, see Plan for and design database storage and management (Office SharePoint Server).

The database server role affects the availability of your solution more than any other role. If a Web server or an application server fails, these roles can quickly be restored or redeployed. However, if a database server fails, your solution depends on restoring the database server. This can potentially include rebuilding the database server and then restoring data from your backup media. In this case, you can potentially lose any new or changed data dating back to your last backup job, depending on how SQL Server is configured. Additionally, the solution will be completely unavailable for the time it takes to restore the database server role.

There are several scenarios that justify the reduced cost of deploying a single database server. To determine if your solution fits into this category, answer the following questions.

|  |  |  |
| --- | --- | --- |
| Question | Yes | No |
| Is your overall availability requirement below 99%? |  |  |
| Can employees of your organization continue to reasonably perform their job responsibilities if the solution is unavailable for one or more days? |  |  |
| Can your organization tolerate loss of customer access to the solution for more than one day? |  |  |

If you answered Yes to all of these questions, your organization might be able to justify deploying the database server role to a single server computer.

If you answered No to any of these questions, database redundancy is important for your organization. In this case, plan to deploy at least two database servers.

|  |
| --- |
| Worksheet action |
| In the [Availability plan worksheet](http://go.microsoft.com/fwlink/?LinkID=73333&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73333&clcid=0x409), record whether redundancy is required for the database server role. |

## Select a baseline topology

After you identify the redundancy requirements for the individual server roles, review the baseline server topologies and choose the topology that is most appropriate for your environment.

|  |
| --- |
| Worksheet action |
| Copy and paste your selected topology into the [Availability plan worksheet](http://go.microsoft.com/fwlink/?LinkID=73333&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73333&clcid=0x409). Use the Notes section to record additional decisions regarding your availability plan, such as the specific load-balancing technology you are planning to implement or if you plan to deploy the query role across the front-end Web servers. |

# XV Design logical architecture

In this chapter:

 [Chapter overview: Design logical architecture](#DSDOC_1a8e707a_a9b9_4cc1_9daa_08d450692d)

 [Plan authentication methods [Office SharePoint Server]](#DSDOC_40117fda_70a0_4e3d_8cd3_0def768da1)

 [Plan authentication settings for Web applications in Office SharePoint Server](#DSDOC_d3e0e0fc_77b6_4109_87d6_53ad088db0)

# Chapter overview: Design logical architecture

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

In this article:



# Logical architecture elements

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# A Design an intranet solution architecture

Insert introduction here.

## Subhead

Insert section body here.

### Subhead

Insert section body here.

# Chapter overview: Design an intranet solution architecture

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

Modular design:

 Diff service-level agreement for each app. In the event of a farm-wide failure, you can more easily restore sites based on business priority.

# Design team sites architecture

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Design published intranet site architecture

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Design records repository site architecture

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Design additional application sites within your intranet

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Design an Internet solution architecture

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# B Design farm-level architecture

Insert introduction here.

## Subhead

Insert section body here.

### Subhead

Insert section body here.

# Chapter overview: Design farm-level architecture

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Design user access and zones

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Plan Shared Services Provider architecture

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Plan for administrative sites

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Plan alternate access mappings

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Plan for host-named site collections

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# C Design the logical architecture for an extranet solution

Insert introduction here.

## Subhead

Insert section body here.

### Subhead

Insert section body here.

# Chapter overview: Design the logical architecture for an extranet solution

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Design the farm-level logical architecture for an extranet solution

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Plan reverse-proxy settings

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Plan for caching across the extranet environment

ISA caching can be configured independent of the caching configuration in MOSS.

Use ISA caching in addition to MOSS caching only if the following are true:

o Content is static (no post-cache substitution or URL modification)

o Content is 100% anonymous

Adding ISA caching can improve performance in the following scenarios:

o There is a high demand for content hosted by a single farm. Adding ISA caching can improve performance where WFEs might otherwise be a bottleneck. This allows you to improve performance where the max number of WFE servers is already reached or to reduce the number of WFE servers that might otherwise be required.

o To optimize performance over the WAN where one or more regional sites consume content hosted by a central farm. In this scenario, an ISA server at the regional site caches the page requests. Subsequent page requests are served locally instead of over the WAN.

# D Plan for user accounts and authentication

Insert introduction here.

## Subhead

Insert section body here.

### Subhead

Insert section body here.

# Chapter overview: Plan for user accounts and authentication [Office SharePoint Server]

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this chapter:

 [Plan for user accounts [Office SharePoint Server]](#DSDOC_0b99fe82_0762_4317_b6ba_5501af0a99)

 [Plan authentication methods [Office SharePoint Server]](#DSDOC_40117fda_70a0_4e3d_8cd3_0def768da1)

 [Plan authentication settings for Web applications in Office SharePoint Server](#DSDOC_d3e0e0fc_77b6_4109_87d6_53ad088db0)

 [Authentication samples](#DSDOC_23b837d1_15d9_4621_aa0b_9ce3f1c715)

# Plan for user accounts [Office SharePoint Server]

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Plan authentication methods [Office SharePoint Server]

In this article:

 [About authentication](#DSDOC_section140117fda_70a0_4e3d_8cd3_0d)

 [Supported authentication methods](#DSDOC_section240117fda_70a0_4e3d_8cd3_0d)

 [Configure authentication](#DSDOC_section340117fda_70a0_4e3d_8cd3_0d)

 [Choose methods of authentication allowed in your environment](#DSDOC_section440117fda_70a0_4e3d_8cd3_0d)

 [Worksheet](#DSDOC_section540117fda_70a0_4e3d_8cd3_0d)

This article describes the authentication methods that are supported by Microsoft Office SharePoint Server 2007. After reading this article, you will be able to:

 Understand how authentication is implemented in Office SharePoint Server 2007.

 Identify the authentication methods that are appropriate for your environment.

## About authentication

Authentication is the process of validating a user's identity. After a user's identity is validated, the authorization process determines which sites, content, and other features the user can access.

In Office SharePoint Server 2007, the authentication process is managed by Internet Information Services (IIS). After IIS performs authentication of users, the security features in Office SharePoint Server 2007 perform the authorization process.

For more information about implementing Office SharePoint Server 2007 authorization, see [Chapter overview: Plan site and content security [Office SharePoint Server]](#DSDOC_85a1866e_2743_4f98_a1ac_9ea61905c6).

Planning for authentication is important not only to protect your solution by validating users' identities, but also to secure user credentials over the network.

## Supported authentication methods

Office SharePoint Server 2007 provides a flexible and extensible authentication system, which supports authentication for identity management systems that are based or are not based on the Microsoft Windows operating system. By integrating with ASP .NET pluggable authentication, Office SharePoint Server 2007 supports a variety of forms-based authentication schemes. Authentication support in Office SharePoint Server 2007 enables a variety of authentication scenarios, including:

 Using standard Windows authentication methods.

 Using a simple database of user names and passwords.

 Connecting directly to an organization's identity management system.

 Using two or more methods of authentication for accessing partner applications (for example, connecting to your partner company's identity management system for authenticating partner employees while using Windows authentication methods to authenticate your internal employees).

 Participating in federated identity management systems.

The following table lists the supported authentication methods.

|  |  |  |
| --- | --- | --- |
| Authentication method | Description | Examples |
| Windows | The standard IIS Windows authentication methods are supported. | **** Anonymous  **** Basic  **** Digest  **** Certificates  **** Kerberos (Integrated Windows)  **** NTLM (Integrated Windows)  **** |
| ASP.NET forms | Office SharePoint Server 2007 adds support for identity management systems that are not based on Windows by integrating with the ASP.NET forms authentication system. ASP.NET authentication enables Office SharePoint Server 2007 to work with identity management systems that implement the MembershipProvider interface. You do not need to rewrite the security administration pages or manage shadow Active Directory directory service accounts. | **** Lightweight Directory Access Protocol (LDAP)  **** SQL database or other database  **** Other ASP.NET-based forms authentication solutions |
| Web Single Sign-On (SSO) | Office SharePoint Server 2007 supports federated authentication through Web SSO vendors. Web SSO enables SSO in environments that include services running on disparate platforms. You do not need to manage separate Active Directory accounts. | **** Active Directory Federation Services (AD FS)  **** Other identity management systems |

### Authentication of system accounts

ASP.NET forms authentication and Web SSO can be used to authenticate only user accounts. The process accounts used to connect to Microsoft SQL Server database software and run the Web farm must be Windows accounts, even when using alternative methods of authentication to authenticate users.

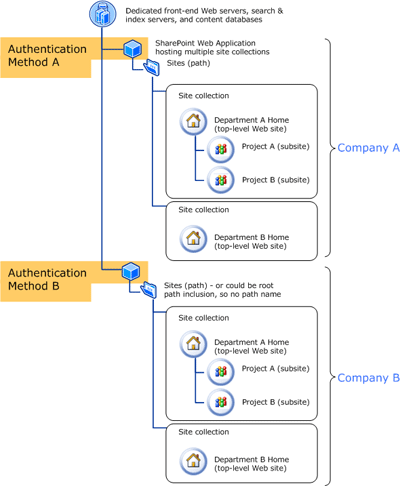
Office SharePoint Server 2007 supports SQL Server authentication and local computer process accounts for farms that are not running Active Directory. For example, you can implement local accounts by using identical user names and passwords across all servers within a farm.

## Configure authentication

Although configuring Windows authentication is a straightforward process, configuring authentication to use ASP.NET forms or Web SSO requires more planning. This section provides a summary of how authentication is configured in Office SharePoint Server 2007. This information will help you understand how to put together an authentication strategy for your solution and determine who in your organization needs to be involved in planning for authentication.

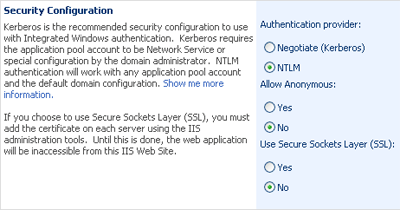
### Configure authentication for SharePoint Web applications

Authentication in Office SharePoint Server 2007 is configured at the SharePoint Web application level. The following diagram illustrates a Windows SharePoint Services server farm that is configured to host sites for multiple companies. Authentication is configured separately for each company.



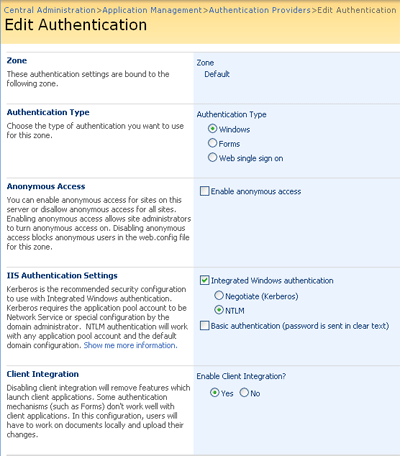
When you initially create or extend a Web application, you are presented with a limited number of authentication options (Kerberos, NTLM, and anonymous). If you are using one of these methods, you can configure authentication when you create or extend the Web application.

The following illustration shows the limited authentication choices that are available when you initially create or extend a Web application.



However, if you are using different authentication settings, select the default authentication options, and then configure authentication after the Web application is created or extended. (To do so, in Central Administration, on the Application Management page, in the Application Security section, select Authentication providers, and then click the zone to open the Edit Authentication page.) The settings that are configured on this page depend on the type of authentication that is selected: Windows, forms, or Web SSO.

The following illustration shows the Edit Authentication page.



Depending on the authentication choices that you select in Central Administration, additional configuration might be necessary. The following table summarizes the configuration steps based on the authentication method. This table also indicates if specialized roles in addition to SharePoint Administrator are needed.

|  |  |  |
| --- | --- | --- |
| Authentication method | Additional configuration | Specialized roles |
| Anonymous, | None | None |
| Basic | None | None |
| Digest | Configure Digest authentication directly in IIS. | None |
| Certificates | 1. Select Windows authentication in Central Administration.  2. Configure IIS for certificate authentication.  3. Enable Secure Sockets Layer (SSL).  4. Obtain and configure certificates from a certification authority (CA). | Windows Server 2003 administrator, to obtain and configure certificates |
| NTLM (Integrated Windows) | None | None |
| Kerberos (Integrated Windows) | 1. Configure the Web application to use Kerberos authentication.  2. Configure a Service Principal Name (SPN) for the domain user account that is used for the application pool identity (application pool process account).  3. Register the SPN for the domain user account in Active Directory. | IIS administrator |
| Forms | 1. Register the membership provider in the Web.config file for the SharePoint Web application.  2. Register the role manager in the Web.config file for the SharePoint Web application (optional).  3. Register the membership provider in the Web.config file for the Central Administration site. | **** ASP.NET developer  **** Administrator of the identity management system you are connecting to |
| Web SSO | In addition to configuration steps required for ASP.NET forms authentication, register an HTTP module for the Web SSO provider. | **** ASP.NET developer  **** Administrator of the identity management system you are connecting to |

### Connect to identity management systems that are external or not based on Windows

To use ASP.NET forms or Web SSO to authenticate users against an identity management system that is not based on Windows or that is external, you must register the membership provider in the Web.config file. In addition to registering a membership provider, you can register a role manager as well. Office SharePoint Server 2007 uses the standard ASP.NET role manager interface to gather group information about the current user. Each ASP.NET role is treated like a domain group by the authorization process in Office SharePoint Server 2007. You register role managers in the Web.config file the same way you register membership providers for authentication.

If you want to manage membership user or roles from the Central Administration site, you can optionally register the membership provider and the role manager in the Web.config file for the Central Administration site (in addition to registering these in the Web.config file for the Web application that hosts the content).

Ensure that the membership provider name and role manager name that you registered in the Web.config file is the same as the name that you entered in the Central Administration authentication.aspx page. If you do not enter the role manager in the Web.config file, the default provider specified in the machine.config file might be used instead.

For example, the following string in a Web.config file specifies a SQL membership provider:

<membership defaultProvider="AspNetSqlMembershipProvider">

For additional information about using ASP.NET forms authentication to connect to a SQL Server authentication provider, see [Authentication samples](#DSDOC_23b837d1_15d9_4621_aa0b_9ce3f1c715).

Finally, if you are using Web SSO to connect to an external identity management system, you must also register an HTTP module for the Web SSO. An HTTP module is an assembly that is called on every request made to your application. HTTP modules are called as part of the ASP.NET request pipeline. For more information, see [Introduction to HTTP Modules](http://go.microsoft.com/fwlink/?LinkId=77954&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=77954&clcid=0x409).

Integrating with ASP.NET forms authentication places additional requirements on the authentication provider. In addition to registering the various elements in the Web.config file, the membership provider, role manager, and HTTP module must be programmed to interact with Office SharePoint Server 2007 and ASP.NET methods, as indicated in the following table.

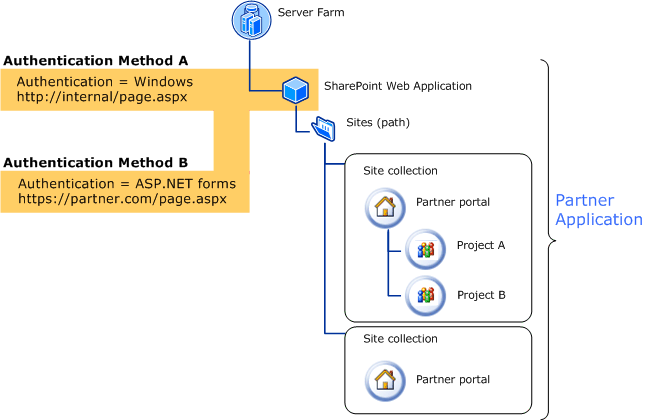
|  |  |
| --- | --- |
| Category | Description |
| Membership provider | To work with Office SharePoint Server 2007, the membership provider must implement the following methods:  **** GetUser (String)   Office SharePoint Server 2007 calls this method to resolve user names during invitations and to get the user's display name.  **** GetUserNameByEmail   Office SharePoint Server 2007 calls this method to resolve user names in invitations.  **** FindUsersByName, FindUsersByEmail   Office SharePoint Server 2007 calls these methods to populate the user picker control on the Add Users page. If the membership provider does not return any users, the picker will not function and administrators will need to type the user name or e-mail address in the Add User text box. |
| Role manager | The role manager must implement the following methods:  **** RoleExists   Office SharePoint Server 2007 calls this method during invitations to verify that a role name exists.  **** GetRolesForUser   Office SharePoint Server 2007 calls this method at access check to gather the roles for the current user.  **** GetAllRoles   Office SharePoint Server 2007 calls this method to populate the group and role picker. If the role provider does not return any groups or roles, the Office SharePoint Server 2007 picker will not function and the administrator will need to type the name of the role in the Add User text box. |
| HTTP module | The HTTP module must handle the following events:  **** AuthenticateRequest   This event is called when ASP.NET is ready to authenticate the user. The Web SSO module must unpack the user's authentication cookie and set the HttpContext.User object with the identity of the current user.  **** EndRequest   This is the last event in the ASP.NET pipeline. This event is called just before returning the code to the client. The Web SSO module must capture 401 responses coming from Office SharePoint Server 2007 and turn these into an appropriate 302 redirect for authentication to the Web SSO logon server. |

### Enabling Anonymous Access

You can enable anonymous access for a Web application in addition to configuring a more secure authentication method. With this configuration, administrators of sites within the Web application can choose to allow anonymous access. If anonymous users want to gain access to secured resources and capabilities, they can click a logon button to submit their credentials.

### Using different authentication methods to access a site

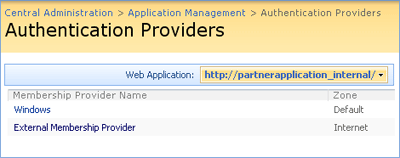
You can configure Web applications in Office SharePoint Server 2007 to be accessed by up to five different authentication methods or identity management systems. The following figure illustrates a partner application that is configured to be accessed by users from two different identity management systems. Internal employees are authenticated by using one of the standard Windows authentication methods. Employees of the partner company are authenticated against their own company's identity management system.



To configure a Web application to be accessed by two or more different authentication systems, you must configure additional zones for the Web application. Zones represent different logical paths of gaining access to the same physical application. With a typical partner application, employees of a partner company access the application through the Internet, while internal employees access the application directly through the intranet.

To create a new zone, extend the Web application. On the Extend Web Application to Another IIS Web Site page, in the Load Balanced URL section, specify the URL and zone type. The zone type is simply a category name applied to the zone and does not affect the configuration of the zone.

After extending the Web application, you can configure a separate authentication method for the new zone. The following figure shows the Authentication Providers page for a Web application that is configured by using two different zones. The default zone is the zone used by internal employees. The Internet zone is configured for partner access and uses ASP.NET forms to authenticate partner employees against the partner identity management system.



### Authentication requirements for crawling content

The index component requires NTLM-authenticated access to content within sites. Consequently, to crawl content in a site that is configured with an authentication method that is not based on Windows, you must configure an additional zone for the Web application and configure the zone to use NTLM. If a zone is already configured to use NTLM, the index component can access the content through this zone.

Also, there is an additional configuration that will prevent the index component from crawling content. If the default zone uses a Windows authentication method other than NTLM, the index component is prevented from using this zone and any other zone to crawl content. For example, if the default zone is configured to use Kerberos authentication or Basic authentication, the index component cannot access content using one of these methods and does not attempt to access content through a different zone. However, if the default zone is configured to use forms authentication, the index component attempts to access content through a zone that is configured for Windows authentication.

To ensure that the index component can crawl content within the Web application:

 Configure at least one zone to use NTLM authentication. Ensure that the search content access account has the Read permission level to content accessed through this zone. You can do so by creating a policy that gives this account the Read permission level.

 Do not configure the default zone to use Anonymous, Basic, Digest, Certificates, or Kerberos authentication (that is, any forms of authentication other than NTLM).

### Planning zones for your authentication design

If you plan to implement more than one authentication method for a Web application by using zones, use the following guidelines:

 Use the default zone to implement your most secure authentication settings. If a request cannot be associated with a specific zone, the authentication settings and other security policies of the default zone are applied. The default zone is the zone that is created when you initially create a Web application. Typically, the most secure authentication settings are designed for end-user access. Consequently, the default zone will likely be the zone that is accessed by end users.

 Use the minimum number of zones that is required by the application. Each zone is associated with a new IIS site and domain for accessing the Web application. Only add new access points when these are required.

 If you want content within the Web application to be included in search results, ensure that at least one zone is configured to use NTLM authentication. NTLM authentication is required by the index component to crawl content. Do not create a dedicated zone for the index component unless necessary.

## Choose methods of authentication allowed in your environment

In addition to understanding how authentication is configured, planning for authentication includes:

 Considering the security context or environment of your Web application in Office SharePoint Server 2007.

 Evaluating the recommendations and tradeoffs for each method.

 Understanding how user credentials and related identity data are cached and consumed by Office SharePoint Server 2007.

 Understanding how user accounts are managed.

 Ensuring that authentication methods are compatible with browsers that are used by your users.

|  |
| --- |
| Worksheet action |
| Use the [Authentication methods worksheet](http://go.microsoft.com/fwlink/?LinkId=77970&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=77970&clcid=0x409) to identify which authentication methods you are willing to support in your environment and to record your decisions and recommendations for each. This worksheet will be used when planning authentication methods for individual Web applications in Office SharePoint Server 2007. |

### Recommendations for specific security environments

Your choice of authentication methods will primarily be driven by the security context of your application. The following table provides recommendations based on the most common security environments.

|  |  |
| --- | --- |
| Environment | Considerations |
| Internal intranet | At a minimum, protect user credentials from plain view. Integrate with the user management system that is implemented in your environment. If Active Directory is implemented, use the Windows authentication methods built into IIS. |
| External secure collaboration | Configure a separate zone for each partner company that connects to the site. Use Web SSO to authenticate against each partner’s own identity management system. This eliminates the need to create accounts in your own identity management system and also ensures that contributor identities continue to be maintained and validated by partner employers. If a contributor is no longer employed by a partner company, the contributor cannot continue to gain access to your partner application. |
| External anonymous | Enable anonymous access (no authentication) and allow read-only permissions for users who connect from the Internet. If you want to provide targeted or role-based content, you can use ASP.NET forms authentication to register users by using a simple database of user names and roles. Use the registration process to identify users by role (such as doctor, patient, or pharmacist). When users log on, your site can present content that is specific to the user role. In this scenario, authentication is not used to validate credentials or to limit who can access the content; the authentication process simply provides a method of targeting content. |

### Recommendations and tradeoffs for authentication methods

Understanding the advantages, recommendations, and tradeoffs for each specific authentication method can help you to determine which methods to use in your environment. The following table highlights the recommendations and tradeoffs for each authentication method. For more information about each of the Windows authentication methods supported by IIS, see [IIS Authentication](http://go.microsoft.com/fwlink/?LinkId=78066&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=78066&clcid=0x409).

|  |  |  |
| --- | --- | --- |
| Authentication method | Advantages and recommendations | Tradeoffs |
| Windows | **** Authenticate by using your existing Active Directory accounts.  **** Simplify user management.  **** Take advantage of Active Directory groups when configuring Office SharePoint Server 2007 authorization.  **** Avoid writing custom code. | **** Each of the methods has its own associated pros and cons.  **** Some IIS authentication protocols are not supported by all Web browsers. |
| ASP.NET forms | **** Set up Office SharePoint Server 2007 in an environment that does not use Active Directory (does not require Windows accounts).  **** Authenticate against two or more different identity management systems when creating partner applications.  **** Implement a custom authentication scheme using arbitrary criteria.  **** Authenticate users coming from the Internet. | **** Requires customization of the Web.config file.  **** Subject to replay attacks for the lifetime of the cookie, unless using SSL Transport Layer Security (TLS). |
| Web SSO | **** Implement Office SharePoint Server 2007 in an environment that uses federated authentication to secure digital identities across organizations and security environments.  **** Implement Office SharePoint Server 2007 in an environment that provides SSO to services running on disparate platforms, including environments that do not use Active Directory.  **** Take advantage of AD FS.  **** Authenticate against two or more different identity management systems when creating partner applications. | **** Requires an existing federated authentication system.  **** Requires customization of the Web.config file.  **** AD FS requires SSL. Other SSO systems might have other requirements. |

### Management of user identity information

How user credentials and other identity information is processed and used by Office SharePoint Server 2007 can influence your decision about which of the authentication options is best for your intended purpose. This section details how user identity information is processed in the following categories:

 Binary IDs   How user binary identifiers (IDs) are created or used by Office SharePoint Server 2007.

 Caching   The process of retaining a user's identity for a period of time to avoid repeating the authentication process for each request.

 Role and group membership   In addition to determining who users are, the authentication process also determines which groups or roles a user belongs to. This information is used during the authorization process to determine which actions a user has permissions to perform. For the purpose of authorization, Office SharePoint Server 2007 treats Active Directory groups and ASP.NET roles as the same type of entity.

The following table details how Office SharePoint Server 2007 manages user binary IDs, cached user data, and role and group membership data depending on which authentication method is used.

|  |  |  |
| --- | --- | --- |
| Item | Windows authentication | ASP.NET forms and Web SSO |
| Binary IDs | Office SharePoint Server 2007 uses the Windows security identifier (SID). | Office SharePoint Server 2007 creates a unique binary ID by combining the provider name with the user name. |
| Caching | User credentials are cached and managed by IIS, Internet Explorer, and Windows. | ASP.NET uses an encrypted cookie to keep the user's credentials for the duration of a session. |
| Role and group membership | Windows maintains the list of Active Directory domain groups the user belongs to in the access token. Office SharePoint Server 2007 uses information stored in the access token. | When a role manager is registered, Windows SharePoint Services uses the standard role manager interface to gather group information about the current user. Each ASP.NET role is treated like a domain group by the authorization process. ASP.NET can cache the roles the user belongs to in a cookie, depending on the settings that are configured in the Web.config file. |

### Management of user accounts

Understanding how Office SharePoint Server 2007 handles typical user account management tasks can also influence which authentication method you choose. Generally, users who are members of an authentication provider in one zone can manage accounts across all zones as long as they are granted permissions. The information in the following list applies regardless of which authentication method is implemented:

 Adding and inviting new users   You can add or invite a new user from any zone and all authentication methods that are configured if the membership provider and role manager are registered in the current Web.config file. When you add a new user, Office SharePoint Server 2007 resolves the user name against the following sources in the following order:

 The UserInfoList table stored by Office SharePoint Server 2007. User information will be in this list if users have already been added to another site.

 The authentication provider that is configured for the current zone. For example, if a user is a member of the authentication provider that is configured for the default zone, Office SharePoint Server 2007 first checks this associated membership provider.

 All other authentication providers.

 Deleting users   User accounts are marked as deleted in the Office SharePoint Server 2007 database. However, the user record is not removed.

Some user account management behaviors within Office SharePoint Server 2007 differ, depending on the authentication provider. The following table highlights several common user account tasks that differ depending on the authentication method that is implemented.

|  |  |  |
| --- | --- | --- |
| Task | Windows authenticated accounts | ASP.NET forms–authenticated and Web SSO-authenticated accounts |
| Adding and inviting new users | Office SharePoint Server 2007 validates user identities by using Active Directory. | Office SharePoint Server 2007 calls the membership provider and the role manager to verify that the user and roles exists. |
| Changes to logon names | Updated user names are automatically recognized by Office SharePoint Server 2007. New entries are not added to the UserInfoList table. | You must delete the old account name and then add the new account name. Permissions cannot be migrated. |
| Logging on | If Integrated Windows authentication (Kerberos or NTLM) is used and the browser is configured to automatically log on, users do not need to manually log on to SharePoint sites. By default, Internet Explorer is configured to automatically log on to intranet sites. If a logon is required (for example, sites that require a different set of credentials), users are prompted only for a user name and password. However, if Basic authentication is used, or the user is using a browser that is not configured to automatically log on, users might be prompted for logon credentials when they access a SharePoint site. | Office SharePoint Server 2007 provides a standard logon page for use with forms authentication. This page includes the following fields: user name, password, sign in automatically (to persist the cookie). You can create your own logon page to add additional logon controls (for example, create a new account, or reset password). |

### Browser support

Not all browsers work with each of the authentication methods that are supported. Before selecting authentication methods to allow in your environment, determine which browsers you need to support. Then, determine which authentication methods are supported by the browsers. Internet Explorer works with each of the supported authentication methods. Additional browsers that are supported by Office SharePoint Server 2007 include:

 Netscape 8.0

 Netscape 7.2

 Mozilla 1.7.12

 Firefox 1.5

 Safari 2.02

## Worksheet

Use the following worksheet to record which authentication methods are appropriate for your environment.

 [Authentication methods worksheet](http://go.microsoft.com/fwlink/?LinkId=77970&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=77970&clcid=0x409)

The following table represents an example of a completed worksheet.

|  |  |  |  |
| --- | --- | --- | --- |
| Authentication method | Allow | Don't allow | Notes and recommendations |
| Anonymous |  | x |  |
| Basic |  | x |  |
| Digest |  | x |  |
| Certificates |  | x |  |
| NTLM (Integrated Windows) | x |  | "Use NTLM for all department sites except finance." |
| Kerberos (Integrated Windows) | x |  | "Use Kerberos authentication for sites with a high security service level agreement." |
| ASP.NET forms | x |  | "Use forms authentication to allow partner company access to sites hosted in the partner extranet. We currently allow authentication against the following identity management systems: Active Directory, LDAP. Work with Sidney Higa to develop authentication settings for use with forms authentication." |
| Web SSO | x |  | "Use this method for partner applications only if a partner company is participating in federated identity management systems. See David Jones for more information." |

Additional Notes:"Work with Denise Smith to sign off on all authentication settings for SharePoint Web applications prior to implementing."

# Plan authentication settings for Web applications in Office SharePoint Server

In this article:

 [Plan authentication settings](#DSDOC_section1d3e0e0fc_77b6_4109_87d6_53)

 [Plan authentication exclusions](#DSDOC_section2d3e0e0fc_77b6_4109_87d6_53)

 [Worksheet](#DSDOC_section3d3e0e0fc_77b6_4109_87d6_53)

This article discusses the authentication configuration settings that need to be planned for individual Web applications in Microsoft Office SharePoint Server 2007. Use this article with the [Web application authentication settings worksheet](http://go.microsoft.com/fwlink/?LinkID=73334&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73334&clcid=0x409.) Complete a separate worksheet for each of the following elements that are a part of your solution design in Office SharePoint Server 2007:

 New or extended Web applications in Office SharePoint Server 2007.

 Additional zones within a Web application (other than the default zone). Include zones that are created for the search account.

Use completed worksheets with Deploy and configure SharePoint sites [Office SharePoint Server].

## Plan authentication settings

This section discusses each of the settings on the Edit Authentication page of the SharePoint Central Administration Web site. To get to this page, on the Application Management page, in the Application Security section, click Authentication providers. Click the zone that you want to modify authentication settings for. The Edit Authentication page opens.

Depending on the authentication options you choose, you might be able to specify your authentication settings directly when you create or extend the Web application in Office SharePoint Server 2007. However, not all options are available when you initially create or extend a Web application. If you cannot configure authentication when you create or extend the Web application, you can accept the default authentication settings initially and then edit the settings on the Edit Authentication page.

### Authentication type

Select the method that you want to use. If you are planning to allow anonymous access instead of implementing an authentication method listed in this section, select Windows authentication.

If you select Windows, specify the Windows authentication method in the IIS Authentication Settings section of the Edit Authentication page. If you select Forms or Web single sign on, the options on the Edit Authentication page change to allow you to enter the membership provider name and the role manager name.

If you want to use Certificate authentication or Kerberos authentication, review the following table to identify the additional configuration steps required to configure these methods.

|  |  |  |
| --- | --- | --- |
| Authentication method | Additional configuration | Specialized roles |
| Certificates | 1. Select Windows authentication in Central Administration.  2. Configure Internet Information Services (IIS) for certificates.  3. Enable Secure Sockets Layer (SSL).  4. Obtain and configure certificates from a certification authority (CA). | Microsoft Windows Server 2003 administrator, to obtain and configure certificates |
| Kerberos (Integrated Windows) | 1. Select Kerberos authentication in Central Administration.  2. Configure a Service Principal Name (SPN) for the domain user account that is used for the application pool identity (application pool process account).  3. Register the SPN for the domain user account in Active Directory. | IIS administrator |

|  |
| --- |
| Worksheet action |
| Record the additional configuration necessary in the Additional Configuration section of the [Web application authentication settings worksheet](http://go.microsoft.com/fwlink/?LinkID=73334&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73334&clcid=0x409). |

### Anonymous access

Indicate whether anonymous access is allowed. If you selected Forms or Web single sign-on in the Authentication Type section, select the Enable anonymous access check box.

### Client integration

You can disable client integration, which removes features that start client applications. This is the optimal configuration for some scenarios, such as publishing read-only content to the Web for anonymous access. Additionally, if you select ASP.NET forms authentication or Web Single Sign-On (SSO) authentication, client integration is set to No by default.

##### Expected behaviors when client integration is disabled

When client integration is disabled, sites behave in the following ways:

 Links that start client applications are not visible.

 Documents are opened in the browser. Documents cannot be opened by client applications.

 Users cannot edit documents on the site directly from the client applications. However, users can download the document, edit the document locally, and then upload the document.

The following table lists specific menu commands and features that are not available when client integration is disabled.

|  |  |
| --- | --- |
| Category | Command or feature that is unavailable |
| Toolbars | New document  Work in Microsoft Office Outlook  Open in Windows Explorer  Export to spreadsheet  Open with Database Program |
| Editing documents | Edit in Microsoft Office applications such as Word and Excel. |
| Views | Explorer view  Create an Access view |
| Picture libraries | Upload multiple  Edit picture  Download  Send to |
| Slide libraries | Publish slide  Send to Microsoft Office PowerPoint |
| Other | Discuss  Connect to Office Outlook |

##### Behaviors of specific authentication methods

In addition to the deployment scenario (such as publishing read-only content), the choice of authentication method might determine how to configure client integration. Some authentication methods behave differently with client applications. In some cases, the behavior depends on whether client browsers are configured to use persistent cookies or session cookies.

The following table summarizes the potential behaviors of client integration when used with specific authentication methods.

|  |  |
| --- | --- |
| Authentication method | Behavior |
| Basic | Users are prompted to enter their credentials each time they access a document. Other features might also require that they enter their credentials again. |
| ASP.NET forms and Web SSO | If the following conditions are true, a persistent cookie is created:  **** The authentication provider supports persistent cookies.  **** The user clicks Sign me in automatically when they log in.  The persistent cookie is shared by all applications that use the same cookie store and the user can open documents in the client applications. The persistent cookie is created with a default time-out value of 30 minutes. This value can be changed by adding or updating the time-out parameter in the forms node in the Web.config file. For example:  <forms loginUrl="login.aspx" name=".ASPXFORMSAUTH" timeout="100" />  When the cookie expires, client integration stops working. If users are in a browser, they will be prompted to re-enter credentials.  If the authentication provider does not support persistent cookies or the user did not click Sign me in automatically when they logged in, a session cookie is used. A session cookie is only accessible by the browser. The user will not be able to open document directly in the client applications.  If the authentication provider does not provide support for persistent cookies or if persistent cookies are not allowed in your environment, turn off client integration. For example, Active Directory Federation Services (AD FS) does not provide support for persistent cookies. |
| Anonymous | When opening a document, users are repeatedly prompted for their credentials. If they click Cancel in the authentication dialog box 10 times, the site might open the document by using the client application. Because of this poor experience, it is recommended that client integration be turned off for anonymous access scenarios. |

##### Using the Windows Vista operating system with Internet Explorer 7

In Windows Vista, Internet Explorer 7 includes an additional security feature called protected mode. By default, protected mode is enabled for the Internet, Intranet, and Restricted Sites zones. Because this feature places persistent cookies in a location that prevents sharing across applications, client integration does not work as intended.

To configure Internet Explorer 7 to work with client integration, do one of the following:

 Disable protected mode.

 If protected mode is enabled, add SharePoint sites to the Trusted sites zone in Internet Explorer.

For information about disabling protected mode, see "Configuring Protected Mode" in [Understanding and Working in Protected Mode Internet Explorer](http://go.microsoft.com/fwlink/?LinkId=78098&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=78098&clcid=0x409).

##### Testing client integrations settings

If you are uncertain about how to configure the client integration setting, test the results in a test environment before deploying sites into production. If this setting is changed after it is applied, sites and client applications might behave unusually.

|  |
| --- |
| Worksheet action |
| On the [Web application authentication settings worksheet](http://go.microsoft.com/fwlink/?LinkID=73334&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73334&clcid=0x409), in the Enable Client Integration section, select Yes or No. |

### Settings for ASP.NET forms authentication and Web SSO

If you are implementing ASP.NET forms authentication or Web SSO, you must develop the configuration settings to insert into the applicable Web.config files. See [Authentication samples](#DSDOC_23b837d1_15d9_4621_aa0b_9ce3f1c715) to review examples of properly configured strings for several common scenarios.

|  |
| --- |
| Worksheet action |
| On the [Web application authentication settings worksheet](http://go.microsoft.com/fwlink/?LinkID=73334&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73334&clcid=0x409), enter the following two types of information:  **** Name   The name of the membership provider, role manager, and HTTP module (if applicable). These names appear in the Central Administration site.  **** Web.config configuration   Paste the appropriate configuration strings into the worksheet. These strings can be copied from the worksheet into the Web.config files when the Web application is deployed. |

Ensure that the MembershipProvider name and RoleManager name you registered in the Web.config file is the same as the name that you entered in the Central Administration authentication.aspx page. If you do not enter the role manager in the Web.config file, the default provider specified in the machine.config file might be used instead.

For example, the following string in a Web.config file specifies a SQL membership provider:

<membership defaultProvider="AspNetSqlMembershipProvider">

For more information about requirements for membership providers and role managers, see "Connect to identity management systems that are not based on Windows or that are external" in [Plan authentication methods [Office SharePoint Server]](#DSDOC_40117fda_70a0_4e3d_8cd3_0def768da1).

## Plan authentication exclusions

If you are implementing ASP.NET forms authentication or Web SSO, you need to plan for authentication exclusions. If you are implementing Windows authentication, you do not need to read this section.

When you create or extend a Web application or when you add a zone to a Web application, IIS creates a new Web site. Authentication settings that are registered in the Web.config file for this Web application are inherited by virtual directories below the Web site. Virtual directories that are added below a Web application in Office SharePoint Server 2007 are not managed by Office SharePoint Server 2007 and are considered to be excluded virtual directories.

If you are implementing ASP.NET forms authentication or Web SSO and you plan to add virtual directories below these Web sites, you need to decide whether you want these excluded virtual directories to inherit the ASP.NET forms authentication or Web SSO settings.

|  |
| --- |
| Worksheet action |
| On the [Web application authentication settings worksheet](http://go.microsoft.com/fwlink/?LinkID=73334&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73334&clcid=0x409), indicate whether excluded virtual directories will be added in IIS beneath the Web site that corresponds to this Web application in Office SharePoint Server 2007. If excluded virtual directories will be added, indicate whether authentication settings should be inherited. |

Use the following procedure to configure IIS so authentication settings are not inherited.

procedure_ddConfigure IIS so authentication settings are not inherited

|  |
| --- |
| 1. Add a new IIS virtual directory beneath the IIS Web site that corresponds to the applicable Web application or zone in Office SharePoint Server 2007.  2. In IIS Manager, right-click the new virtual directory, and then click Properties.  3. Click the Virtual Directory tab.  4. Click Create (this makes the virtual directory an application).  5. Click Configuration.  6. Select the wildcard application maps, and then click Remove.  7. Click Yes, and then click OK.  8. Create a new Web.config file at the root of the new virtual directory file system path, and add the following entries:  <?xml version="1.0" encoding="UTF-8" standalone="yes"?>  <configuration>  <system.web>  <httpModules>  <clear />  </httpModules>  <httpHandlers>  <clear />  </httpHandlers>  </system.web>  </configuration>  9. |

## Worksheet

Use the following worksheet to plan and record configuration settings for each of your Web applications in Office SharePoint Server 2007.

 [Web application authentication settings worksheet](http://go.microsoft.com/fwlink/?LinkID=73334&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73334&clcid=0x409)

# Authentication samples

In this article:

 [SQL membership provider](#DSDOC_section123b837d1_15d9_4621_aa0b_9c)

 [Active Directory membership provider](#DSDOC_section223b837d1_15d9_4621_aa0b_9c)

 [LDAP membership provider](#DSDOC_section323b837d1_15d9_4621_aa0b_9c)

 [Web SSO with AD FS](#DSDOC_section423b837d1_15d9_4621_aa0b_9c)

This article includes sample configuration settings for several common forms authentication and Web single sign-on (SSO) authentication providers.

## SQL membership provider

The following table provides examples of Web.config file entries for using ASP.NET forms authentication to connect to a SQL membership provider.

|  |  |
| --- | --- |
| Configuration steps | Description and example Web.config file entries |
| Turn on ASP.NET forms authentication. | You can set the authentication type for a particular zone to forms authentication on the Edit Authentication page on the SharePoint Central Administration Web site.  This automatically changes the mode specified in the authentication element of the Web.config file for that zone to forms.  For example:  <authentication mode="Forms">  </authentication> |
| Register the membership provider. | If you are using Microsoft SQL Server database software on the local server as your membership provider database, and you specify AspNetSqlMembershipProvider for the membership provider name, you might not need to make any additional changes to the Web.config file. In this scenario, if the machine.config file has the correct configuration for the AspNetSqlMembershipProvider, you can use it for Windows SharePoint Services without making any changes.  If the default configuration in the machine.config file does not apply (for example, if you want to use a SQL Server database on a remote server), you must edit the Web.config files for both the Web application and the Central Administration Web site to specify the connection information in the connectionStrings element for the membership provider database.  For example:  <connectionStrings>  <add name="SqlProviderConnection" connectionString="server=SQLSERVERMACHINE;database=aspnetdb;Trusted\_Connection=True" />  </connectionStrings>  Replace SQLSERVERMACHINE with the name of server computer on which you have installed the SQL Server membership database.  Next, add the membership and providers elements to register the membership provider in the Web.config file. Because a default provider is already registered in the machine.config file, you must include a <remove> element prior to the <add> element.  For example:  <membership defaultProvider="AspNetSqlMembershipProvider">  <providers>  <remove name="AspNetSqlMembershipProvider" />  <add connectionStringName="SqlProviderConnection" name="AspNetSqlMembershipProvider" type="System.Web.Security.SqlMembershipProvider, System.Web, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />  </providers>  </membership>  The membership element must be included within the system.web element of the Web.config file for both the Web application and the Central Administration site. |
| Register the role manager (optional). | You can use the default role provider for ASP.NET by adding a roleManager element to the system.web element of the Web.config file. For example:  <roleManager enabled="true" />  The preceding syntax uses the AspNetSqlRoleProvider, which is defined in the machine.config file. This role manager can connect to the ASPNETDB database in either the local or remote instance of SQL Server. If you want to use a SQL Server database on a remote server as your role provider database, you must edit the Web.config file to specify the connection information for the remote database server.  For example:  <connectionStrings>  <add  name="SqlProviderConnection"  connectionString="server=SQLSERVERMACHINE; database=aspnetdb; Trusted\_Connection=True"  />  </connectionStrings>  Replace SQLSERVERMACHINE with the name of the remote server that hosts the SQL database. You can specify the same connectionStringName element value for both the membership provider and role manager, so you do not need to add a new connectionStrings element for the role provider. However, if you want to use a different database for the role provider, you must add a separate connectionStrings element for the role provider.  Next, you need to add the roleManager and providers elements to register the roleManager provider in the Web.config. Because a default provider is already registered in the machine.config file, you must include a <remove> element prior to the <add> element.  For example:  <roleManager enabled="true" defaultProvider="AspNetSqlRoleProvider">  <providers>  <remove name="AspNetSqlRoleProvider" />  <add connectionStringName="SqlProviderConnection" applicationName="/" description="Stores and retrieves roles data from the local Microsoft SQL Server database" name="AspNetSqlRoleProvider" type="System.Web.Security.SqlRoleProvider, System.Web, Version=2.0.3600.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />  </providers>  </roleManager>  The roleManager element must be included within the system.web element of the Web.config file for both the Web application and the Central Administration Web site. |
| Register the HTTP module. | Not applicable |

## Active Directory membership provider

The following table provides examples of Web.config file entries for using ASP.NET forms authentication to use an Active Directory directory service membership provider.

note_ddNote:

This will only work in a scenario with a single domain.

|  |  |
| --- | --- |
| Configuration steps | Description and example Web.config file entries |
| Turn on ASP.NET forms authentication. | You can set the authentication type for a particular zone to forms authentication on the Edit Authentication page in Central Administration.  This automatically changes the mode specified in the authentication element of the Web.config file for that zone to forms.  For example:  <authentication mode="Forms">  </authentication>  You can also specify the login page URL in the forms element, for example:  <authentication mode="Forms">  <forms loginUrl="/\_layouts/login.aspx"></forms>  </authentication> |
| Register the membership provider. | If you want to use an Active Directory server for a membership provider, you must edit the Web.config file to register the membership provider. To do this, you must specify the connection information to the Active Directory server in the connectionStrings element.  For example:  <connectionStrings>  <add name="ADConnectionString"  connectionString=  "LDAP://DirectoryServer/CN=Users,DC=DirectoryServer " />  </connectionStrings>  Replace DirectoryServer with the name of membership directory server.  <membership defaultProvider="MembershipADProvider">  <providers>  <add name="MembershipADProvider" type="System.Web.Security.ActiveDirectoryMembershipProvider, System.Web, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a"  connectionStringName="ADConnectionString"/></providers>  </membership>  note_ddNote:  The preceding example does not specify account credentials. If you do not specify account credentials, your application's process identity is used to access Active Directory.  If another account is required to access Active Directory, you can specify different account credentials in the connectionUsername and connectionPassword attributes, which means you are supplying the user name and password in plaintext. As a result, we recommend that you encrypt this configuration section. For more information, see the following articles:   [How To: Encrypt Configuration Sections in ASP.NET 2.0 Using DPAPI](http://go.microsoft.com/fwlink/?LinkId=78123&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=78123&clcid=0x409)   [How To: Encrypt Configuration Sections in ASP.NET 2.0 Using RSA](http://go.microsoft.com/fwlink/?LinkId=76778&clcid=0x409) (<http://go.microsoft.com/fwlink/?LinkId=76778&clcid=0x409>) |
| Register the role manager (optional). |  |
| Register the HTTP module. | Not applicable |

## LDAP membership provider

The following table provides examples of Web.config file entries for using ASP.NET forms authentication with a Lightweight Directory Access Protocol (LDAP) membership provider.

|  |  |
| --- | --- |
| Configuration steps | Description and example Web.config file entries |
| Turn on ASP.NET forms authentication. | You can set the authentication type for a particular zone to forms authentication from the Edit Authentication page in Central Administration.  This automatically changes the mode specified in the authentication element of the Web.config file for that zone to forms.  <system.web>  <!-mode=[Windows|Forms|Passport|None]>  <authentication mode="Forms" />  </system.web> |
| Register the membership provider. | The membership element must be included within the system.web element of the Web.config file.  <membership defaultProvider="LdapMembershipProvider">  <providers>  <add  name="LdapMembership"  type="Microsoft.Office.Server.Security.LDAPMembershipProvider, Microsoft.Office.Server, Version=12.0.0.0, Culture=neutral, PublicKeyToken=71E9BCE111E9429C"  server="DC"  port="389"  useSSL="false"  userDNAttribute="distinguishedName"  userNameAttribute="sAMAccountName"  userContainer="CN=Users,DC=userName,DC=local"  userObjectClass="person"  userFilter="(|(ObjectCategory=group)(ObjectClass=person))"  scope="Subtree"  otherRequiredUserAttributes="sn,givenname,cn"  />  </providers>  </membership>  You will need to change the values specified for the server and userContainer attributes to match your environment. |
| Register the role manager (optional). | <roleManager defaultProvider="LdapRoleProvider" enabled="true" cacheRolesInCookie="true" cookieName=".PeopleDCRole">  <providers>  <add  name="LdapRoleProvider"  type="Microsoft.Office.Server.Security.LDAPRoleProvider, Microsoft.Office.Server, Version=12.0.0.0, Culture=neutral, PublicKeyToken=71E9BCE111E9429C"  server="DC"  port="389"  useSSL="false"  groupContainer="DC=userName,DC=local"  groupNameAttribute="cn"  groupMemberAttribute="member"  userNameAttribute="sAMAccountName"  dnAttribute="distinguishedName"  groupFilter="(ObjectClass=group)"  scope="Subtree"  />  </providers>  </roleManager>  You will need to change the values specified for the server and groupContainer attributes to match your environment. |
| Register the HTTP module. | Not applicable |

## Web SSO with AD FS

The Microsoft Windows Server 2003 R2 operating system introduces Active Directory Federation Services (AD FS), which enables organizations to securely share a user's identity information. AD FS provides Web single sign-on (SSO) technologies to authenticate a user to multiple Web applications during a single online session.

The following two membership and role provider pairs are included with AD FS:

 SingleSignOnMembershipProvider/SingleSignOnRoleProvider   The standard membership provider and role provider included with Windows Server 2003 R2.

 SingleSignOnMembershipProvider2/SingleSignOnRoleProvider2   The membership provider and role provider that operate in partial trust environments. These providers are included in Service Pack 2 of Windows Server 2003 R2.

##### SingleSignOnMembershipProvider/SingleSignOnRoleProvider

The following table provides examples of Web.config file entries for a Web SSO AD FS environment that uses the standard provider.

|  |  |
| --- | --- |
| Configuration steps | Description and example Web.config file entries |
| Turn on ASP.NET forms authentication. | <system.web>  <!-mode=[Windows|Forms|Passport|None]>  <authentication mode="Forms" />  </system.web> |
| Register the membership provider. | <membership defaultProvider="SingleSignOnMembershipProvider">  <providers>  <add  name="SingleSignOnMembershipProvider"  type="System.Web.Security.SingleSignOn.SingleSignOnMembershipProvider, System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"  fs="https://FEDERATIONSERVER/adfs/fs/federationserverservice.asmx"  />  </providers>  </membership>  For the fs attribute, replace FEDERATIONSERVER with the actual server name.  The membership element must be included within the system.web element of the Web.config file. |
| Register the role manager (optional). | <roleManager enabled="true" defaultProvider="SingleSignOnRoleProvider">  <providers>  <add  name="SingleSignOnRoleProvider"  type="System.Web.Security.SingleSignOn.SingleSignOnRoleProvider, System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"  fs="https://FEDERATIONSERVER/adfs/fs/federationserverservice.asmx"  />  </providers>  </roleManager>  For the fs attribute, you will need to replace FEDERATIONSERVER with the actual server name. |
| Register the HTTP module. | <httpModules>  <add name="Identity Federation Services Application Authentication Module" type="System.Web.Security.SingleSignOn.WebSsoAuthenticationModule, System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35, Custom=null" />  </httpModules> |

##### SingleSignOnMembershipProvider2/SingleSignOnRoleProvider2

If you are implementing the second AD FS provider set, the settings for registering the membership provider and role manager are different. The following table provides examples of Web.config file entries for a Web SSO AD FS environment that uses the provider that operates in partial trust environments.

|  |  |
| --- | --- |
| Configuration steps | Description and example Web.config file entries |
| Turn on ASP.NET forms authentication. | <system.web>  <!-mode=[Windows|Forms|Passport|None]>  <authentication mode="Forms" />  </system.web> |
| Register the membership provider. | <membership defaultProvider="SingleSignOnMembershipProvider2">  <providers>  <add name="SingleSignOnMembershipProvider2"  type="System.Web.Security.SingleSignOn.SingleSignOnMembershipProvider2, System.Web.Security.SingleSignOn.PartialTrust, Version=1.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"  fs=https://FEDERATIONSERVER/adfs/fs/federationserverservice.asmx  />  </providers>  </membership>  For the fs attribute, replace FEDERATIONSERVER with the actual server name.  The membership element must be included within the system.web element of the Web.config file. |
| Register the role manager (optional). | <roleManager enabled="true" defaultProvider="SingleSignOnRoleProvider2">  <providers>  <add  name="SingleSignOnRoleProvider2"  type="System.Web.Security.SingleSignOn.SingleSignOnRoleProvider2, System.Web.Security.SingleSignOn.PartialTrust, Version=1.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"  fs="https://FEDERATIONSERVER/adfs/fs/federationserverservice.asmx"  />  </providers>  </roleManager>  For the fs attribute, you will need to replace FEDERATIONSERVER with the actual server name. |
| Register the HTTP module. | <httpModules>  <add name="Identity Federation Services Application Authentication Module" type="System.Web.Security.SingleSignOn.WebSsoAuthenticationModule, System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35, Custom=null" />  </httpModules> |

# XVI Plan for and design security

In this chapter:

 [Chapter overview: Plan for and design security (Office SharePoint Server)](#DSDOC_3df68222_235b_45de_82fa_b89166c5c6)

 [Choose your security environment (Office SharePoint Server)](#DSDOC_753fc3f6_e888_4bb6_ab67_288df065c2)

 [Chapter overview: Plan server farm security (Office SharePoint Server)](#DSDOC_d449e995_a3eb_4191_9d37_7c5e96d9c9)

 [Plan secure configurations for Office SharePoint Server features](#DSDOC_e8493b73_ad1a_4642_8141_05405f0026)

 [Chapter overview: Plan environment-specific security (Office SharePoint Server)](#DSDOC_8e81f0f8_e68e_42c0_b9dc_ebe59bcb73)

 [Plan for security roles [Office SharePoint Server]](#DSDOC_81b06f7d_430f_4387_8a29_122cc5928f)

 [Plan for single sign-on](#DSDOC_3c78e886_5d20_44cb_b4e4_f823c4c019)

 Plan for accounts (Office SharePoint Server)

# Chapter overview: Plan for and design security (Office SharePoint Server)

This chapter provides a methodical approach to building security into your solution design for Microsoft Office SharePoint Server 2007. This approach is based on a foundation of the following security guides that are provided in [Microsoft patterns & practices](http://go.microsoft.com/fwlink/?LinkId=73704&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73704&clcid=0x409):

 [Securing Your Web Server](http://go.microsoft.com/fwlink/?LinkId=73705&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73705&clcid=0x409)

 [Securing Your Database Server](http://go.microsoft.com/fwlink/?LinkId=73706&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73706&clcid=0x409)

 [Securing Your Network](http://go.microsoft.com/fwlink/?LinkId=73707&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73707&clcid=0x409)

These guides explain practical secure configurations for specific server roles. The guidance for each server role includes recommended secure settings for the network, the operating system, and the applications that are installed, including Internet Information Services (IIS), Microsoft ASP.NET Framework, and Microsoft SQL Server.

The information in this chapter supplements the patterns & practices security guides in several ways:

 Provides recommendations for each server role within a server farm.

 Identifies additional networking, operating system, and application settings that are appropriate for server roles.

 Provides recommendations for securing the specific applications and features that are installed by Office SharePoint Server 2007.

 Targets security recommendations to security environments that are common for Office SharePoint Server 2007 solutions.

Plan for and design security by using the following steps:

1. Plan your security environment   The security guidance that is recommended for your organization depends on which environment best matches your intended use of Office SharePoint Server 2007. Use the following article to help plan your security environment:

 [Choose your security environment (Office SharePoint Server)](#DSDOC_753fc3f6_e888_4bb6_ab67_288df065c2) describes the four key security environments: internal team or department, internal IT-hosted, external secure collaboration, and external anonymous access.

2. Plan server farm security   Plan how to secure individual servers within a server farm. The patterns & practices security guides are used as a foundation for securing Office SharePoint Server 2007 environments. Use the following articles to help plan server farm security:

 [Review the secure topology design checklists (Office SharePoint Server)](#DSDOC_007ecb03_5808_495a_bb72_4f0641eaf8) to ensure that your topology and logical architecture meet the criteria for a secure design.

 [Plan for secure communication within a server farm [Office SharePoint Server]](#DSDOC_a29ecba7_813e_4815_bdc7_ca1e3517e4) to ensure that the methods of secure communication are most appropriate for your solution.

 [Plan security hardening for server roles within a server farm [Office SharePoint Server]](#DSDOC_763613ac_83f4_424e_99d0_32efd0667b) to determine the specific hardening settings for each of the server roles in your server farm.

3. Plan secure configurations for features   Plan how to configure Office SharePoint Server 2007 features in a secure manner. Use the following article to help plan secure configurations:

 [Plan secure configurations for Office SharePoint Server features](#DSDOC_e8493b73_ad1a_4642_8141_05405f0026) provides recommendations for securely configuring Office SharePoint Server 2007 features. The recommendations in this article are usually configured by using Central Administration, rather than in the network, operating system, IIS, or .NET Framework.

4. Plan environment-specific security   Plan security targeted to your specific environment. Use the following articles to help plan environment-specific security:

 [Plan security for an internal team or department environment (Office SharePoint Server)](#DSDOC_9e5d48a2_9f1a_4225_a03b_22cc2c49ff) provides additional security guidance targeted to the internal team or department environment.

 [Plan security for an internal IT-hosted environment (Office SharePoint Server)](#DSDOC_252afeb0_ac39_41a0_a680_2067e7e621) provides additional security guidance targeted to the internal IT-hosted environment.

 [Plan security for an external secure collaboration environment (Office SharePoint Server)](#DSDOC_a6ee7781_e2f1_4cf8_8f38_3a7ae2af74) provides additional security guidance targeted to the external secure collaboration environment.

 [Plan security for an external anonymous access environment (Office SharePoint Server)](#DSDOC_f507f5d6_4c9d_4f98_909f_069c53b9a3) provides additional security guidance targeted to the external anonymous access environment.

5. Plan security roles   Use the following article to plan for and design security roles:

 [Plan for security roles [Office SharePoint Server]](#DSDOC_81b06f7d_430f_4387_8a29_122cc5928f) describes planning roles for administrators and for users.

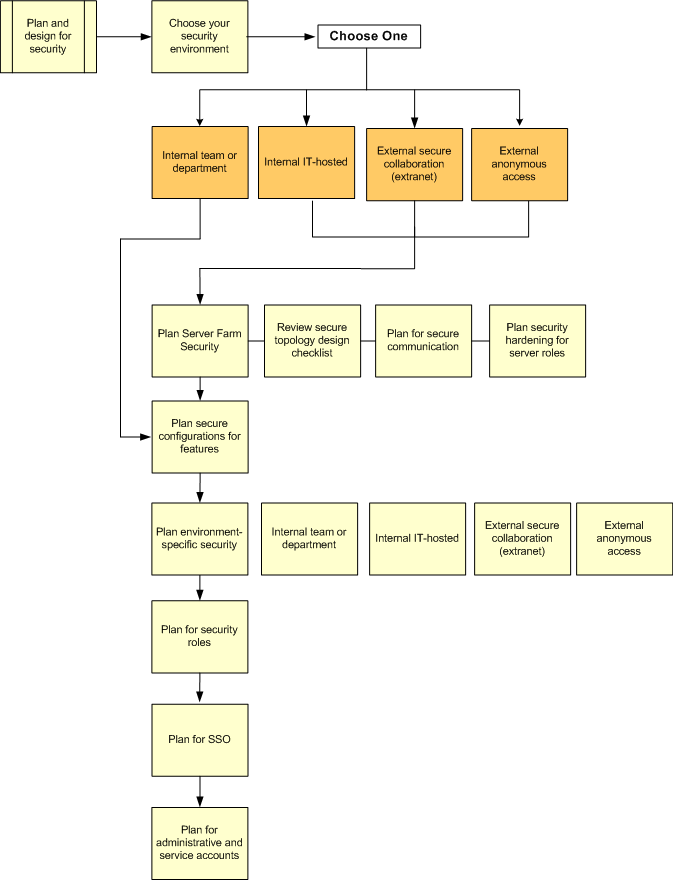
6. Plan for single sign-on   If you plan to connect to data sources outside of your server farm, single sign-on can be used to automatically authenticate users, rather than prompting for credentials. Use the following article to help plan for sign sign-on:

 [Plan for single sign-on](#DSDOC_3c78e886_5d20_44cb_b4e4_f823c4c019) describes using single sign-on in Office SharePoint Server 2007.

7. Plan for accounts   Use the following article to plan for administrative and service accounts:

 [Plan for administrative and service accounts (Office SharePoint Server)](#DSDOC_f07768d4_ca37_447a_a056_1a67d93ef5) provides requirements and recommendations for configuring administrative and service accounts.

Some of these planning articles are intended for specific security environments. The following figure shows the intended planning flow based on the security environment.



# Choose your security environment (Office SharePoint Server)

Use this article to identify the security environment that most closely matches your intended use of Microsoft Office SharePoint Server 2007.

The security guidance that is recommended for your organization depends on the environment. This article describes the following four security environments:

 [Internal team or department](#DSDOC_section1753fc3f6_e888_4bb6_ab67_28)

 [Internal IT-hosted](#DSDOC_section2753fc3f6_e888_4bb6_ab67_28)

 [External secure collaboration](#DSDOC_section3753fc3f6_e888_4bb6_ab67_28)

 [External anonymous access](#DSDOC_section4753fc3f6_e888_4bb6_ab67_28)

Review the description for each environment and identify the one that most closely matches your environment.

## Internal team or department

Security guidance for an internal team or department environment within a larger organization focuses on recommending practical security configurations and settings for a team or department that uses Office SharePoint Server 2007 for collaboration.

This environment is a one- or two-server deployment in which the servers are not hosted by the primary IT team within the organization. Although the guidance for this environment requires some IT knowledge, it is not necessary for server farm administrators to be IT specialists.

The guidance for the internal team or department environment relies on the security of the overall network environment. Many of the default settings are intended to be used with this environment.

This environment is not intended for multiple teams or projects where secure isolation of content is required. If your team or department requires secure isolation of content, a greater number of servers, or a greater level of security than is provided by your overall network environment, use the guidance for the internal IT-hosted environment.

If your environment most closely matches the internal team or department environment, go to the article [Plan secure configurations for Office SharePoint Server features](#DSDOC_e8493b73_ad1a_4642_8141_05405f0026).

## Internal IT-hosted

An internal IT-hosted environment is one in which an IT team hosts Web applications and sites for multiple teams and departments in an organization. Security guidance for this environment focuses on:

 Securing a server farm environment, including isolating content between groups.

 Securing server-to-server communication and client-server communication.

 Hardening servers for specific server roles.

 Securely configuring features.

Guidance for this environment assumes that all servers reside within a single internal network.

If your environment most closely matches the internal IT-hosted environment, go to [Chapter overview: Plan server farm security (Office SharePoint Server)](#DSDOC_d449e995_a3eb_4191_9d37_7c5e96d9c9). The three articles in this chapter describe designing solutions for security, securing server-to-server communication and client-server communication, and hardening servers for specific roles.

## External secure collaboration

An external secure collaboration environment is one in which content is hosted in an extranet so that contributors who do not have general access to your corporate network can collaborate on content. This environment enables external partners to participate in a workflow or to collaborate on content with employees in your organization. This environment is also intended to support remote employee access, where employees who are working from home or traveling can gain access to sites and data without logging on to the corporate network.

Security guidance for this environment focuses on:

 Isolating Web applications or content to ensure that users can view or have access to only the projects on which they are authorized to work.

 Authenticating and securing communication between contributors and the server farm.

 Protecting database servers from direct user interaction and securing the server farm against risks associated with hosting Internet-facing servers.

If your environment most closely matches the external secure collaboration environment, go to [Chapter overview: Plan server farm security (Office SharePoint Server)](#DSDOC_d449e995_a3eb_4191_9d37_7c5e96d9c9). The three articles in this chapter describe designing solutions for security, securing server-to-server communication and client-server communication, and hardening servers for specific roles.

## External anonymous access

An external anonymous access environment is one which allows anonymous access to content from the Internet while protecting the server farm from the risks associated with hosting Internet-facing servers. This environment can include multiple farms for testing, staging, and publishing content.

Security guidance for this environment focuses on:

 Making content anonymously available.

 Securing communication between farms when content is deployed to the publishing farm.

 Ensuring that content caching does not expose sensitive data.

 Protecting database servers from direct user interaction and securing the server farm against risks associated with hosting Internet-facing servers in an anonymous environment.

If your environment most closely matches the external anonymous access environment, go to [Chapter overview: Plan server farm security (Office SharePoint Server)](#DSDOC_d449e995_a3eb_4191_9d37_7c5e96d9c9). The three articles in this chapter describe designing solutions for security, securing server-to-server communication and client-server communication, and hardening servers for specific roles.

# A Plan server farm security (Office SharePoint Server)

Insert introduction here.

## Subhead

Insert section body here.

### Subhead

Insert section body here.

# Chapter overview: Plan server farm security (Office SharePoint Server)

Planning server farm security includes the following tasks:

 [Review the secure topology design checklists (Office SharePoint Server)](#DSDOC_007ecb03_5808_495a_bb72_4f0641eaf8)

 [Plan for secure communication within a server farm [Office SharePoint Server]](#DSDOC_a29ecba7_813e_4815_bdc7_ca1e3517e4)

 [Plan security hardening for server roles within a server farm [Office SharePoint Server]](#DSDOC_763613ac_83f4_424e_99d0_32efd0667b)

Use these tasks with the following security environments:

 Internal IT-hosted

 External secure collaboration

 External anonymous access

# Review the secure topology design checklists (Office SharePoint Server)

In this article:

 [Server topology design checklist](#DSDOC_section1007ecb03_5808_495a_bb72_4f)

 [Networking topology design checklist](#DSDOC_section2007ecb03_5808_495a_bb72_4f)

 [Logical architecture design checklist](#DSDOC_section3007ecb03_5808_495a_bb72_4f)

 [Operating system design checklist](#DSDOC_section4007ecb03_5808_495a_bb72_4f)

In Microsoft Office SharePoint Server 2007, successful server hardening depends on a server topology and logical architecture that are designed for targeted isolation and secure communication.

Previous planning articles address topology and logical architecture in depth. This article provides checklists that you can use to ensure that your plans meet the criteria for a secure design.

Use the secure topology design checklists with the following security environments:

 Internal IT hosted

 External secure collaboration

 External anonymous access

## Server topology design checklist

Review the following checklist to ensure that your plans meet the criteria for a secure server topology design.

|  |  |
| --- | --- |
| [ ] | The topology incorporates dedicated front-end Web servers. |
| [ ] | Servers that host application server roles and database server roles are protected from direct user access. |
| [ ] | The SharePoint Central Administration site is hosted on a dedicated application server, such as the index server. |

## Networking topology design checklist

Review the following checklist to ensure that your plans meet the criteria for a secure networking topology design.

|  |  |
| --- | --- |
| [ ] | All servers within the farm reside within a single data center and on the same vLAN. |
| [ ] | Access is allowed through a single point of entry, which is a firewall. |
| [ ] | For a more secure environment, the farm is separated into three tiers (front-end Web, application, and database), which are separated by routers or firewalls at each vLAN boundary. |

## Logical architecture design checklist

Review the following checklist to ensure that your plans meet the criteria for a secure logical architecture design.

|  |  |
| --- | --- |
| [ ] | At least one zone in each Web application uses NTLM authentication. This is required for the search account to crawl content within the Web application. For more information, see [Plan authentication methods [Office SharePoint Server]](#DSDOC_40117fda_70a0_4e3d_8cd3_0def768da1). |
| [ ] | Web applications are implemented by using host names instead of the randomly generated port numbers that are automatically assigned. Do not use Internet Information Services (IIS) host header bindings if the Web application will be hosting host-named site collections. |
| [ ] | Consider using separate Web applications for the following circumstances:   Your company policy requires process isolation for content and applications.   You are implementing sites that integrate with external data sources where the content provided by these data sources is sensitive or requires greater security. |
| [ ] | In a reverse proxy environment, consider using the default port for the public-facing network while using a nondefault port on your internal network. This can help prevent simple port attacks on your internal network that assume HTTP will always be on port 80. |
| [ ] | When deploying custom Web Parts, only trustworthy Web Parts are deployed within Web applications that host sensitive or secure content. This protects the sensitive content against intradomain scripting attacks. |
| [ ] | Separate application pool accounts are used for central administration and for each unique Web application. |

## Operating system design checklist

Review the following checklist to ensure that your plans meet the criteria for a secure operating system design.

|  |  |
| --- | --- |
| [ ] | The server operating system is configured to use the NTFS file system. |
| [ ] | Clocks on all servers within the farm are synchronized. |

# Plan for secure communication within a server farm [Office SharePoint Server]

In this article:

 [Plan server-to-server communication](#DSDOC_section1a29ecba7_813e_4815_bdc7_ca)

 [Plan client-server communication](#DSDOC_section2a29ecba7_813e_4815_bdc7_ca)

 [Plan for using SSL](#DSDOC_section3a29ecba7_813e_4815_bdc7_ca)

Use this article to plan server farm security. This article provides guidance on securing server-to-server communication and client-server communication.

The tasks in the article are appropriate for the following security environments:

 Internal IT hosted

 External secure collaboration

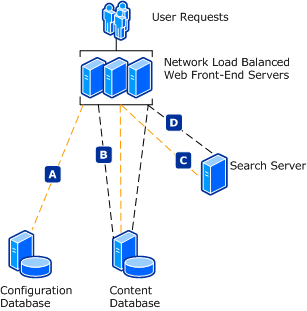
 External anonymous access

## Plan server-to-server communication

If your servers are not inside a physically secure data center where the network eavesdropping threat is considered insignificant, you need to use an encrypted communication channel to protect data sent between servers.

In Microsoft Office SharePoint Server 2007, server-to-server communication within a server farm is extensive. Securing this communication helps ensure that sensitive data is not compromised and also helps protect the servers from malicious attacks or unintentional threats.

The following figure shows several common communication transactions among servers in a farm.



Common communication transactions among servers in a farm include the following:

 Configuration changes   Front-end Web servers communicate with the configuration database to communicate configuration changes for farm settings.

 Change requests   User requests to add, delete, modify, or view content within a site are sent directly to the content database.

 Search requests   Front-end Web servers first communicate with the query server to generate results for search queries. Next, the front-end Web servers communicate with the content database to satisfy user requests for specific documents within the search results.

 Indexing   The indexing component communicates through a front-end Web server to crawl content in the content databases and build an index.

note_ddNote:

In an Office SharePoint Server 2007 environment, search is provided by two roles: query and index. These roles can be installed on different server computers.

Internet Protocol security (IPsec) and Secure Sockets Layer (SSL) can both be used to help protect communication between servers by encrypting traffic. Each of these methods works well. The choice of which method to use depends on the specific communication channels you are securing and the benefits and tradeoffs that are most appropriate for your organization.

### IPsec

IPsec is generally recommended for protecting the communication channel between two servers and restricting which computers can communicate with one another. For example, you can help protect a database server by establishing a policy that permits requests only from a trusted client computer, such as an application server or a Web server. You can also restrict communication to specific IP protocols and TCP/UDP ports.

The networking requirements and recommendations for a server farm make IPsec a good option because:

 All servers are contained on one physical LAN (to improve IPsec performance).

 Servers are assigned static IP addresses.

IPsec can also be used between trusted Windows Server 2003 or Windows 2000 Server domains. For example, you can use IPsec to secure communication of a Web server or application server in a perimeter network that connects to a computer running Microsoft SQL Server on an internal network. For more information, see [Selecting IPSec Authentication Methods](http://go.microsoft.com/fwlink/?LinkId=76093&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=76093&clcid=0x409) in the [Windows Server 2003 Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=76095&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=76095&clcid=0x409).

For more information about recommended environments for IPsec, see [Determining Your IPSec Needs](http://go.microsoft.com/fwlink/?LinkId=76094&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=76094&clcid=0x409) in the [Windows Server 2003 Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=76095&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=76095&clcid=0x409).

### SSL

The general recommendations for using SSL is to use this encryption method when you need granular channel protection for a particular application instead of for all applications and services running on a computer. SSL must be implemented by individual applications. Therefore, you cannot use SSL to encrypt all communications between two hosts.

Additionally, SSL is less flexible than IPsec because it only supports authentication by means of public key certificates. SSL does provide several distinct advantages, however. Most significantly, SSL is supported by a wide variety of servers and client computers, and the maturity of the standard has practically eliminated interoperability problems.

#### Scenarios to consider for SSL

There are several scenarios that make SSL a good option, including the following:

 Administration sites   The Central Administration site and Shared Services Administration sites can be secured by using SSL.

 Content deployment   The content deployment process copies files from one site directory on a server within an authoring or staging server farm to a matching site directory on one or more servers within a publishing server farm. In this scenario, IPsec might not be practical if server farms are in different network zones or if there is a high volume of content to deploy or a large number of servers to which to deploy the content. SSL can be used to target secure communication to these specific communication transactions.

 Intrafarm Shared Services Providers (SSPs)   If child farms are consuming shared services from a parent farm, sensitive data is shared between farms.

 Communication to external data sources   Several Office SharePoint Server 2007 features rely on connecting to servers that are external to the server farm. In these scenarios, data is shared between specific applications. While you can use IPsec to secure all of the communication among these servers, the network configuration, location of the external servers, and the platform of the external servers might make SSL a better option.

## Plan client-server communication

It might not be practical to secure all client-server communication. However, there are several scenarios that justify the extra configuration required to secure communication between client computers and servers within your server farm:

 Secure collaboration with partners   Partners access and contribute to applications in an extranet environment.

 Remote employee access   Employees access internal data remotely.

 Customers accessing or providing sensitive data   Customers log on and provide or gain access to sensitive data. For example, customers might be required to log on to an Internet news site or provide personal information to complete a business transaction.

 Basic or forms authentication   If you are using either of these methods of authentication, credentials are sent in the clear. At a minimum, secure the client-server communication for the logon page.

SSL is generally recommended to secure communications between users and servers when sensitive information must be secured. SSL can be configured to require server authentication or both server and client authentication.

## Plan for using SSL

SSL can decrease the performance of your network. There are several common guidelines that you can use to optimize pages that use SSL. First, use SSL only for pages that require it. This includes pages that contain or capture sensitive data, such as passwords or other personal data. Use SSL only if the following conditions are true:

 You want to encrypt the page data.

 You want to guarantee that the server to which you send the data is the server that you expect.

For pages where you must use SSL, follow these guidelines:

 Make the page size as small as possible.

 Avoid using graphics that have large file sizes. If you use graphics, use graphics that have smaller file sizes and resolution.

# Plan security hardening for server roles within a server farm [Office SharePoint Server]

In this article:

 [About security hardening](#DSDOC_section1763613ac_83f4_424e_99d0_32)

 [Application server recommendations](#DSDOC_section2763613ac_83f4_424e_99d0_32)

 [Secure communication with the Microsoft SQL Server database](#DSDOC_section3763613ac_83f4_424e_99d0_32)

 [File and Printer Sharing service requirements](#DSDOC_section4763613ac_83f4_424e_99d0_32)

 [Single sign-on hardening requirements](#DSDOC_section5763613ac_83f4_424e_99d0_32)

 [Restricting DCOM ports](#DSDOC_section6763613ac_83f4_424e_99d0_32)

 [Service requirements for e-mail integration](#DSDOC_section7763613ac_83f4_424e_99d0_32)

 [Service requirements for session state](#DSDOC_section8763613ac_83f4_424e_99d0_32)

 [Office SharePoint Server services](#DSDOC_section9a763613ac_83f4_424e_99d0_3)

 [Accounts and groups](#DSDOC_section10763613ac_83f4_424e_99d0_3)

 [Web.config file](#DSDOC_section11763613ac_83f4_424e_99d0_3)

 [Secure snapshot additions](#DSDOC_section12763613ac_83f4_424e_99d0_3)

Use this article to plan server farm security. The tasks in the article are appropriate for the following security environments:

 Internal IT hosted

 External secure collaboration

 External anonymous access

## About security hardening

In a server farm environment, individual servers play specific roles. Security hardening recommendations for these servers depend on the role each plays.

The server hardening recommendations are built on top of the recommendations provided in the following security guides that are provided in [Microsoft patterns & practices](http://go.microsoft.com/fwlink/?LinkId=73704&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73704&clcid=0x409):

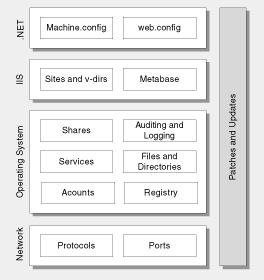
 [Securing Your Web Server](http://go.microsoft.com/fwlink/?LinkId=73705&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73705&clcid=0x409)

 [Securing Your Database Server](http://go.microsoft.com/fwlink/?LinkId=73706&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73706&clcid=0x409)

 [Securing Your Network](http://go.microsoft.com/fwlink/?LinkId=73707&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73707&clcid=0x409)

These guides follow a methodical approach to securing servers for specific roles and for securing the supporting network. The order in which settings are applied and applications are installed and hardened is prescribed as well, starting with applying patches and updates, then hardening networking settings and operating system settings, and then followed by application-specific hardening. For example, [Securing Your Web Server](http://go.microsoft.com/fwlink/?LinkId=73705&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73705&clcid=0x409) recommends that you install and harden Internet Information Services (IIS) only after patching and hardening the operating system. Additionally, this guide prescribes installing the Microsoft .NET Framework only after IIS is fully patched and hardened.

The categories of security settings that are methodically prescribed in [Securing Your Web Server](http://go.microsoft.com/fwlink/?LinkId=73705&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73705&clcid=0x409) are detailed in the following figure.



Additionally, each of the three guides includes a secure snapshot and a list of recommended security settings for either the specific server role or for the network. The snapshot lists are organized by categories that correspond to security settings illustrated in the preceding figure.

The security design and hardening guidance provided in this article is based on the guidance published in these three guides. This guidance assumes that you will use these guides as a baseline for securing and hardening your server farm.

This article describes the exceptions or additions to the snapshots that are recommended for your environment. These are detailed in table format by using the same categories and order as the three security guides. This format is intended to make it easy to identify and apply specific recommendations as you use the guides.

The guide [Deployment for Office SharePoint 2007](http://go.microsoft.com/fwlink/?LinkId=76139&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=76139&clcid=0x409) includes instructions for applying specific security guidance that is not covered in the patterns & practices security guides.

The nature of server-to-server communication within a server farm and the specific features provided by Microsoft Office SharePoint Server 2007 are the primary reasons for specific hardening recommendations. This article also describes how key communication channels and Office SharePoint Server 2007 features affect security requirements.

## Application server recommendations

In Office SharePoint Server 2007, application server roles are not typical middle-tier application servers that are packaged inside Enterprise Services applications. Consequently, the recommendations in [Securing Your Application Server](http://msdn.microsoft.com/library/en-us/dnnetsec/html/THCMCh17.asp?frame=true) do not apply for Office SharePoint Server 2007 application servers. Instead, use the guidance provided in [Securing Your Web Server](http://go.microsoft.com/fwlink/?LinkId=73705&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73705&clcid=0x409) to harden Office SharePoint Server 2007 application servers:

 Apply the guidance for networking and operating system settings to all application servers in the server farm. This guidance is contained in the following categories: patches and updates, services, protocols, accounts, files and directories, shares, ports, registry, and auditing and logging.

 Apply the guidance for hardening IIS and other Web settings only on the application server that hosts the Central Administration Web site. This guidance includes the following categories: IIS, Machine.config, code access security, LocalIntranet\_Zone, and Internet\_Zone.

In addition to using the secure snapshot in [Securing Your Web Server](http://go.microsoft.com/fwlink/?LinkId=73705&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73705&clcid=0x409), also apply the recommendations provided in the [Secure snapshot additions](#DSDOC_section12763613ac_83f4_424e_99d0_3) section later in this article.

## Secure communication with the Microsoft SQL Server database

[Securing Your Database Server](http://go.microsoft.com/fwlink/?LinkId=73706&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73706&clcid=0x409) recommends restricting access to two default Microsoft SQL Server communications ports: TCP port 1433 and UDP port 1434. For secure server farm environments, the recommendation is to:

 Block UDP port 1434 entirely.

 Configure SQL Server named instances to listen on a nonstandard port (other than TCP port 1433 or UDP port 1434).

 For additional security, block TCP port 1433 and reassign the port used by the default instance to a nonstandard port.

 Configure SQL client aliases on all front-end Web servers and application servers in the server farm. After you block TCP port 1433 or UDP port 1434, SQL client aliases are necessary on all computers that communicate with the SQL Server computer.

This approach provides a much higher degree of control over how SQL Server is deployed and run, including the ability to ensure that only authorized computers can communicate with the SQL Server computer.

The hardening steps for creating a SQL client alias must be completed prior to installing Office SharePoint Server 2007. When you run Setup for Office SharePoint Server 2007 and you are prompted to enter the name of the SQL Server computer to which to connect, you will need to enter the name of the SQL client alias.

### Blocking the standard SQL Server ports

The specific ports used to connect to SQL Server are affected by whether databases are installed on a default instance of SQL Server or a named instance of SQL Server. The default instance of SQL Server listens for client requests on TCP port 1433. A named instance of SQL Server listens on a randomly assigned port number. Additionally, the port number for a named instance can be reassigned if the instance restarts (depending on if the previously assigned port number is available).

By default, client computers that connect to SQL Server first connect by using TCP port 1433. If this communication is unsuccessful, then the client computers query the SQL Server Resolution Service listening on UDP port 1434 to determine on which port the database instance is listening.

The default port-communication behavior of SQL Server introduces several issues that affect server hardening. First, the ports used by SQL Server are well-publicized ports and the SQL Server Resolution Service has been the target of buffer overrun attacks and denial-of-service attacks, including the "Slammer" worm virus. Even if SQL Server is patched to mitigate security issues in the SQL Server Resolution Service, the well-publicized ports remain a target. Second, if databases are installed on a named instance of SQL Server, the corresponding communication port is randomly assigned and can change. This behavior can potentially prevent server-to-server communication in a hardened environment. The ability to control which TCP ports are open or blocked is essential to securing your environment.

Consequently, the recommendation for a server farm is to assign static port numbers to named instances of SQL Server and to block UDP port 1434 to prevent potential attackers from accessing the SQL Server Resolution Service. Additionally, consider reassigning the port used by the default instance and blocking TCP port 1433 as well.

There are several methods you can use to block ports. You can block these ports by using a firewall. However, unless you can be sure that there are no other routes into the network segment and that there are no malicious users that have access to the network segment, the recommendation is to block these ports directly on the server that hosts SQL Server. This can be accomplished by using Windows Firewall in Control Panel.

### Configuring SQL Server database instances to listen on a nonstandard port

SQL Server provides the ability to reassign the ports that are used by the default instance and any named instances. In SQL Server 2000, you reassign ports by using SQL Server Network Utility. In SQL Server 2005, you reassign ports by using SQL Server Configuration Manager.

### Configuring SQL client aliases

In a server farm, all front-end Web servers and application servers are SQL Server client computers. If you block UDP port 1434 on the SQL Server computer or you change the default port for the default instance, you must configure a SQL client alias on all servers that connect to the SQL Server computer.

To connect to an instance of SQL Server 2000, you install the SQL Server client tools on the target computer and then configure the SQL client alias. You install these by running Setup for SQL Server and selecting SQL Server Client Tools.

To connect to an instance of SQL Server 2005, you install SQL Server client components on the target computer and then configure the SQL client alias by using SQL Server Configuration Manager. To install SQL Server client components, run Setup and select only the following client components to install:

 Connectivity Components

 Management Tools (includes SQL Server Configuration Manager)

SQL Server client components work with SQL Server 2000 and can be used instead of the SQL Server client tools.

### Hardening steps

#### Configure SQL Server

##### Configure a SQL Server 2000 instance to listen on a nondefault port

Use SQL Server Network Utility to change the TCP port that is used by an instance of SQL Server 2000.

1. On the SQL Server computer, run SQL Server Network Utility.

2. On the Instance(s) on this server menu, select the instance. Ensure that you have selected the intended instance. By default, the default instance listens on port 1433. Named instances of SQL Server 2000 are assigned a random port number, so you might not know the current port number assigned to a named instance when you run SQL Server Network Utility.

3. In the Enabled Protocols pane on the right side of the SQL Server Network Utility interface, click TCP/IP, and then click Properties.

4. In the Network Protocol Default Value Setup dialog box, change the TCP port number. Avoid using any of the well-known TCP ports. For example, select a higher-range port number, such as 40000. Do not select the Hide Server check box.

5. Click OK.

6. In the SQL Server Network Utility dialog box, click OK. You will receive a message indicating that the change will not take effect until the SQL Server service is restarted. Click OK.

7. Restart the SQL Server service and confirm that your SQL Server computer is listening on the port you selected. You can confirm this by looking in the event viewer log after restarting the SQL Server service. Look for an information event similar to the following event:

Event Type:Information

Event Source:MSSQLSERVER

Event Category:(2)

Event ID:17055

Date:3/6/2008

Time:11:20:28 AM

User:N/A

Computer:computer\_name

Description:

19013:

SQL Server listening on 10.1.2.3: 40000

##### Configure a SQL Server 2005 instance to listen on a nondefault port

Use SQL Server Configuration Manager to change the TCP port that is used by an instance of SQL Server 2005.

1. Use SQL Server Configuration Manager to change the TCP port that is used by an instance of SQL Server 2005.

2. On the SQL Server computer, open SQL Server Configuration Manager.

3. In the left pane, expand SQL Server 2005 Network Configuration.

4. Under SQL Server 2005 Network Configuration, click the corresponding entry for the instance that you are configuring. The default instance is listed as Protocols for MSSQLSERVER. Named instances will appear as Protocols for named\_instance.

5. In the right pane, right-click TCP/IP and click Properties.

6. Click the IP Addresses tab. For every IP address assigned to the SQL Server computer, there is a corresponding entry on this tab. By default, SQL Server is listening on all IP addresses assigned to the computer.

7. To globally change the port that the default instance is listening on, perform the following:

a. For each IP except IPAll, clear all values for both TCP dynamic ports and TCP Port.

b. For IPAll, clear the value for TCP dynamic ports. In the TCP Port field, enter the port that you want the instance of SQL Server to listen on. For example, enter 40000.

8. To globally change the port that a named instance is listening on, perform the following:

a. For each IP including IPAll, clear all values for TCP dynamic ports. A value of 0 for this field indicates that SQL Server uses a dynamic TCP port for the IP address. A blank entry for this value means that SQL Server 2005 will not use a dynamic TCP port for the IP address.

b. For each IP except IPAll, clear all values for TCP Port.

c. For IPAll, clear the value for TCP dynamic ports. In the TCP Port field, enter the port that you want the instance of SQL Server to listen on. For example, enter 40000.

9. Click OK. You will receive a message indicating that the change will not take effect until the SQL Server service is restarted. Click OK.

10. Close SQL Server Configuration Manager.

11. Restart the SQL Server service and confirm that the SQL Server computer is listening on the port you selected. You can confirm this by looking in the event viewer log after restarting the SQL Server service. Look for an information event similar to the following event:

Event Type:Information

Event Source:MSSQL$MSSQLSERVER

Event Category:(2)

Event ID:26022

Date:3/6/2008

Time:1:46:11 PM

User:N/A

Computer:computer\_name

Description:

Server is listening on [ 'any' <ipv4>50000]

#### Configure Windows Firewall

##### Configure Windows Firewall to block default SQL Server listening ports

1. In Control Panel, open Windows Firewall.

2. On the General tab, click On. Ensure that the Don't allow exceptions check box is cleared.

3. On the Exceptions tab, click Add Port.

4. On the Add a Port dialog box, enter a name for the port. For example, enter UDP-1434. Then, enter the port number. For example, enter 1434.

5. Select the appropriate option button: UDP or TCP. For example, to block port 1434, click UDP. To block port 1433, click TCP.

6. Click Change Scope and ensure that the scope for this exception is set to Any computer (including those on the Internet).

7. Click OK.

8. On the Exceptions tab, locate the exception you created. To block the port, clear the check box for this exception. By default, this check box is selected, which means that the port is open.

##### Configure Windows Firewall to open manually assigned ports

1. Follow steps 1-7 in the previous procedure to create an exception for the port you manually assigned to a SQL instance. For example, create an exception for TCP port 40000.

2. On the Exceptions tab, locate the exception you created. Ensure that the check box for the exception is checked. By default, this check box is selected, which means that the port is open.

note_ddNote:

For more information about using Internet Protocol security (IPsec) to secure communication to and from your SQL Server computer, see the Microsoft Knowledge Base article 233256: [How to Enable IPSec Traffic Through a Firewall](http://go.microsoft.com/fwlink/?LinkId=76142&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=76142&clcid=0x409).

#### Configure a SQL client alias

##### Configure a SQL client alias

If you block UDP port 1434 or TCP port 1433 on the SQL Server computer, you must create a SQL client alias on all other computers in the server farm. You can use SQL Server client components to create a SQL client alias for computers that connect to SQL Server 2000 or SQL Server 2005.

1. Run Setup for SQL Server 2005 on the target computer and select the following client components to install:

a. Connectivity Components

b. Management Tools

2. Open SQL Server Configuration Manager.

3. In the left pane, click SQL Native Client Configuration.

4. In the right pane, right-click Aliases, and select New Alias.

5. In the Alias dialog box, enter a name for the alias and then enter the port number for the database instance. For example, enter SharePoint\_alias.

6. In the Port No field, enter the port number for the database instance. For example, enter 40000. Ensure that the protocol is set to TCP/IP.

7. In the Server field, enter the name of the SQL Server computer.

8. Click Apply, and then click OK.

##### Test the SQL client alias

Test connectivity to the SQL Server computer by using Microsoft SQL Server Management Studio, which is available by installing SQL Server client components.

1. Open SQL Server Management Studio.

2. When you are prompted to enter a server name, enter the name of the alias that you created, and then click Connect. If the connection is successful, SQL Server Management Studio is populated with objects that correspond to the remote database.

note_ddNote:

To check connectivity to additional database instances from within SQL Server Management Studio, click the Connect button and select Database Engine.

## File and Printer Sharing service requirements

Several core features depend on the File and Printer Sharing service and the corresponding protocols and ports. These include, but are not limited to, the following:

 Setup   This uses the File and Printer Sharing service to copy files and create databases, such as the configuration database.

 Search queries   All search queries require the File and Printer Sharing service.

 Crawling and indexing content   To crawl content, the index component sends requests through the front-end Web server. The front-end Web server communicates with content databases directly and sends results back to the index server. This communication requires the File and Printer Sharing service.

 Index propagation   If the query role is installed on a different server than the index role, the index server copies content indexes to the query servers. This action requires the File and Printer Sharing service and the corresponding protocols and ports.

 Excel Services   Excel Services uses the protocols and ports used by the File and Printer Sharing service to receive Microsoft Excel workbooks over a UNC path.

The File and Printer Sharing service requires the use of named pipes. Named pipes can communicate by using either direct-hosted SMB or NBT protocols. For a secure environment, direct-hosted SMB is recommended instead of NBT. The hardening recommendations provided in this article assume that SMB is used.

The following table describes the hardening requirements that are introduced by the dependency on the File and Printer Sharing service.

|  |  |  |
| --- | --- | --- |
| Category | Requirement | Notes |
| Services | File and Printer Sharing | Requires use of named pipes. |
| Protocols | Named pipes that use direct-hosted SMB  Disable NBT | Named pipes can use NBT instead of direct-hosted SMB. However, NBT is not considered as secure as direct-hosted SMB. |
| Ports | TCP/UDP port 445 | Used by direct-hosted SMB. |

For more information about disabling NBT, see the Microsoft Knowledge Base article 204279: [Direct hosting of SMB over TCP/IP](http://go.microsoft.com/fwlink/?LinkId=76143&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=76143&clcid=0x409).

## Single sign-on hardening requirements

The single sign-on (SSO) feature in Office SharePoint Server 2007 is used to connect to data sources that reside outside the server farm. By default, the SSO feature is not enabled on an Office SharePoint Server 2007 server farm. Do not configure SSO unless you require this feature to connect to external data sources. Because the SSO feature requires user authentication, this feature does not work in an external anonymous access environment.

SSO relies on the Microsoft Single Sign-On service and the corresponding protocols and ports. This service must be enabled on all front-end Web servers and the designated encryption-key server, a role that is typically hosted by an application server.

The SSO feature introduces several hardening requirements for the server farm. The Single Sign-On service uses remote procedure call (RPC). RPC uses port 135. It also uses a dynamically assigned port in the range of 1024–65535/TCP. This is referred to as dynamic RPC. It is possible to use a Windows registry key to limit the range of the dynamic RPC ports assigned. Rather than using all of the high-numbered ports (1024–65535), you can limit the range of dynamic RPC ports to a much smaller number. This is referred to as static RPC. For more information, see [Active Directory in Networks Segmented by Firewalls](http://www.microsoft.com/downloads/details.aspx?FamilyID=c2ef3846-43f0-4caf-9767-a9166368434e&displaylang=en) (http://go.microsoft.com/fwlink/?LinkId=76147&clcid=0x409).

For more information about dynamic RPX ports, see the Microsoft Knowledge Base article 154596: [How to configure RPC dynamic port allocation to work with firewalls](http://go.microsoft.com/fwlink/?LinkId=76145&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=76145&clcid=0x409).

The following table lists the hardening requirements that are introduced by SSO. These requirements apply to all servers within the server farm.

|  |  |  |
| --- | --- | --- |
| Category | Requirement | Notes |
| Services | Single Sign-On service | Requires use of the RPC protocol. |
| Protocols | RPC | Configure static RPC to limit the range of ports used by dynamic RPC. |
| Ports | TCP port 135 plus the port range that you configure for dynamic RPC |  |

While these hardening requirements are configured in the operating system, the order in which the requirements are configured is critical to the successful deployment of SSO. The requirements for protocols and ports can be configured at any time prior to configuring the SSO feature in Office SharePoint Server 2007. However, the order in which the Single Sign-On service is enabled on servers in the farm affects the configuration of SSO.

The first server that you enable the service on becomes the encryption-key server for the server farm. This server stores the encryption key. The recommendation is to host this role on one of the application servers. The Single Sign-On service must also be enabled on each front-end Web server in the server farm. These computers forward credentials to the encryption-key server.

Successful configuration of the SSO feature in Office SharePoint Server 2007 requires configuration in the Central Administration site in addition to enabling the Single Sign-On service. Consequently, do not enable the Single Sign-On service before installing Office SharePoint Server 2007. For more information about configuring SSO, see the article [Plan for single sign-on](#DSDOC_3c78e886_5d20_44cb_b4e4_f823c4c019).

## Restricting DCOM ports

DCOM over RPC is used by Office SharePoint Server 2007 as a communications channel. By default, DCOM uses dynamic RPC port allocation, which randomly selects port numbers greater than 1024. In addition, port 135 is used by the RPC endpoint mapping service. You can restrict the ports required to support DCOM on the internal firewall in two ways:

 Define port ranges   This allows you to control the ports dynamically allocated by RPC. For more information about dynamic port restrictions, see the Microsoft Knowledge Base article 300083: [How To Restrict TCP/IP Ports on Windows 2000 and Windows XP](http://go.microsoft.com/fwlink/?LinkId=76148&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=76148&clcid=0x409).

 Use static endpoint mapping   Windows 2000 Server SP3 (or QFE 18.1 and later) or Windows Server 2003 allows you to configure Enterprise Services applications to use a static endpoint. Static endpoint mapping means that you only need to open two ports in the firewall: port 135 for RPC and a nominated port for your Enterprise Services application. For more information about static endpoint mapping, see the Microsoft Knowledge Base article 312960: [Cannot s](http://go.microsoft.com/fwlink/?LinkId=76149&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=76149&clcid=0x409).

The recommendation to restrict DCOM ports applies to all servers within the server farm.

## Service requirements for e-mail integration

E-mail integration requires the use of two services:

 Simple Mail Transfer Protocol (SMTP) service

 Microsoft SharePoint Directory Management Service

### SMTP service

E-mail integration requires the use of the SMTP service on at least one of the front-end Web servers in the server farm. The SMTP service is required for incoming e-mail. For outgoing e-mail, you can either use the SMTP service or route outgoing e-mail through a dedicated e-mail server in your organization, such as a Microsoft Exchange Server computer.

### Microsoft SharePoint Directory Management Service

Office SharePoint Server 2007 includes an internal service, the Microsoft SharePoint Directory Management Service, for creating e-mail distribution groups. When you configure e-mail integration, you have the option to enable the Directory Management Service feature, allowing users to create distributions lists. When users create a SharePoint group and they select the option to create a distribution list, the Microsoft SharePoint Directory Management Service creates the corresponding Active Directory directory service distribution list in the Active Directory environment.

In security-hardened environments, the recommendation is to restrict access to the Microsoft SharePoint Directory Management Service by securing the file associated with this service, which is SharePointEmailws.asmx. For example, allow access to this file by the server farm account only.

Additionally, this service requires permissions in the Active Directory environment to create Active Directory distribution list objects. The recommendation is to setup a separate organizational unit in Active Directory for SharePoint objects. Only this organizational unit should allow write access to the account used by the Microsoft SharePoint Directory Management Service.

## Service requirements for session state

Both Microsoft Office Project Server 2007 and Microsoft Office Forms Server 2007 maintain session state. If you are deploying these features or products within your server farm, do not disable the ASP.NET State service. Additionally, if you are deploying InfoPath Forms Services, do not disable the View State service.

## Office SharePoint Server services

Do not disable services that are installed by Office SharePoint Server 2007.

The following services are installed on all front-end Web servers and application servers and appear in the Microsoft Management Console (MMC) Services snap-in (alphabetical order):

 Office SharePoint Server Search

 Windows SharePoint Services Administration

 Windows SharePoint Services Search

 Windows SharePoint Services Timer

 Windows SharePoint Services Tracing

 Windows SharePoint Services VSS Writer

If your environment disallows services that run as a local system, you can consider disabling the Windows SharePoint Services Administration service only if you are aware of the consequences and can work around these. This service is a Win32 service that runs as a local system.

This service is used by the Windows SharePoint Services Timer service to perform actions that require administrative privileges on the server, such as create IIS Web sites, deploy code, and stop and start services. If you disable this service, you cannot run deployment-related tasks from the Central Administration site. You will need to use the Stsadm.exe command-line tool and run the execadminsvcjobs command to complete multi-server deployments for Windows SharePoint Services 3.0 and to run other deployment-related tasks.

## Accounts and groups

The secure snapshots in the patterns & practices security guides provide recommendations for securing accounts and groups.

For recommendations on planning for accounts, see [Plan for administrative and service accounts (Office SharePoint Server)](#DSDOC_f07768d4_ca37_447a_a056_1a67d93ef5).

For recommendations on planning for administrative and user roles, see [Plan for security roles [Office SharePoint Server]](#DSDOC_81b06f7d_430f_4387_8a29_122cc5928f).

## Web.config file

The .NET Framework, and ASP.NET in particular, uses XML-formatted configuration files to configure applications. The .NET Framework relies on configuration files to define configuration options. The configuration files are text-based XML files. Multiple configuration files can, and typically do, exist on a single system.

System-wide configuration settings for the .NET Framework are defined in the Machine.config file. The Machine.config file is located in the %SystemRoot%\Microsoft.NET\Framework\%VersionNumber%\CONFIG\ folder. The default settings that are contained in the Machine.config file can be modified to affect the behavior of applications that use the .NET Framework on the whole system. For recommendations about configuring Machine.config files, see [Securing Your Web Server](http://go.microsoft.com/fwlink/?LinkId=73705&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73705&clcid=0x409).

You can change the ASP.NET configuration settings for a single application if you create a Web.config file in the root folder of the application. When you do this, the settings in the Web.config file override the settings in the Machine.config file.

When you extend a Web application by using Central Administration, Office SharePoint Server 2007 automatically creates a Web.config file for the Web application.

The [Secure snapshot additions](#DSDOC_section12763613ac_83f4_424e_99d0_3) section later in this article lists recommendations for configuring Web.config files. These recommendations are intended to be applied to each Web.config file that is created, including the Web.config file for the Central Administration site.

For more information about ASP.NET configuration files and editing a Web.config file, see [ASP.NET Configuration](http://go.microsoft.com/fwlink/?LinkID=73257&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkID=73257&clcid=0x409).

## Secure snapshot additions

This section lists the additions to snapshots in the patterns & practices security guides that are recommended for Office SharePoint Server 2007 environments. These are detailed in table format by using the same categories and order as the patterns & practices security guides.

This format is intended to make it easy to identify and apply specific recommendations as you use the patterns & practices security guides. Except for a few noted exceptions, these hardening recommendations are intended to be applied before running Setup for Office SharePoint Server 2007.

The following table describes recommendations for securing your network additions.

|  |  |
| --- | --- |
| Component | Characteristic exception |
| All | No additional recommendations |

The following table describes recommendations for securing your Web server additions.

|  |  |
| --- | --- |
| Component | Characteristic |
| Services | Enable:   File and Printer Sharing   Office SharePoint Server Search   Single Sign-On service (only if using SSO)   ASP.NET State service (if using InfoPath Forms Server or Project Server)   View State service (if using InfoPath Forms Server)   World Wide Web Publishing Service  Ensure these services remain enabled after running Setup:   Office SharePoint Server Search   Windows SharePoint Services Administration   Windows SharePoint Services Search   Windows SharePoint Services Timer   Windows SharePoint Services Tracing   Windows SharePoint Services VSS Writer |
| Protocols | Enable:   SMB   SMTP (if using integrated e-mail)   RPC (only if using SSO)  Disable:   NBT |
| Accounts |  If the Microsoft Directory Management Service is enabled as part of e-mail integration, configure your Active Directory environment to allow write access to the account used by the Microsoft Directory Management Service (the server farm account).   For additional guidance on configuring accounts, see [Plan for administrative and service accounts (Office SharePoint Server)](#DSDOC_f07768d4_ca37_447a_a056_1a67d93ef5) for Office SharePoint Server 2007 account requirements and recommendations. |
| Files and directories | If e-mail integration is enabled and the Directory Management Service feature is turned on, restrict access to the Microsoft SharePoint Directory Management service by securing the file associated with this service: SharePointEmailws.asmx. For example, allow access to this file only to the server farm account. |
| Shares | No additional recommendations |
| Ports |  Open TCP/UDP port 445.   Open TCP port 135 plus ports in the range that you specify when you configure static RPC (only if using SSO).   If UDP port 1434 is blocked on the SQL Server computer and databases are installed on a named instance, configure a SQL client alias for connecting to the named instance.   If TCP port 1433 is blocked on the SQL Server computer and databases are installed on the default instance, configure a SQL client alias for connecting to the named instance.   Ensure that ports remain open for Web applications that are accessible to users.   Block external access to the port used for the Central Administration site.   Restrict DCOM ports by either defining port ranges or by using static endpoint mapping. |
| Registry | If using SSO, edit the registry to configure static RPC. |
| Auditing and logging | If log files are relocated, ensure that the log file locations are updated to match. |
| IIS | See guidance for IIS below. |
| Sites and virtual directories | No additional recommendations |
| Script mappings | No additional recommendations |
| ISAPI filters | No additional recommendations |
| IIS metabase | No additional recommendations |
| .NET Framework | See guidance for .NET Framework below. |
| Machine.config: HttpForbiddenHandler | No additional recommendations |
| Machine.config: Remoting | No additional recommendations |
| Machine.config: Trace | No additional recommendations |
| Machine.config: compilation | No additional recommendations |
| Machine.config: customErrors | No additional recommendations |
| Machine.config: sessionState | No additional recommendations |
| Code access security | Ensure that you have a minimal set of code access security permissions enabled for your Web application. (The <trust> element in Web.config for each Web application should be set to WSS\_Minimal (where WSS\_Minimal has its low defaults as defined in 12\config\wss\_minimaltrust.config) or your own custom policy file, which is minimally set.) |
| LocalIntranet\_Zone | No additional recommendations |
| Internet\_Zone | No additional recommendations |
| Web.config | Apply the following recommendations to each Web.config file that is created after running Setup:   Do not allow compilation or scripting of database pages via the PageParserPaths elements.   Ensure <SafeMode> CallStack=""false"" and AllowPageLevelTrace=""false"".   Ensure that the Web Part limits around maximum controls per zone is set low.   Ensure that the SafeControls list is set to the minimum set of controls needed for your sites.   Ensure that your Workflow SafeTypes list is set to the minimum level of SafeTypes needed.   Ensure that customErrors is turned on (<customErrors mode=""On""/>).   Consider your Web proxy settings as needed (<system.net>/<defaultProxy>).   Set the upload.aspx limit to the highest size you reasonably expect users to upload (default is 2 GB). Performance of can be affected by uploads greater than 100 MB. |

The following table describes recommendations for securing your database server additions.

|  |  |
| --- | --- |
| Component | Characteristic exception |
| Services | Enabled:   Windows Firewall/Internet Connection Sharing (ICS) (if you are using Windows Firewall to block standard SQL ports)   File and Printer Sharing   Single Sign-On service (only if using SSO) |
| Protocols | Enable:   Named pipes that use direct-hosted SMB   RPC (only if using SSO)  Disable:   NBT |
| Accounts | Manually remove unused accounts regularly. |
| Files and directories | No additional recommendations |
| Shares | No additional recommendations |
| Ports |  Block UDP port 1434. Consider blocking TCP port 1433.   Allow port 445.   Open TCP port 135 plus ports in the range that you specify when you configure static RPC (only if using SSO).   Restrict DCOM ports by either defining port ranges or by using static endpoint mapping.   Ensure that ports required for front-end Web servers and application servers to communicate with the database server remain open (TCP/UDP ports 135-139 and 445). |
| Registry | If using SSO, edit the registry to configure static RPC. |
| Auditing and logging | No additional recommendations |
| SQL Server settings | See guidance for SQL Server settings below. |
| SQL Server security | No additional recommendations |
| SQL Server logins, users, and roles | No additional recommendations |
| SQL Server database objects | No additional recommendations |

# Plan secure configurations for Office SharePoint Server features

In this article:

 [Recommendations for Office SharePoint Server features](#DSDOC_section1e8493b73_ad1a_4642_8141_05)

Use this article to find recommendations for configuring and managing Microsoft Office SharePoint Server 2007 features in a more secure manner. You will usually perform the recommended configurations in Central Administration, rather than in the network, operating system, Internet Information Services (IIS), or the Microsoft .NET Framework. The recommendations in this article are appropriate for the following security environments:

 Internal team or department

 Internal IT hosted

 External secure collaboration

 External anonymous access

For more information about these environments, see [Choose your security environment (Office SharePoint Server)](#DSDOC_753fc3f6_e888_4bb6_ab67_288df065c2).

## Recommendations for Office SharePoint Server features

The following table describes secure recommendations for Office SharePoint Server 2007 features.

|  |  |
| --- | --- |
| Feature or area | Description and recommendation |
| Authentication |  Do not use client-side automatic logon when using the Central Administration site.   Allow only front-end Web server computers to perform authentication of users. Do not allow end-user accounts or groups to authenticate against the database server computer. |
| Authorization | Assign permissions to groups instead of individual accounts. |
| Permission levels | Assign users the least permissions required to complete their tasks. |
| Administration | Use access permissions to secure the Central Administration site and allow administrators to connect to the site remotely (as opposed to enabling the Central Administration site for local computer use only). This alleviates the requirement for administrators to log on locally to the computer that is hosting Central Administration. Configuring Terminal Services access to the computer creates a greater security risk than leaving the Central Administration Web site available for remote access. |
| E-mail integration |  Configure Office SharePoint Server 2007 to accept only e-mail that has been relayed through a dedicated mail server, such as Microsoft Exchange Server, which filters out viruses and unsolicited commercial e-mail, and authenticates the mail sender.   When configuring workflow settings, Office SharePoint Server 2007 allows you to enable participants who do not have permissions to access a document on a site to receive the document as an e-mail attachment instead. In a secure environment, do not select the Allow external users to participate in workflow by sending them a copy of the document option. In Office SharePoint Server 2007, this option is not selected, by default. |
| Web Part storage and security |  Ensure that you deploy only trusted code to your server farm. All code, XML, or ASP.NET code that you deploy should be from a trusted source, even if you intend to tighten security after deployment with defense-in-depth measures such as code access security.   Ensure that the SafeControl list in the Web.config file contains the set of controls and Web Parts that you want to allow.   Ensure that custom Web Parts that you plan to reinforce with defense-in-depth measures are installed into the bin directory of the Web application (where partial trust is turned on), with specific permissions for each assembly.   Consider removing the Content Editor Web Part from the SafeControl list. This prevents users from adding JavaScript into the page as a Web Part and using JavaScript that is hosted on external servers.   Ensure that appropriate people in your organization are granted the Design and Contribute permission levels in your site. A user with the Contribute permission level can upload Active Server Page Extension (ASPX) pages to a library and add Web Parts. Users with the Design permission level, who are allowed to add Web Parts, can modify pages, including the home page on your site (Default.aspx). |
| Search |  The Office SharePoint Server Search service account and the Windows SharePoint Services Help Search service account must not be members of the Farm Administrators group; otherwise, the search services will index unpublished versions of documents.   Ensure that additional IFilters and word breakers that you deploy are trusted by your IT team.   By default, the search index file is accessible only by members of the Farm Administrators group. Ensure that this file is not accessible to users who do not belong to this group. |
| User profiles | The User Profile and Properties content access account is used to connect to and import data from a directory service. If you do not provide credentials for this account, the default content access account is used instead. You can specify a different account for each directory service. For a more secure environment, use an account that has read access to the directory service. Do not give the default content access account access to the directory service. For more information, see [Plan for administrative and service accounts (Office SharePoint Server)](#DSDOC_f07768d4_ca37_447a_a056_1a67d93ef5). |
| My Sites |  People who have the Read permission level can view all My Sites. By default, all authenticated users are granted the Read permission level. For a more secure environment, grant only the necessary groups the Read permission level. You can grant individual groups the Read permission level in the Default Reader Site Group section on the My Site Settings page in the Shared Services Administration Web site. To specify the actions that members of a group can perform, on the Shared Services Administration home page, click Personalization services permissions settings, select the group whose permissions you want to change, and then click Modify Permissions of Selected Users.   Shared Services Providers (SSPs) can be configured to trust other SSPs in an environment. This trust allows an SSP to determine to which SSP a user belongs. Consequently, when a user creates a My Site, trusted SSPs can determine which SSP should host the My Site, regardless of where the user is browsing when they click the link to create a My Site. This ensures that users have only one My Site in the organization. Also, when users add links to their personal site, trusted SSPs will create the link from the context of the user's SSP, rather than the SSP the user is currently browsing. Trusted SSPs also ensure that links are not added to nontrusted locations. For a more secure environment, ensure that the Trusted My Site Hosts Locations lists are uniformly managed across all SSPs. Ideally, configure the lists the same for all SSPs. |
| Self-service site creation | You can use the Self-Service Site Management page to allow users to create and manage their own top-level Web sites automatically. When you enable self-service site creation for a Web application, users can create their own top-level Web sites under a specific path (by default, the /sites path). When self-service site creation is enabled, an announcement is added to the top-level site at the root path of the Web application, and users who have permissions to view that announcement can link to the new site.  Whether you should enable self-service site creation depends on the environment:   Intranet environment   Enable self-service site creation according to business need.   Secure collaboration environment   Enable self-service site creation only for people or groups who have a business need for this feature.   External anonymous environment   Do not enable self-service site creation on the Internet. |
| Site directory | Some site templates include a site directory. A site directory is a Web page of site links that are approved. Anybody can submit a site for consideration in the site directory. Only site directory administrators can approve and add sites to the site directory.   In a secure intranet, do not approve links to sites outside the corporate firewall.   By default, anyone who has the Contributor permission level can submit sites for approval. This is not recommended for large intranet sites and for public-facing sites. For these sites, limit the number of people who can submit sites by reducing the number of people to whom you grant the Contributor permission level or by allowing only site directory administrators to submit sites. |
| RSS Web Part | By default, the RSS Web Part can access only anonymous feeds. To allow authenticated feeds (such as feeds to authenticated SharePoint site content), you must grant the Web server computers access to the appropriate server computers by using constrained delegation in the Active Directory directory service. |
| Content caching of pages with personalized content | You can use output caching to optimize performance for sites that display some personalized content. In this scenario, post-cache substitution is used to ensure that the personalized content is refreshed for the user. Consequently, if the entire page or most of the page includes personalized content, performance does not greatly improve if you use output caching.  If you plan to enable output caching on pages with personalized content, ensure that sites that display personalized content support post-cache substitution if the following conditions apply:   Both anonymous and authenticated users are accessing content.   Your solution includes sites with controls that display personalized content (for authenticated users).  In this scenario, anonymous users all see identical content. The content that authenticated users see depends on whether personalized content is displayed and if post-cache substation is supported for this content:   If post-cache substitution is supported for personalized content, authenticated users with the same permissions can view only their own personalized content.   If post-cache substitution is not supported for personalized content, users with the same permissions will also see identical content. For example, if personalized content is first cached for user A, all subsequent users with the same permissions will see user A's personalized content instead of their own. |
| Content deployment | If you are not using the content deployment feature, do not permit the server farm to accept incoming content deployment jobs from another farm The default setting is to reject incoming content deployment jobs. |
| InfoPath Forms Server |  If enabled, the InfoPath Forms Services Web service proxy should run under a unique application pool account. Disable the proxy if not used.   Review all form templates that contain code before uploading to the server computer. For more information, see Deploy administrator-approved form templates (Office SharePoint Server).   In browser-only scenarios, use the access control lists (ACLs) in Office SharePoint Server 2007 to prevent the XSN from being downloaded by users.   Carefully consider whether to allow user form templates to be browser-enabled.   Carefully consider whether to allow browser rendering of user form templates.   Use the configurable thresholds to mitigate denial-of-service attacks. User sessions are terminated based on thresholds, including:   Maximum number of postbacks allowed per form session state.   Maximum number of actions allowed per postback.   Maximum size of form session state.   Maximum time that a form session can be active.   Carefully use features in browser-enabled forms. The following features can cause form XML to increase significantly in size, which might increase the risk of denial-of-service attacks:   Digital signatures   File attachment control   Rich-text control   Data connection queries that could return large result sets |
| InfoPath data connections |  Leave Content Approval turned on in data connection libraries, and ensure that only trusted users have content approval rights.   Protect server-only authentication information by using the AltDataSource attribute in the universal data connection (UDC) file and by giving users only the View permission on the server UDC file, or by setting webAccessible to false in the administrator-managed connection library (Manage Data Connection Files).   Review and monitor the use of cross-domain data connections to ensure that only appropriate data is moving into and out of the domain.   By default, user form templates rendered in a browser cannot use server-only authentication. In a secure environment, limit the use of server-only authentication, such as single sign-on (SSO) or explicit user name and password authentication.   Do not use explicit user names and passwords in UDC files except for prototyping on a test server computer. Use SSO instead.   Do not use embedded SQL Server credentials in a database connection string. Use SSO instead.   Use the Web Service proxy only with a Web service designed to use the supplied UserNameToken to authorize access to the data or to limit the data set that is returned.   Require a Secure Sockets Layer (SSL) connection when connecting to data sources that require basic or digest authentication, because credentials are passed insecurely over the network.   Do not authenticate users based on data entered into a form by the user. Instead, use a more secure method of authentication. |
| Excel Calculation Services data access | There are two data access models you can use for any of the Excel Services server farm topologies: trusted subsystem and constrained Kerberos delegation.   Trusted subsystem   The default setting for a Windows server farm, because it does not have the extra configuration requirements of the delegation model. In the trusted subsystem model, front-end Web servers and application servers running Excel Calculation Services trust the accounts of the associated Office SharePoint Server 2007 applications by using the SSP. In a trusted subsystem environment, when opening files from Office SharePoint Server 2007, permission checks on the files can be performed against end-user identities even if Kerberos authentication is not configured. If Excel Calculation Services application servers are opening workbooks from Universal Naming Convention (UNC) shared folders or HTTP Web sites, the user account cannot be impersonated, and the process account must be used.   Constrained Kerberos delegation   Constrained Kerberos delegation is the preferred configuration for deploying Excel Services. Constrained Kerberos delegation is the most secure configuration for communication between front-end Web servers and Excel Calculation Services application servers. Constrained Kerberos delegation is also the most secure configuration for accessing back-end data sources from application servers. For external data connections, Integrated Windows authentication will only work if the delegation model is implemented. |
| Excel Calculation Services secure communication | You can use Internet Protocol security (IPsec) or SSL to encrypt data transmission among Excel Services application servers, data sources, client computers, and front-end Web servers. To require encrypted data transmission between client computers and front-end Web servers, on the Shared Services Administration Web site, on the Excel Services Settings page, change the Connection Encryption setting from Not required to Required. Not Required is the default setting. If you change the Connection Encryption setting to Required, the Excel Calculation Services application server only allows data transmission between client computers and front-end Web servers over SSL connections.  If you decide to require encrypted data transmission, you must manually configure IPsec or SSL. You can require encrypted connections between client computers and front-end Web servers while allowing unencrypted connections between front-end Web servers and Excel Calculation Services application servers." |

# B Plan environment-specific security (Office SharePoint Server)

Insert introduction here.

## Subhead

Insert section body here.

### Subhead

Insert section body here.

# Chapter overview: Plan environment-specific security (Office SharePoint Server)

Planning environment-specific security includes the following tasks:

 [Plan security for an internal team or department environment (Office SharePoint Server)](#DSDOC_9e5d48a2_9f1a_4225_a03b_22cc2c49ff)

 [Plan security for an internal IT-hosted environment (Office SharePoint Server)](#DSDOC_252afeb0_ac39_41a0_a680_2067e7e621)

 [Plan security for an external secure collaboration environment (Office SharePoint Server)](#DSDOC_a6ee7781_e2f1_4cf8_8f38_3a7ae2af74)

 [Plan security for an external anonymous access environment (Office SharePoint Server)](#DSDOC_f507f5d6_4c9d_4f98_909f_069c53b9a3)

Use the appropriate tasks based on your target security environment:

 Internal team or department

 Internal IT-hosted

 External secure collaboration

 External anonymous access

For the internal team or department environment, these recommendations are intended to be used instead of the recommendations provided in [Chapter overview: Plan server farm security (Office SharePoint Server)](#DSDOC_d449e995_a3eb_4191_9d37_7c5e96d9c9). This approach relies on the security implemented in an organization's overall network environment and greatly simplifies the amount of security configuration required for an individual team or department.

For the other three environments, the recommendations provided represent additional guidance that is intended to be used together with the recommendations provided in [Chapter overview: Plan server farm security (Office SharePoint Server)](#DSDOC_d449e995_a3eb_4191_9d37_7c5e96d9c9).

This article provides the following information for each environment, as applicable:

 Server design checklist, including topology and logical architecture

 Security hardening for server roles

 Secure configurations for Microsoft Office SharePoint Server 2007 features

# Plan security for an internal team or department environment (Office SharePoint Server)

In this article:

 [Secure design checklist](#DSDOC_section19e5d48a2_9f1a_4225_a03b_22)

 [Plan security hardening for server roles](#DSDOC_section29e5d48a2_9f1a_4225_a03b_22)

 [Plan secure configurations for Office SharePoint Server features](#DSDOC_section3a9e5d48a2_9f1a_4225_a03b_2)

Security guidance for an internal team or department focuses on recommending practical security configurations and settings for a team or department within a larger organization. This guidance assumes that the servers are not hosted by the primary IT team within the organization.

While the guidance for this environment requires some IT knowledge, it is not necessary for farm administrators to be dedicated IT specialists. If more specialized roles are required to implement a setting, these roles are noted.

This guidance is intended to be used together with the guidance provided in [Plan secure configurations for Office SharePoint Server features](#DSDOC_e8493b73_ad1a_4642_8141_05405f0026).

## Secure design checklist

Review the following checklist to ensure that your plans meet the criteria for a secure server topology design.

Topology

|  |  |
| --- | --- |
| [ ] | For a team or department deployment that has internal access only, Microsoft Office SharePoint Server 2007 can be installed on a single server or on two servers. |
| [ ] | In a two-server or more deployment, the Central Administration site should be hosted on a different server than the front-end Web server, where possible. This can only be accomplished if application server roles are hosted on a different server than the front-end Web server role.  For example, if Server A hosts the front-end Web server role and Server B hosts the database and application server roles, the most secure location for the Central Administration site is on Server B. However, if Server A hosts the front-end Web server and application server roles and Server B hosts only the database role, the only option is to host the Central Administration site on Server A. |

Logical architecture

|  |  |
| --- | --- |
| [ ] | At least one zone in each Web application uses NTLM authentication. This is required for the search account to crawl content within the Web application. The search account cannot use Kerberos authentication to crawl content.  For more information, see [Plan authentication methods [Office SharePoint Server]](#DSDOC_40117fda_70a0_4e3d_8cd3_0def768da1). |
| [ ] | When deploying custom Web Parts, ensure that only trustworthy Web Parts are deployed within Web applications that host sensitive or secure content. This protects the sensitive content against intradomain scripting attacks. |

## Plan security hardening for server roles

Guidance for an internal team or department environment assumes that only internal access is allowed for the servers, sites, and content and that the overall network environment is secured by policies developed by an IT department. Consequently, hardening servers for specific roles is not necessary to the same extent as for other environments. However, there are several features that require specific services or other settings that otherwise might not be configured.

The following table describes recommended hardening settings for an internal team or department.

|  |  |
| --- | --- |
| Feature | Setting |
| E-mail integration | If e-mail integration is enabled, the SMTP service is required on one front-end Web server. |
| Microsoft Office Project Server 2007 and Microsoft Office Forms Server 2007 | Both Office Project Server 2007 and Office Forms Server 2007 maintain session state. If you are deploying these features or products within your server farm, do not disable the ASP.NET State Service. Additionally, if you are deploying InfoPath Forms Services, do not disable the View State service. |
| Single sign-on (SSO) | SSO relies on the Microsoft Single Sign-On service. For more information about configuring this feature, see [Plan for single sign-on](#DSDOC_3c78e886_5d20_44cb_b4e4_f823c4c019). |

## Plan secure configurations for Office SharePoint Server features

The following table describes additional recommendations for securing Office SharePoint Server 2007 features. These recommendations are appropriate for an internal team or department environment.

|  |  |
| --- | --- |
| Feature or area | Recommendation |
| Authentication | Authenticate against the existing identity management system. If this is not the Active Directory directory service, use ASP.NET forms authentication to connect to your identity management system. Using forms authentication might require assistance from the following roles:   ASP.NET developer to develop the authentication provider.   Administrator of the identity management system to which you are connecting. |
| Central Administration site |  Restrict access to the Central Administration site to appropriate users only.   If you are enabling the Central Administration site for remote administration, secure the Central Administration site by using Secure Sockets Layer (SSL).   Administrators who run deployment operations must be members of the local administrators group on the server that hosts the Central Administration site. |
| Windows SharePoint Services Administration service | In a single-server deployment, the Windows SharePoint Services Administration service is disabled by default for the following reasons:   This service, which is used to run deployment tasks that are initiated from the Central Administration site, is generally not required for a single-server deployment. However, deployment tasks can be run by using the Stsadm.exe command-line tool, which does not require the use of this service.   The account that is used for the Central Administration site is shared with all other processes. Consequently, disabling this service results in a more secure configuration.  For a secure single-server deployment, it is recommended to:   Change the server farm account after running Setup.   Start the Windows SharePoint Services Administration service.  Performing these actions will enable you to perform deployment-related tasks directly from the Central Administration site. |

# Plan security for an internal IT-hosted environment (Office SharePoint Server)

In this article:

 [Secure design checklist](#DSDOC_section1252afeb0_ac39_41a0_a680_20)

 [Plan security hardening for server roles](#DSDOC_section2252afeb0_ac39_41a0_a680_20)

 [Plan secure configurations for Office SharePoint Server features](#DSDOC_section3a252afeb0_ac39_41a0_a680_2)

Security guidance for the internal IT-hosted environment targets guidance to an IT team that is hosting Microsoft Office SharePoint Server 2007 Web applications and sites for multiple teams and departments in an organization.

## Secure design checklist

Logical architecture

|  |  |
| --- | --- |
| [ ] | Organize your environment into separate hosted services. A hosted service includes sites and services that need to be managed by a distinct group. This includes managing user profiles, audience services, and user permissions. Plan a separate Shared Services Provider (SSP) for each hosted service and securely manage the administrative permissions for configuring each SSP. |

## Plan security hardening for server roles

No additional guidance is recommended for this environment.

## Plan secure configurations for Office SharePoint Server features

No additional guidance is recommended for this environment.

# Plan security for an external secure collaboration environment (Office SharePoint Server)

In this article:

 [Protect back-end servers](#DSDOC_section1a6ee7781_e2f1_4cf8_8f38_3a)

 [Secure client-server communication](#DSDOC_section2a6ee7781_e2f1_4cf8_8f38_3a)

 [Secure the Central Administration site](#DSDOC_section3a6ee7781_e2f1_4cf8_8f38_3a)

 [Secure Shared Services Provider administration sites](#DSDOC_section4a6ee7781_e2f1_4cf8_8f38_3a)

 [Secure design checklist](#DSDOC_section5a6ee7781_e2f1_4cf8_8f38_3a)

 [Plan security hardening for server roles](#DSDOC_section6a6ee7781_e2f1_4cf8_8f38_3a)

 [Plan secure configurations for Office SharePoint Server features](#DSDOC_section7aa6ee7781_e2f1_4cf8_8f38_3)

Security guidance for an external secure environment is targeted to hosting content in an extranet for the purpose of collaborating on content with contributors who do not have general access to your corporate network. This environment allows external partners to participate in a workflow or to collaborate on content together with employees of your organization.

There are several unique recommendations for an external secure collaboration environment. Some of these recommendations might not be practical for all solutions.

## Protect back-end servers

External secure collaboration requires Internet-facing servers. You can limit the exposure to traffic from the Internet by protecting back-end servers:

 Protecting database servers   At a minimum, place a firewall between front-end Web servers and servers that host databases. Some environments dictate that database servers be hosted in an internal network instead of directly in an extranet environment.

 Protect application servers   At a minimum, protect application servers by requiring Internet Protocol security (IPsec) to secure communication between server farm computers. You can additionally place application servers behind the firewall used to protect database servers. Or, you can introduce an additional firewall between front-end Web servers and application servers.

 Protect the index role   The index component communicates through a front-end Web server to crawl content in sites. To protect this communication channel, consider configuring a dedicated front-end Web server for use by one or more index servers. This isolates crawling communication to a front-end Web server that is not accessible to users. Additionally, configure Internet Information Services (IIS) to restrict SiteData.asmx (the crawler SOAP service) to allow only the index server (or other crawlers) to access it. Providing a front-end Web server dedicated to content crawling also improves performance by reducing the load on the main front-end Web servers, thereby improving the user experience.

## Secure client-server communication

Secure collaboration in an extranet environment relies on secure communication between client computers and the server farm environment. Where appropriate, use Secure Sockets Layer (SSL) to secure communication between client computers and servers. To increase security, consider the following:

 Require certificates on client computers. SSL can be implemented without requiring client certificates. You can increase the security of external collaboration by requiring certificates on all client computers.

 Use IPsec. If client computers support IPsec, you can configure IPsec rules to achieve a greater level or granularity of security compared with SSL.

## Secure the Central Administration site

Because external users have access to the network zone, it is important to secure the Central Administration site to block external access and secure internal access:

 Ensure that the Central Administration site is not hosted on a front-end Web server. The recommendation for this environment is to host the Central Administration site on the same server that hosts the index component.

 Block external access to the Central Administration site. This can be achieved by placing a firewall between front-end Web servers and the server that hosts the Central Administration site.

 Configure the Central Administration site by using SSL. This ensures that communication from the internal network to the Central Administration site is secured.

## Secure Shared Services Provider administration sites

Shared Services Provider (SSP) administration sites (one site per SSP) are installed on front-end Web servers. Each SSP administration site is created in a dedicated Web application. The recommendations for securing these sites include:

 Configure all SSP administration sites by using SSL. This ensures that communication from the internal network to these sites is secured.

 Configure a policy for the Web application to deny access to all external users.

## Secure design checklist

Use this design checklist together with the checklists in [Chapter overview: Plan server farm security (Office SharePoint Server)](#DSDOC_d449e995_a3eb_4191_9d37_7c5e96d9c9).

Topology

|  |  |
| --- | --- |
| [ ] | Protect back-end servers by placing at least one firewall between front-end Web servers and the application and database servers. |
| [ ] | Plan a dedicated front-end Web server for crawling content. Do not include this front-end Web server in the end-user front-end Web rotation. |

Logical architecture

|  |  |
| --- | --- |
| [ ] | Block access to the Central Administration site and configure SSL for this site. |
| [ ] | Secure SSP administration sites by configuring these sites with SSL, by hosting these sites in a dedicated Web application, and by configuring a policy to deny external access to these sites. |

## Plan security hardening for server roles

The following table describes additional hardening recommendations for an external secure collaboration environment.

|  |  |
| --- | --- |
| Component | Recommendation |
| Ports | Block external access to the port for the Central Administration site. |
| IIS | Restrict SiteData.asmx (the crawler SOAP service) to allow only the index server (or other crawlers) to access it. |

## Plan secure configurations for Office SharePoint Server features

The following table describes additional recommendations for securing Microsoft Office SharePoint Server 2007 features. These recommendations are appropriate for an external secure collaboration environment.

|  |  |
| --- | --- |
| Feature or area | Recommendation |
| Authentication | Use SSL for authenticated users. This does not apply to the anonymous user who is browsing the site. |
| Authorization | Use security policy to cap external users permission (create deny policies to limit what external users can do). |
| My Sites | Grant the Create Personal Site right only to contributors who need to create personal sites. |
| InfoPath Forms Server | Disable the InfoPath Forms Services Web service proxy. |

# Plan security for an external anonymous access environment (Office SharePoint Server)

In this article:

 [Protect back-end servers](#DSDOC_section1f507f5d6_4c9d_4f98_909f_06)

 [Configure anonymous access](#DSDOC_section2f507f5d6_4c9d_4f98_909f_06)

 [Secure the Central Administration site](#DSDOC_section3f507f5d6_4c9d_4f98_909f_06)

 [Secure content deployment by using SSL](#DSDOC_section4f507f5d6_4c9d_4f98_909f_06)

 [Disable incoming e-mail](#DSDOC_section5f507f5d6_4c9d_4f98_909f_06)

 [Use lockdown mode](#DSDOC_section6f507f5d6_4c9d_4f98_909f_06)

 [Secure design checklist](#DSDOC_section7f507f5d6_4c9d_4f98_909f_06)

 [Plan security hardening for server roles](#DSDOC_section8f507f5d6_4c9d_4f98_909f_06)

 [Plan secure configurations for Office SharePoint Server features](#DSDOC_section9af507f5d6_4c9d_4f98_909f_0)

Security guidance for an external anonymous access environment is targeted to allow anonymous access to content while protecting back-end servers in the farm from direct user access or malicious actions targeted through front-end Web servers. In an environment where multiple farms might be deployed to support authoring, staging, and publishing, the guidance for this environment is intended for the published farm (the farm that is anonymously accessed by users).

There are several unique recommendations for an external anonymous access environment. Some of these recommendations might not be practical for all solutions.

## Protect back-end servers

Hosting sites for anonymous use requires Internet-facing servers. You can limit the exposure to traffic from the Internet by protecting back-end servers, including the index server and other application server roles and servers that host databases:

 Protecting database servers   At a minimum, place a firewall between front-end Web servers and servers that host databases. Some environments dictate that database servers be hosted in an internal network instead of directly in an extranet environment.

 Protect application servers   At a minimum, protect application servers by requiring Internet Protocol security (IPsec) to secure communication between server farm computers. Additionally, you can place application servers behind the firewall used to protect database servers. Or, you can introduce an additional firewall between front-end Web servers and application servers.

 Protect the index role   The index component communicates through a front-end Web server to crawl content in sites. To protect this communication channel, consider configuring a dedicated front-end Web server for use by one or more index servers. This isolates crawling communication to a front-end Web server that is not accessible to users. Additionally, configure Internet Information Services (IIS) to restrict SiteData.asmx (the crawler SOAP service) to allow only the index server (or other crawlers) to access it. Providing a front-end Web server dedicated to content crawling also improves performance by reducing the load on the main front-end Web servers, thereby improving the user experience.

## Configure anonymous access

For content to be available for anonymous access, the following must be configured:

 The site or site collection must be configured to allow anonymous access.

 At least one zone in the Web application must be configured to allow anonymous access.

Enable anonymous access only for Web applications that require unauthenticated access. If you want to use authentication for personalization, implement forms authentication by using a simple database authentication provider.

## Secure the Central Administration site

Because external users have access to the network zone, it is important to secure the Central Administration site to block external access and secure internal access:

 Ensure that the Central Administration site is not hosted on a front-end Web server. The recommendation for this environment is to host the Central Administration site on the same server that hosts the index component.

 Block external access to the Central Administration site. This can be achieved by placing a firewall between front-end Web servers and the server that hosts the Central Administration site.

 Configure the Central Administration site by using Secure Sockets Layer (SSL). This ensures that communication from the internal network to the Central Administration site is secured.

## Secure content deployment

If you are not using the content deployment feature, disable the server farm from receiving content deployments (under Content Deployment Settings, select Reject incoming content deployment jobs). This is the default setting.

If you are using content deployment features to deploy content from one server farm to another server farm, ensure that the Central Administration site for the receiving server farm is configured to use SSL. This will ensure that server communication related to content deployment between the two server farms is secured by using SSL.

Additionally, to protect the identities of your authors, disable the Deploy user names setting when you configure the content deployment path.

## Disable incoming e-mail

Do not use e-mail integration for incoming e-mail. This protects your environment from risks associated with e-mail sent from anonymous sources on the Internet. If you do allow incoming e-mail, configure the Central Administration site to enable anonymous e-mail. While this option is available, it is not very secure.

## Use lockdown mode

Lockdown mode is a feature that you can use to secure published sites. When lockdown mode is turned on, fine-grain permissions for the limited access permission level are reduced. The following table details the default permissions of the limited access permission level and the reduced permissions when lockdown mode is turned on.

|  |  |  |
| --- | --- | --- |
| Permission | Limited access — default | Limited access — lockdown mode |
| List permissions: View Application Pages | ● |  |
| Site permissions: Browse User Information | ● | ● |
| Site permissions: Use Remote Interfaces | ● |  |
| Site permissions: Use Client Integration Features | ● | ● |
| Site permissions: Open | ● | ● |

Lockdown mode is applied to sites under the following circumstances:

 The Stsadm.exe command-line tool is used to turn lockdown mode on.

 The Publishing Portal site template is applied to the site collection. By default, lockdown mode is turned on when this template is applied.

Consider using lockdown mode on published sites if greater security on these sites is a requirement. Additionally, if you applied the Publishing Portal site template, determine if lockdown mode is the desired configuration for these sites. If not, use the Stsadm.exe command-line tool to turn off lockdown mode.

The following table lists the Stsadm commands related to using lockdown mode.

|  |  |
| --- | --- |
| Action | Command |
| Turn on lockdown mode for a site collection | stsadm -o activatefeature -url <site collection url> -filename ViewFormPagesLockDown\feature.xml |
| Turn off lockdown mode for a site collection | stsadm -o deactivatefeature -url <site collection url> -filename ViewFormPagesLockDown\feature.xml |

## Secure design checklist

Use this design checklist together with the checklists in [Review the secure topology design checklists (Office SharePoint Server)](#DSDOC_007ecb03_5808_495a_bb72_4f0641eaf8).

Topology

|  |  |
| --- | --- |
| [ ] | Protect back-end servers by placing at least one firewall between front-end Web servers and the application and database servers. |
| [ ] | Plan a dedicated front-end Web server for crawling content. Do not include this front-end Web server in the end-user front-end Web rotation. |

Logical architecture

|  |  |
| --- | --- |
| [ ] | Enable anonymous access only for Web application zones that host sites or site collections that are configured to allow anonymous access.  For more information, see [Plan authentication methods [Office SharePoint Server]](#DSDOC_40117fda_70a0_4e3d_8cd3_0def768da1). |
| [ ] | Use SSL to secure content deployment. |
| [ ] | Block access to the Central Administration site and configure SSL for the site. |

## Plan security hardening for server roles

The following table describes additional hardening recommendations for an external anonymous access environment.

|  |  |
| --- | --- |
| Component | Recommendation |
| Ports | Block external access to the port for the Central Administration site. |
| Protocols |  Disable SMTP.   Use SSL to secure content as it is deployed from the authoring farm to the staging and published farms. |
| IIS | If you are configuring a dedicated front-end Web server for indexing, configure IIS to restrict SiteData.asmx (the crawler SOAP service) to allow only the index server (or other crawlers) to access it. |

## Plan secure configurations for Office SharePoint Server features

The following table describes additional recommendations for securing Microsoft Office SharePoint Server 2007 features in an external anonymous access environment.

|  |  |
| --- | --- |
| Feature or area | Recommendation |
| Authentication | Specify Anonymous authentication in IIS. |
| Content deployment | If you are not using the content deployment feature, disable the server farm from receiving content deployments. This is the default setting.  If you are using the content deployment feature, the following configurations are recommended:   Turn on SSL for the Central Administrator site on the receiving server farm.   Disable the Deploy user names setting when you configure the content deployment path. |
| E-mail integration | Do not enable e-mail integration for incoming mail. |
| Content caching of pages that have personalized content | Output caching can be used to optimize performance for sites that display some personalized content. In this scenario, post-cache substitution is used to ensure that the personalized content is refreshed for the user. Consequently, if the entire page or most of the page includes personalized content, there is little benefit received by using output caching.  If you are using output caching on pages that have personalized content, be aware of the security implications resulting from how this is configured. If the following conditions are true, ensure that sites that display personalized content support post-cache substitution:   You plan to enable page output caching (to optimize performance).   Both anonymous and authenticated users are accessing content.   Your solution includes sites that have controls that display personalized content (for authenticated users).  In this scenario, anonymous users all see identical content. The content that authenticated users see depends on whether personalized content is displayed and if post-cache substitution is supported for this content:   If post-cache substitution is supported for personalized content, authenticated users who have the same rights can view only their own personalized content.   If post-cache substitution is not supported for personalized content, users who have the same rights as each other will also see identical content. In this scenario, if personalized content is first cached for user A, all subsequent users who have the same rights will see user A's personalized content instead of their own. |
| InfoPath Forms Server | In an anonymous environment, disable the InfoPath Forms Services Web service proxy. This service runs as a trusted service account and forwards requests to Web services by using the identity of the trusted service account.  In environments where InfoPath forms are accessed only by authenticated users, access to a back-end data system is protected by authentication. However, if subsequent InfoPath forms are created for use by anonymous users and these forms access the same back-end data system, the back-end data system is configured to trust the Web service proxy and provide the requested data. In this case, it is possible for anonymous users to access data that is typically only available to authenticated users.  By default, the Web service proxy is disabled. You manage this service in Central Administration. On the Application Management tab, look in the InfoPath Forms Services category and click Manage the Web service proxy. |

# Plan for security roles [Office SharePoint Server]

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Plan for single sign-on

In this article:

 [About single sign-on](#DSDOC_section13c78e886_5d20_44cb_b4e4_f8)

 [Common SSO scenarios](#DSDOC_section23c78e886_5d20_44cb_b4e4_f8)

 [Office SharePoint Server SSO architecture](#DSDOC_section33c78e886_5d20_44cb_b4e4_f8)

 [Plan farm-level SSO settings](#DSDOC_section43c78e886_5d20_44cb_b4e4_f8)

 [Plan enterprise application definition settings](#DSDOC_section53c78e886_5d20_44cb_b4e4_f8)

 [Plan for SSO operations](#DSDOC_section63c78e886_5d20_44cb_b4e4_f8)

 [Worksheets](#DSDOC_section73c78e886_5d20_44cb_b4e4_f8)

Use this article to plan for using single sign-on (SSO) in Microsoft Office SharePoint Server 2007. This article describes how SSO is configured in a secure environment, including how to use SSO to connect to back-end data systems.

## About single sign-on

The SSO feature in Office SharePoint Server 2007 maps user credentials to back-end data systems. Using SSO, you can access data from server computers and services that are external to Office SharePoint Server 2007. From within Office SharePoint Server 2007 Web Parts, you can view, create, and change this data. The SSO feature ensures that:

 User credentials are managed securely.

 User permission levels that are configured on the external data source are enforced.

 Users are not prompted to reenter their credentials when viewing data from external data sources within Office SharePoint Server 2007.

 Office SharePoint Server 2007 can connect to multiple external data systems regardless of the platform and authentication requirements.

SSO requires the use of Windows credentials for user accounts. In environments where Web SSO is used to authenticate user accounts, SSO can be used only if the current thread that is invoking SSO application programming interfaces (APIs) has a Windows identity associated with it.

## Common SSO scenarios

SSO is primarily used for business intelligence scenarios. In Office SharePoint Server 2007, many features depend on SSO, including the following:

 Business Data Catalog

 Excel Services

 InfoPath Forms Services

 Business Data Web Parts

 KPI Web Part

 1st SharePoint Designer Data Form Web Part

 Business data search

 Business data in lists

Additionally, you can introduce custom Web Parts that connect to external data sources including those that are based on operating systems other than Windows. For example, you can connect to the following enterprise applications:

 SAP Business Information Warehouse

 Siebel eBusiness Applications

 Microsoft BizTalk Server

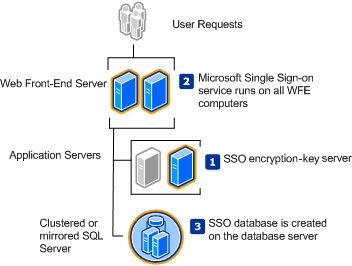
For more information about business intelligence scenarios, see Plan for business intelligence.

## Office SharePoint Server SSO architecture

This section describes how SSO is implemented in Office SharePoint Server 2007.

### Microsoft Single Sign-On service

The SSO feature in Office SharePoint Server 2007 uses the Microsoft Single Sign-On service (SSOSrv). The following figure shows how the Single Sign-On service is implemented in an Office SharePoint Server 2007 server farm.



1. SSO encryption-key server   The first server computer on which the Single Sign-On service is enabled becomes the encryption-key server. The encryption-key server generates and stores the encryption key. The encryption key is used to encrypt and decrypt the credentials that are stored in the SSO database. The encryption-key server should be an application server computer, such as the index server.

2. Single Sign-On service   This service must be installed on all Web server computers in the server farm. Additionally, the service must be installed on any computers that are hosting the Excel Services application server role. If a Business Data Catalog search is used, the service must be installed on the index server as well.

3. SSO database   When you configure SSO server settings in the Central Administration site, Office SharePoint Server 2007 creates an SSO database on the database server computer that hosts the configuration database. If Microsoft SQL Server is installed, the SSO database is a SQL Server database. If SQL Server is not installed, the Single Sign-On service uses SQL Server 2005 Express Edition. The SSO database stores the encrypted credentials.

note_ddNote:

If you are upgrading from a previous version of SharePoint Portal Server, you must re-create your SSO environment, including creating a new SSO database. SSO cannot be migrated or upgraded to Office SharePoint Server 2007.

### Enterprise application definitions

In an SSO environment, the back-end external data sources and systems are referred to as enterprise applications. After the SSO environment is configured, you can create enterprise application definitions. For each enterprise application that Office SharePoint Server 2007 connects to, there is a corresponding enterprise application definition configured by an administrator. Or, several enterprise application definitions can be configured for the same physical enterprise application to secure different groups who have access.

An enterprise application definition defines:

 The enterprise application identity (display name, programmatic name, and contact e-mail address).

 The type of user accounts that are mapped to the enterprise applications. This depends on whether the enterprise application (or in some cases, the Web Part) enforces permissions based on individual accounts or group accounts.

 The type of credentials that are collected from users (user name, password, or other credentials, such as a smart card).

 The account used by Office SharePoint Server 2007 Web Parts to connect to the enterprise application.

The single sign-on functionality enables scenarios where multiple Web Parts access different enterprise applications. The different enterprise applications can each use a different type of authentication. The enterprise applications can also be based on operating systems other than Windows.

### SSO tickets

In an enterprise environment where a user interacts with various systems and applications, it is very likely that the environment does not maintain the user context through multiple processes, products, and computers. This user context is crucial to provide single sign-on capabilities, because it is necessary to verify who initiated the original request. In scenarios where multiple servers participate in passing credentials from the encryption-key server to the enterprise application, the Single Sign-On service provides an SSO ticket (not a Kerberos ticket). These servers use this ticket to get the credentials that correspond to the user who made the original request.

For example, a payroll environment might be configured to access data in a SAP system through BizTalk Server. If a Web Part is connecting to the SAP system, credentials are routed through the BizTalk Server computer. In an SSO environment, a Web Part sends an SSO ticket to the service on the BizTalk Server computer that connects to the SAP system. If the user belongs to an account or group account that is specified in the enterprise application definition, the service redeems the SSO ticket for credentials to the SAP system. In order for the service on the BizTalk Server computer to redeem SSO tickets, the account that is used by the service must be added to the SSO Administrators group.

The Single Sign-On service issues a ticket when a Windows user requests a ticket or when an application requests a ticket on behalf of a user. The Single Sign-On service can only issue a ticket for the user who makes the request (you cannot request a ticket for other users). A ticket contains the encrypted domain and user name of the current user, and the ticket expiration time.

After an enterprise application verifies the identity of the original requestor, the application redeems the ticket to obtain the credentials of the user who initiated the request. Tickets expire in two minutes by default. SSO administrators can modify the expiration time for tickets. The ticket time-out value must be long enough to last between the time the ticket is issued and the time that it is redeemed.

### SSO administration

Administering SSO involves two types of administrators:

 SSO administrators   These administrators set up and configure SSO, manage SSO accounts, back up the encryption key, and create and change the encryption key. For security reasons, SSO administrators are required to log on to the encryption-key server locally to set up, configure, and manage SSO. SSO administrators are prevented from managing SSO server settings from a remote server computer.

 Enterprise application definition administrators   These administrators create and manage enterprise application definitions, and update accounts and credentials used to access enterprise applications. These administrators can manage enterprise application definitions remotely.

Specific accounts and permissions for SSO administrators are detailed later in this article.

### Networking dependencies

Within an Office SharePoint Server 2007 server farm, the Single Sign-On service relies on NetBIOS names to communicate between the encryption-key server and the database server computer. If NetBIOS name resolution is not available for the database server computer, SSO configuration will fail.

## Plan farm-level SSO settings

This section describes planning choices for farm-level settings. These planning choices include:

 Deciding which server computer will host the SSO encryption-key server role.

 Setting up SSO accounts and ensuring that these accounts are created with the appropriate permissions.

 Recording decisions for farm-level settings that are configured on the Manage Server Settings for Single Sign-On page in Central Administration.

|  |
| --- |
|  Worksheet action |
|  Use the [Single sign-on server farm settings worksheet](http://go.microsoft.com/fwlink/?LinkId=73336&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73336&clcid=0x409) to record your planning choices. |

### SSO encryption-key server

Determine which computer in your farm will host the SSO encryption-key server role. The recommended configuration is to select an application server computer, such as the index server, for the following reasons:

 All server computers that run the Single Sign-On service must be able to communicate over the network with the encryption-key server. When using a farm with multiple Web server computers, some load-balancing technologies do not allow the Web servers to communicate with each other.

 Application server computers are not directly accessed by end-users and are typically protected by additional layers of security. For example, security protocols such as IPsec or SSL are often implemented to secure server-to-server communication within a server farm. Additionally, some farm topologies implement an additional router or firewall between Web server computers and application server computers.

The Single Sign-On service must be installed on any application server computers that host the Excel Services role. If a Business Data Catalog search is used, the Single Sign-On service must be installed on the index server as well. These requirements make each of these server computers a good choice for the encryption-key server role.

Ensure that SSO administrators can log on locally to the encryption-key server. Additionally, be sure that security settings in Internet Explorer do not prevent administration of SSO by ensuring the following:

 The default option, Automatic logon only in Intranet zone, is selected. (To do this, on the Tools menu, click Internet Options, click the Security tab, click the Custom Level button, and then in the Security Settings dialog box, go to the User Authentication section.)

 Prompt for user name and password is not selected.

### SSO accounts

There are four different accounts that are required to set up, run, and administer the SSO system:

 SSO configuration account

 SSO administrator account

 SSO service account

 Enterprise application administrator account

In an evaluation environment, you can use the server farm account for each of these accounts. However, in a secure environment, you should put some thought into which accounts you use and how you configure these accounts. This section details the account requirements and provides recommendations for configuring these accounts in a secure environment.

The four accounts that are required to set up, run, and administer the SSO system provide separation of roles and isolation of permissions. The following tables list the accounts and describe the actions that are performed using these accounts.

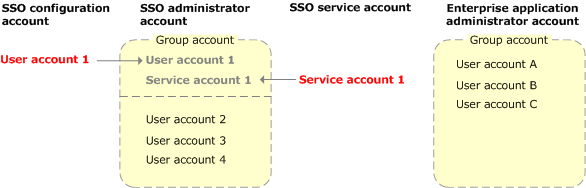
|  |  |
| --- | --- |
| Account | Description |
| SSO configuration account |  Set up the Single Sign-On service in Office SharePoint Server 2007.   Configure and manage the Single Sign-On service in Office SharePoint Server 2007, including managing the encryption key.   Create, modify, or delete enterprise application definitions within Office SharePoint Server 2007. |
| SSO administrator account |  Configure and manage the Single Sign-On service in Office SharePoint Server 2007, including managing the encryption key.   Create, modify, or delete enterprise application definitions within Office SharePoint Server 2007.  Redeem SSO tickets. In scenarios where credentials pass through an intermediary service (such as BizTalk Server) before reaching the enterprise application definition, this account is used to give intermediary services permissions to redeem SSO tickets. |
| SSO service account | Run the Single Sign-On service in Windows. |
| Enterprise application administrator account | Create, modify, or delete enterprise application definitions within Office SharePoint Server 2007. |

|  |  |
| --- | --- |
| Account | Requirements |
| SSO configuration account |  Must be a user domain account. Cannot be a group account.   The user account must be a server farm administrator.   Must be a member of the Administrators group on the encryption-key server computer.   Must be a member of the following SQL Server security roles on the computer running SQL Server:   Dbcreator   Securityadmin   Must be either the same as the SSO administrator account, or be a member of the group account that is the SSO administrator account. |
| SSO administrator account |  Must be either a Windows global group or an individual user account. Cannot be a domain local group account or a distribution list.   The SSO service account must be this user or a member of this group.   The SSO configuration account must be this user or a member of this group.   Must be added to the SharePoint Central Administration site with the Read permission level.   All users that are added to this group for the purpose of administering SSO must be members of the Administrators group on the encryption-key server. Do not make this account itself a member of the Administrators group on the encryption-key server. |
| SSO service account |  Must be a domain user account. Cannot be a group account.   Must be the SSO administrator account or a member of the group account that is the SSO administrator account.   Must be member of the local group WSS\_Admin\_WPG on all server computers running Office SharePoint Server 2007 in the server farm.   Must be member of the public database role on the Office SharePoint Server 2007 configuration database.   Must be member of the Sysadmin server role on the SQL Server instance where the SSO database is located.   In a secure environment, do not run the service under an account that is a member of the Administrators group on the local computer.  note_ddNote:  To change the service account, you must first back up the master key, and then restore the master key after the service account is changed. |
| Enterprise application administrator account |  Must be global group account or individual user account. This account cannot be a domain local group or a distribution list.   Must have the Read permission level on the SharePoint Central Administration site. |

In a secure environment, the recommendation is to configure four distinct accounts and to use a group account, where possible. If you are using a user account for the SSO configuration account, SSO administrator account, and the SSO service account, you must use the same user account. The following table provides recommendations for configuring these accounts.

|  |  |  |
| --- | --- | --- |
| Account | Evaluation environment | Secure environment |
| SSO configuration account | Server farm account | Use the individual user account of an administrator who is a member of the Farm Administrators group. |
| SSO administrator account | Server farm account | Create a dedicated domain group account. Add the following to this group:   User account that will be used as the SSO configuration account.   Account used to run the Single Sign-On service   Users that are allowed to administer the Single Sign-On service in Office SharePoint Server 2007. Also add these users to the Administrators group on the encryption-key server.  Service accounts of services that redeem SSO tickets. These are intermediary services that pass credentials between the encryption-key server and the enterprise application. |
| SSO service account | Server farm account |  Use an individual user account. Use a different account than the SSO configuration account.   Do not add this account to the Farm Administrators group or to the Administrators group on the local computer.  Do not use the same service account that is used to run Internet Information Services (IIS) application pools. |
| Enterprise application administrator account | Server farm account | Create a dedicated domain group account. Add to this group users that are allowed to create and manage enterprise application definitions. |

The following figure shows the recommended secure configuration for these accounts.



### Database settings

Database settings are used to create the SSO database and include:

 Server name   This is the NetBIOS name of the database server computer. Do not enter the fully qualified domain name (FQDN).

 Database name   This is the name of the SSO database.

Unless you are creating databases beforehand, the recommendation is to keep the default settings.

### Time-out settings

Time-out settings include the following:

 Ticket time out (in minutes)   Use to set the number of minutes that can elapse before an SSO ticket expires. Ensure that the ticket time-out value is long enough to last between the time when the ticket is issued and the time that it is redeemed by the enterprise application. Two minutes is the recommended setting that allows ample time for tickets to be redeemed. If tickets are not redeemed within two minutes, networking or other issues might be preventing a connection between computers.

 Delete audit log records older than   Use to set the number of days to hold records in the audit log before deleting.

The default time-out settings are the recommended starting points.

## Plan enterprise application definition settings

This section describes planning choices for enterprise application definitions.

|  |
| --- |
| Worksheet action |
| Use the [Single sign-on enterprise application definition worksheet](http://go.microsoft.com/fwlink/?LinkId=73335&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73335&clcid=0x409) to record your planning choices. Complete this worksheet for each enterprise application definition that you plan to add. |

After you create an enterprise application definition, you cannot modify the following properties:

 Name of the enterprise application definition

 Account type (group or individual, Windows authenticated group or individual, or group that uses restricted account)

 Logon account information fields

### Application and contact information

Application and contact information includes the following settings:

 Display name   The friendly name for the enterprise application.

 Application name   The programmatic name for the enterprise application. This is the name that Web Parts will use to call the enterprise application definition.

 Contact e-mail address   The e-mail address that users can contact for the enterprise application.

### Account type

Account type refers to the type of account that is used to map user credentials to the enterprise application: either an individual account or a group account. If each user has an account in the enterprise application, choose Individual. If the enterprise application uses one account for all users, choose Group.

Be aware that security authorization can be performed by either the enterprise application or by the Web Part that is connecting to the enterprise application. How security authorization is set up affects which type of account is used by the enterprise application. For example, authorization to access personal data in a pay stub application can be set up by using one of two methods:

 Users have their own accounts in the pay stub system to access their pay stub. In this case, individual accounts are used by the enterprise application.

 The Web Part that is used to access pay stub data enforces security authorization. In this case, the Web Part performs user authorization based on user credentials and the pay stub system uses a group account for all users. Consequently, the enterprise application definition for this scenario uses a group account.

Additionally, if a group account is used, the enterprise application definition can be configured to use a privileged account. If you choose a privileged account, credentials are stored separately from regular credentials and a different API is used to access privileged credentials. Privileged accounts are used in scenarios where an intermediary application, such as Business Data Catalog, imposes further security trimming on the data that is retrieved based on the credentials.

Applications that use restricted credentials must perform further authorization and data trimming based on the data that is returned by using the privileged credentials. Farm administrators must ensure that all applications that use privileged accounts perform this authorization and data trimming uniformly. Otherwise, if an application that does not perform this additional authorization and trimming has access to privileged accounts, the application can compromise security by using privileged credentials to access data that would otherwise be trimmed.

Choose Group using privileged account only under the following circumstances:

 The account is a group account.

 Business Data Catalog is used to connect to the enterprise application.

 The intermediary application that connects to the enterprise application complies with the terms of using a privileged account.

 Data is highly sensitive.

### Authentication type

Authentication type refers to the method in which the Office SharePoint Server 2007 server connects to the enterprise application: Windows authentication or no authentication. This authentication applies only to the credentials that the server running Office SharePoint Server 2007 uses to log on to the enterprise application. Authentication of user credentials is not affected.

If the enterprise application is hosted on a computer running Windows, select Windows authentication. If the enterprise application is hosted on a computer that is not running Windows, leave this setting blank. If Windows authentication is not used, logon credentials are not encrypted. If you select Windows authentication and the enterprise application system does not support Windows authentication, the SSO connection will fail.

### Logon account information for users

The fields provided for logon account information determine which pieces of information are required to log on. By default, only the user name and password are specified. You can specify up to five different pieces of information that must be included. For example, you can require an SAP server name or an SAP client number. Users are prompted to enter credentials under the following circumstances:

 Authentication fails or credentials are not found.

 The Web Part is programmed to prompt users for credentials.

Logon account information is used for enterprise application definitions that use individual accounts. Prompting for logon account information is not recommended for enterprise application definitions that use group accounts.

The logon account information that you configure here must match the logon requirements for the enterprise application. Additionally, you must also determine whether the system needs to mask these credentials as the user provides them.

Typically, only a user name and password are required. Some highly secure environments might require additional pieces of user identification. Additionally, some systems might require additional information from users to identify the application. For example, for access to Oracle, users might enter the information shown in the following table.

|  |  |
| --- | --- |
| In this field | Enter this information |
| Field 1 | Oracle user name |
| Field 2 | Oracle user password (select Yes for the Mask option) |
| Field 3 | Oracle database name |

To access the SAP application, users might enter the information shown in the following table.

|  |  |
| --- | --- |
| In this field | Enter this information |
| Field 1 | SAP user name |
| Field 2 | SAP password (select Yes for the Mask option) |
| Field 3 | SAP system number |
| Field 4 | SAP client number |
| Field 5 | language |

### Account information for enterprise application

If you are using a group account to connect to the enterprise application, you need to provide the account credentials. After adding an enterprise application definition, an SSO administrator or a member of the enterprise application administrator account specifies the account name and password used to connect to the external server computer by clicking Manage Account Information for an Enterprise Application Definition in the Central Administration site.

|  |
| --- |
| Worksheet action |
| Use the [Single sign-on enterprise application definition worksheet](http://go.microsoft.com/fwlink/?LinkId=73335&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73335&clcid=0x409) to record the name of the group account. |

The administrator who enters the account information in the Central Administration site must also know the password for the group account.

If you are using individual accounts to connect to the enterprise application, you do not need to enter account information into the Central Administration site.

## Plan for SSO operations

### Managing the encryption key

The encryption key is used as part of the encryption process for credentials used with SSO. The key helps to decrypt encrypted credentials stored in the SSO database. The first time you configure SSO and enterprise application definitions on the Manage Server Settings for Single Sign-On page in Central Administration, the encryption key is created automatically. Managing the encryption key includes auditing the encryption key and regenerating the encryption key.

#### Auditing the encryption key

You can enable auditing of changes that are made to the encryption key. If the key is read or written to, a security event is logged in the security log. You can view the security log by using Event Viewer. Enabling logging involves:

 Modifying an SSO registry key.

 Creating a local computer policy in Group Policy Object Editor.

#### Regenerating the encryption key

Because the encryption key protects security credentials, you should regenerate the key on a regular schedule, such as every 90 days. You should also regenerate the encryption key if account credentials are compromised.

The reencryption process is a long-running operation. It is recommended that you change the encryption key during non-peak periods. Reencrypting the encryption key has the following impact on the SSO environment:

 During the reencryption process, write operations such as updating credentials and changing enterprise application definitions are not allowed.

 Read operations such as retrieving credentials continue to work as normal.

You must be logged on to the encryption-key server locally to reencrypt the encrypting key. You must also be a member of the SSO administrator account.

If the encryption-key server is restarted or the Single Sign-On service is stopped on the encryption-key server during the reencryption process, you should look in the event log for errors. If the event log reports an error, you must restart the reencryption process. If the reencryption process is preempted in any way, it will have to be rerun. If the reencryption process is preempted, it reverts back to its original state.

When you create an encryption key, you can choose to reencrypt the existing credentials with the new key. If you do not reencrypt the existing credentials with the new encryption key, users must retype their credentials for individual enterprise application definitions, and administrators for group enterprise application definitions must retype group credentials.

When you reencrypt the Single Sign-On service credential store, events are logged in the Microsoft Windows Server 2003 application event log. After reencryption is initiated, you can monitor the application event log to verify that the credential store has been reencrypted. Event ID 1032 is recorded in the application event log when reencryption is started. Event ID 1033 is recorded in the application event log when reencryption has ended. If there are any failures during reencryption, an event is recorded in the log.

When you are deciding your planning choices for managing the encryption key, consider the following:

 At what interval do you plan to reencrypt the encryption key?

 Should the existing credentials be reencrypted with the new encryption key at the same time?

 Under what additional circumstances will the encryption key be reencrypted?

|  |
| --- |
| Worksheet action |
| Use the [Single sign-on server farm settings worksheet](http://go.microsoft.com/fwlink/?LinkId=73336&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73336&clcid=0x409) to record your planning choices. |

### Backing up the SSO environment

Backing up the SSO environment involves backing up the following two separate entities:

 Encryption key

 SSO database

You should back up the encryption key after initially setting up SSO and then back up the key again each time it is regenerated. There is no need to back up the encryption key at a regular interval unless the interval is tied to regenerating the encryption key. The encryption key cannot be backed up remotely. You must be a member of the SSO administrator account and logged onto the encryption-key server locally to back up the encryption key. The encryption key can only be backed up to a removable storage media. It cannot be backed up to a local hard disk. The encryption key can be backed up from the Manage Encryption Key page in Central Administration.

You should back up the SSO database after it is initially created and then again each time credentials are reencrypted. Additionally, you can include SSO database backups with the regularly scheduled database backups for your server farm. Regularly scheduled backups will include other changes to the SSO database, such as new enterprise application definitions and updated credentials.

Do not store the backup media for the encryption key in the same location as the backup media for the SSO database. If a user obtains a copy of both the database and the key, the credentials stored in the database could be compromised. Ideally, the backup of the encryption key is locked up in a safe place.

When you are deciding your planning choices for backing up the SSO environment, consider the following:

 Interval to back up the encryption key.

 Plan for backing up the SSO database. The most efficient plan is to include the SSO database along with your regular farm backups.

|  |
| --- |
| Worksheet action |
| Use the [Single sign-on server farm settings worksheet](http://go.microsoft.com/fwlink/?LinkId=73336&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73336&clcid=0x409) to record your planning choices. |

### Restoring the SSO environment

There are several scenarios that require restoring the SSO environment. In some cases, you need to restore only the encryption key or only the SSO database. The following table describes several restore scenarios and indicates what needs to be restored.

|  |  |
| --- | --- |
| Scenario | What to restore |
| Move the encryption-key server role to a different server computer. | Encryption key |
| Change the SSO service account. | Encryption key |
| Restore the failed database server computer. | SSO database |
| Migrate the Office SharePoint Server 2007 farm to a different set of server computers. | Encryption key and SSO database |
| Recover from a farm-wide disaster. | Encryption key and SSO database |

The rest of this section details the specific tasks involved in restoring the SSO environment, depending on the scenario.

To move the encryption-key server role to a different server computer, use the following steps:

procedure_ddMove the encryption-key server role to a different server computer

|  |
| --- |
| 1. Back up the encryption key.  2. Disable the Single Sign-On service on all computers in the farm.  3. Log on to the new encryption-key server.  4. Start the Single Sign-On service.  5. Configure SSO farm-level settings in the Central Administration site. Specify the existing SSO database.  6. Restore the encryption key.  7. Start the Single Sign-On service on all Web server computers in the server farm. |

#### Change the SSO service account

The security identifier (SID) of the SSO service account is used as part of the formula for encrypting SSO credentials. Consequently, to change the SSO service account, you must reconfigure the SSO environment. Use the following steps to change the SSO service account:

procedure_ddChange the SSO service account

|  |
| --- |
| 1. Back up the encryption key.  2. On all server computers in the farm that are running the Single Sign-On service, reconfigure the service with the new service account.  3. Reconfigure SSO farm-level settings in the Central Administration site with the new SSO service account. Specify the existing SSO database.  4. Restore the encryption key.  5. Reencrypt the credentials in the SSO database. The restored encryption key is used to reencrypt the credentials. |

#### Restore only the SSO database server

If the server computer that hosts the SSO database fails, you need to restore only the SSO database. Restore the database by using the same method you would use to restore any other databases in the Office SharePoint Server 2007 environment. If you restore the SSO database to a different server computer, reconfigure the SSO farm-level settings with the name of the new database server computer.

#### Restore the entire SSO environment

There are several scenarios which require restoring both the encryption key and the SSO database. Use the following steps to restore the entire SSO environment:

procedure_ddRestore the entire SSO environment

|  |
| --- |
| 1. Restore the SSO database to the intended database server computer.  2. Set up and configure SSO as if you were configuring a new SSO environment, except enter the server name and database name of the existing SSO database.  3. Restore the encryption key to the new SSO environment. |

### Responding to an SSO security compromise

A security compromise can include lost backup media, a password leak, or another event that can potentially compromise either the credentials stored in the SSO database or the data stored in the enterprise applications. If you experience a security compromise that can potentially affect your SSO environment, do the following to respond to the compromise:

procedure_ddRespond to a security compromise

|  |
| --- |
| 1. Regenerate the encryption key.  2. Reencrypt the credentials in the SSO database (the new encryption key is used).  3. Change passwords for enterprise applications if the passwords might be compromised.  4. Encourage users to change their passwords if their passwords might be compromised. |

If the security compromise is potentially severe, you can stop the Single Sign-On service to immediately halt access to credentials stored in the SSO database. If you need to stop the Single Sign-On service, you can securely restore the service to the existing Office SharePoint Server 2007 server farm by using the following steps:

procedure_ddRestore the Single Sign-On service to the existing server farm

|  |
| --- |
| 1. Restore the SSO environment to an isolated server computer.  2. Regenerate the encryption key.  3. Reencrypt the credentials in the SSO database.  4. Back up the SSO environment.  5. Restore the SSO environment to the existing Office SharePoint Server 2007 server farm. |

## Worksheets

Use the following worksheets to plan for single sign-on:

 [Single sign-on enterprise application definition worksheet](http://go.microsoft.com/fwlink/?LinkId=73335&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73335&clcid=0x409)

 [Single sign-on server farm settings worksheet](http://go.microsoft.com/fwlink/?LinkId=73336&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=73336&clcid=0x409)

# Plan for administrative and service accounts (Office SharePoint Server)

In this article:

 [About administrative and service accounts](#DSDOC_section1f07768d4_ca37_447a_a056_1a)

 [Standard account requirements](#DSDOC_section2f07768d4_ca37_447a_a056_1a)

 [Planning recommendations for accounts](#DSDOC_section3f07768d4_ca37_447a_a056_1a)

Use this article to plan for the account requirements and recommendations for accounts that are required to install, configure, and use Microsoft Office SharePoint Server 2007.

You must provide credentials for these accounts when you run Setup and during configuration. This article does not discuss accounts for which you do not need to configure or provide credentials.

## About administrative and service accounts

This section lists and describes the accounts that you must plan for. The accounts are grouped according to scope. If an account has a limited scope, you might need to plan multiple accounts for this category. For example, if you are implementing multiple Shared Services Providers (SSPs), you must designate multiple SSP accounts.

### Server farm-level accounts

The following table describes the accounts that are used to configure Microsoft SQL Server and to install Office SharePoint Server 2007.

|  |  |
| --- | --- |
| Account | Purpose |
| SQL Server service account | SQL Server prompts for this account during SQL Server Setup. This account is used as the service account for the following SQL Server services:   MSSQLSERVER   SQLSERVERAGENT  If you are not using the default instance, these services will be shown as:   MSSQL$InstanceName   SQLAgent$InstanceName |
| Setup user account | The user account that is used to run Setup on each server |
| Server farm account | This account is also referred to as:   Database access account  This account is:   The application pool account for the Central Administration site   The process account for the Windows SharePoint Services Timer service |

### SSP accounts

The following table describes the accounts that are used to set up and configure an SSP. Plan one set of SSP accounts for each SSP that you plan to implement.

|  |  |
| --- | --- |
| Account | Purpose |
| SSP application pool security account | Security account for the application pool that the SSP resides in. |
| SSP service account | Used by the following:   SSP Web services for inter-server communication   SSP Timer service to run timer jobs |
| Office SharePoint Server Search | Used as the service account for the Office SharePoint Server Search service. There is only one instance of this service and it is used by all SSPs. |
| Default content access account | The default account used within a specific SSP to crawl content. If a specific account is not specified for a content source, the default content access account is used. |
| Content access account | A specific account that is configured to access a content source. This account is optional and is specified when you create a new crawl rule. For example, content sources that are external to Office SharePoint Server 2007 (such as a file share) might require a different access account. |
| User profile and properties content access account | Used to:   Connect to a directory service, such as the Active Directory directory service, a Lightweight Directory Access Protocol (LDAP) directory, a Business Data Catalog application, or other directory source.   Import profile data from a directory service.  If no account is specified, the default content access account is used. If the default content access account does not have read access to the directory or directories that you want to import data from, then plan to use a different account. You can plan up to one account per directory connection. |
| Excel Services unattended service account | The account that Excel Calculation Services uses to connect to data sources that require user name and password strings for authentication. The SSP service account is used by default. If you want to use an account with fewer privileges (such as an account that does not have database privileges), plan to use a different account instead. |

### Windows SharePoint Services Search accounts

The following table described the accounts that are used to set up and configure Windows SharePoint Services Search. In Office SharePoint Server 2007, this service is referred to as the Windows SharePoint Services Help Search service because this service is used to provide search capability for Help. If you are installing Office SharePoint Server 2007, plan for these accounts only if you plan to implement the service to search Help content.

|  |  |
| --- | --- |
| Account | Purpose |
| Windows SharePoint Services Search service account | Used as the service account for the Windows SharePoint Services Search service. |
| Windows SharePoint Services Search content access account | Used by the Windows SharePoint Services Search application server role to crawl content across sites |

### Application pool accounts

The following table describes the application pool account. Plan one application pool account for each application pool you plan to implement.

|  |  |
| --- | --- |
| Account | Purpose |
| Application Pool process account | Used to access content databases associated with the Web application |

## Standard account requirements

This section details the requirements for each of the accounts. The specific requirements for each account depend on whether you are configuring a single server environment or a server farm environment. The account requirements detail the specific permissions that you need to grant prior to running Setup. In some cases, additional permissions that are automatically granted by running Setup are noted.

At this time, this article does not include account requirements for environments that use SQL authentication.

### Server farm-level accounts

The following table describes the standard account requirements for server farm-level accounts.

|  |  |  |
| --- | --- | --- |
| Account | Single server requirements | Server farm requirements |
| SQL Server service account | Local system account (default) |  Database system administrator |
| Setup user account | Member of the Administrators group on the local computer |  Domain user account   Member of the Administrators group on each server on which Setup is run   Member of the following SQL Server security roles:   Logins   Securityadmin   Dbcreator |
| Server farm account | Network Service (default)  No manual configuration is necessary. |  Domain user account   Additional permissions are automatically granted for this account when Office SharePoint Server 2007 is installed and when additional computers are added to the farm, including additional permissions on front-end Web servers and application servers.   This account is automatically added to the following SQL Server security roles:   Logins   Dbcreator   Securityadmin   Database owner (db\_owner) for all databases |

### SSP accounts

The following table describes the standard account requirements for SSP accounts.

|  |  |  |
| --- | --- | --- |
| Account | Single server requirements | Server farm requirements |
| SSP application pool account | No manual configuration is necessary. | No manual configuration is necessary.  The following permissions are automatically granted for this account when Office SharePoint Server 2007 is installed:   Database owner for the SSP content database   Read/write to the SSP content database   Read/write to content databases for Web applications that are associated with the SSP   Read from the configuration database   Read from the Central Administration content database   Additional permissions on front-end Web servers and application servers |
| SSP service account | No manual configuration is necessary. | No manual configuration is necessary. The same permissions as the SSP application pool account are automatically granted. |
| Office SharePoint Server Search account | By default, this account runs as the local service account. If you want to crawl remote content by using crawl rules, change this to a domain account. If you do not change this account to a domain account, you cannot change the default content access account to a domain account. This restriction is designed to prevent elevation of privilege for any other process running as the local service account. |  Must be a domain account   Must not be a member of the Farm Administrators group  Permissions are automatically granted for this account when Office SharePoint Server 2007 is installed:   Read/write to content databases for Web applications   Read from the configuration database   Read/write to the Windows SharePoint Services Search database |
| Default content access account | No manual configuration is necessary if this account is only crawling local content. If you want to crawl remote content by using crawl rules, change this to a domain account, and apply the requirements listed for a server farm. |  Must be a domain account   Must not be a member of the Farm Administrators group   Read access to external or secure content sources that you want to crawl by using this account  Additional permissions for this account are automatically granted when Office SharePoint Server 2007 is installed. |
| Content access account | Same as the SSP default content access account listed previously | Read access to external or secure content sources that this account is configured to access |
| User profile and properties content access account | Same requirements as server farm |  Read access to the directory service   If Enable Server Side Incremental is selected for an Active Directory connection and the environment is Windows 2000 Server, the account must have the Replicate Changes permission in Active Directory. This permission is not required for Windows Server 2003 Active Directory environments.   Manage user profiles shared service right (Personalization services permissions)   View rights on entities used in Business Data Catalog import connections. |
| Excel Services unattended service account | Read/write access to the Excel data sources | Read/write access to the Excel data sources |

### Windows SharePoint Services Search accounts

The following table describes the standard account requirements for Windows SharePoint Services Search accounts.

|  |  |  |
| --- | --- | --- |
| Account | Single server requirements | Server farm requirements |
| Windows SharePoint Services Search service account | By default, this account runs as the local service account. If you want to crawl remote content by using crawl rules, change this to a domain account. If you do not change this account to a domain account, you cannot change the default content access account to a domain account. This behavior is designed to prevent elevation of privilege for any other process running as the local service account. |  Must be a domain account   Must not be a member of the Farm Administrators group  Permissions are automatically granted for this account when  12 is installed:   Read/write to content databases for Web applications   Read from the configuration database   Read/write to the Windows SharePoint Services Search database |
| Windows SharePoint Services Search Content access account | Must not be a member of the Farm Administrators group  Read access to Web applications |  Same requirements as the Windows SharePoint Services Search service account   Read access to Web applications  Permissions are automatically granted for this account when Office SharePoint Server 2007 is installed:   Added to the Web application Full Read policy for your farm |

### Application pool accounts

The following table describes the standard account requirements for application pool accounts.

|  |  |  |
| --- | --- | --- |
| Account | Single server requirements | Server farm requirements |
| Application pool process account | No manual configuration is necessary. | No manual configuration is necessary.  The following SQL Server roles and permissions are automatically assigned to this account:   Database owner role for content databases associated with the Web application   Read/write access to the associated SSP database   Read from the configuration database  Additional permissions for this account on front-end Web servers and application servers are automatically granted by Office SharePoint Server 2007. |

## Planning recommendations for accounts

This section describes planning recommendations for implementing accounts in the following two deployment scenarios:

 [Secure farm environment](#DSDOC_subsection1f07768d4_ca37_447a_a056)

 [Single-server environment](#DSDOC_subsection2f07768d4_ca37_447a_a056)

These recommendations are practical for most environments.

### Secure farm environment

These planning recommendations are for individual accounts in a secure farm environment.

#### Server farm-level accounts

The following table describes the planning recommendations for server farm-level accounts in a secure farm environment.

|  |  |
| --- | --- |
| Account | Recommendation |
| SQL Server service account | A domain account is recommended over a SQL Server account or a local account. No special domain permissions are required.  Do not use the server farm account for this account. |
| Setup user account | A domain account is recommended.  For a workgroup environment, this can be a local Windows account. |
| Server farm account | A domain account is recommended. |

#### SSP accounts

The following table describes the planning recommendations for SSP accounts in a secure farm environment.

|  |  |
| --- | --- |
| Account | Recommendation |
| SSP Application Pool account | A domain account is recommended. Use a domain account that is unique (different from the farm or content application pool accounts). |
| SSP service account | Use the SSP application pool account. |
| Office SharePoint Server Search account | The local service account is used by default. After completing Setup, change this account to a domain account. In an environment with multiple SSPs, do not use the same account for the account that searches a specific SSP. |
| Default content access account | By default, the Network Service account is used. After completing Setup, change this account to a domain account. Do not give the default content access account access to the directory service. |
| User profile and properties content access account | Use an account that has read access to the directory service and the rights to manage user profiles. |
| Excel Services unattended service account | The SSP application pool account is used by default. |

#### Windows SharePoint Services Search accounts

The following table describes the planning recommendations for Windows SharePoint Services Search accounts in a secure farm environment.

|  |  |
| --- | --- |
| Account | Recommendation |
| Windows SharePoint Services Search service account | The local service account is used by default. After completing Setup, change this account to a domain account. |
| Windows SharePoint Services Search content access account | The local service account is used by default. After completing Setup, change this account to a domain account. You can use the same account used by the Windows SharePoint Services Search service. However, if you implement multiple search servers for isolation, use a separate account. It is recommended that you select a unique user account that cannot modify content and is not a member of the Administrators group on your front-end Web servers or on your database servers. |

#### Application pool accounts

The following table describes the planning recommendations for application pool accounts in a secure farm environment.

|  |  |
| --- | --- |
| Account | Recommendation |
| Application pool process account | Plan a unique domain account for each application pool. It is recommended that you select a unique user account that does not have administrative rights on your front-end servers or on your back-end database servers. |

### Single-server environment

The following table describes the planning recommendations for several different single-server environments. These are environments where a single server hosts all server roles.

|  |  |
| --- | --- |
| Scenario | Recommendation |
| Microsoft SQL Server 2005 Express Edition | Use the standard administrator account to run Setup.  Use the default accounts assigned by Setup.  Assign to the Network Service account the necessary permissions to SQL Server. |
| SQL Server in a domain environment | Use the recommendations provided for a secure farm environment. |
| SQL Server in a workgroup environment | Use the recommendations provided for a secure farm environment, except use Windows accounts instead of domain accounts. |

# XVII Plan for performance and capacity

In this chapter:

 [Chapter overview: Plan for performance and capacity (Office SharePoint Server)](#DSDOC_8dd52916_f77d_4444_b593_1f7d6f330e)

 [Plan for software boundaries (Office SharePoint Server)](#DSDOC_6a13cd9f_4b44_40d6_85aa_c70a8e5c34)

 [Chapter overview: Estimate performance and capacity requirements [Office SharePoint Server]](#DSDOC_054526b9_417e_4140_b251_79b68e771c)

 [Portal collaboration environments](#DSDOC_a76963dc_1cd0_4aff_ae9c_3736d89c42)

 [Tools for performance and capacity planning [Office SharePoint Server]](#DSDOC_301ed832_95da_4251_b266_7be6288f7e)

 [Additional performance and capacity planning factors (Office SharePoint Server)](#DSDOC_9f3cfe3f_01b5_406e_8615_04735ae422)

# Chapter overview: Plan for performance and capacity (Office SharePoint Server)

This content is preliminary content. It might be incomplete and is subject to change.

Performance and capacity planning is the process of mapping your solution design to a farm size and set of hardware that will support your business goals.

The articles in this chapter include:

 [Plan for software boundaries (Office SharePoint Server)](#DSDOC_6a13cd9f_4b44_40d6_85aa_c70a8e5c34)

 [Chapter overview: Estimate performance and capacity requirements [Office SharePoint Server]](#DSDOC_054526b9_417e_4140_b251_79b68e771c)

 [Windows SharePoint Services collaboration environments (Office SharePoint Server)](#DSDOC_0a7b2b45_f633_46d2_a4fd_78691d4b8f)

 [Portal collaboration environments](#DSDOC_a76963dc_1cd0_4aff_ae9c_3736d89c42)

 [Excel Services environments](#DSDOC_f0ff6cc9_2f84_4d73_8ac2_390bbcb08c)

 [Document repository environments](#DSDOC_3a693e2d_44a7_4c1a_8b8f_425ab57d8e)

 [Internet environments](#DSDOC_45997bad_da15_4442_8727_78e0f2dc5a)

 [ISP hosting environments](#DSDOC_007e4665_5bad_4591_8fe4_11eae89986)

 [Corporate hosting environments](#DSDOC_e517fe63_c9c1_4388_a27f_fee04cc706)

 [Additional performance and capacity planning factors (Office SharePoint Server)](#DSDOC_9f3cfe3f_01b5_406e_8615_04735ae422)

 [Tools for performance and capacity planning [Office SharePoint Server]](#DSDOC_301ed832_95da_4251_b266_7be6288f7e)

## About performance and capacity planning

This chapter walks you through the process of determining the hardware requirements for a single farm. It identifies the characteristics that will impact your performance and capacity requirements and provides recommendations for the following:

 Number of server computers in the server farm.

 Configuration of application server roles in the server farm.

 Hardware requirements for specific server roles in the server farm.

Your capacity planning process should include a testing program for the characteristics specific to your environment. Due to the variety of factors that can impact performance and capacity in a given environment, testing is a crucial step in establishing the characteristics of your environment.

### Planning for capacity vs. availability

This chapter assumes that you have already used the [Plan for availability (Office SharePoint Server)](#DSDOC_9ccfb27f_ecba_4b7d_b9a0_88fac71478) article to plan for availability requirements. As a result of using the "Plan for availability" article, you will start the capacity planning exercise with a topology that meets your organization's minimum availability requirements. Given the topology you have determined you will deploy, this chapter will help you determine:

 If you need to add additional servers to meet your goals for capacity and performance.

 If you need to adjust the configuration of application server roles to optimize capacity and performance of the server farm.

 If you need to plan for more than one server farm based on your capacity requirements.

In some cases, an organization's requirements for availability can result in a server farm size that provides greater capacity or performance than is otherwise required. If this is the case, your capacity planning process can focus on sizing the server hardware economically, rather than on adding additional server computers or scaling up with higher-performing hardware.

In many cases, the topology that meets an organization's minimum availability requirements is used as a starting point and server computers are added or scaled up to meet capacity and performance goals.

### 64-bit vs. 32-bit

Although Microsoft Windows SharePoint Services 3.0 and Microsoft Office SharePoint Server 2007 can be deployed on 32-bit servers, Microsoft recommends that you employ 64-bit servers in Windows SharePoint Services or Office SharePoint Server farm deployments. The guidance presented in this guide is based on testing conducted on 64-bit servers. Therefore, if you are planning to deploy to 32-bit servers, you should perform additional testing on the 32-bit servers in your environment. The best practices and performance trends in this guide will still generally apply to 32-bit environments, but actual results may vary.

The 64-bit system architecture has several characteristics that contribute to superior server scalability and performance:

 Memory addressability   A 32-bit system can directly address only a 4-GB address space. Windows Server 2003 SP1 running on a 64-bit system architecture supports up to 1,024 gigabytes of both physical and addressable memory.

 Larger numbers of processors and more linear scalability per processor   Improvements in parallel processing and bus architectures enable 64-bit platforms to support larger numbers of processors (up to 64) while providing close to linear scalability with each additional processor. Server platforms that offer more than 32 CPUs are available exclusively on 64-bit architecture.

 Enhanced bus architecture   The bus architecture on current 64-bit chipsets is faster and wider than earlier generations. More data is passed to the cache and processor; this is somewhat analogous to the improvement that broadband connections offer over dial-up connections.

#### Upgrading from SharePoint Portal Server 2003

Due to the richer set of features included in Office SharePoint Server 2007, a more robust server environment is needed to maintain the performance benchmarks you have established with SharePoint Portal Server 2003. You will probably find that, unless your current SharePoint Portal Server hardware is quite current and has substantially greater resources than required to support your current environment, your Office SharePoint Server 2007 deployment will require upgraded hardware.

You can deploy an Office SharePoint Server 2007 farm on a mix of 32-bit and 64-bit servers, provided that you maintain architecture homogeneity at each topology layer. For example, you should not mix 32-bit and 64-bit Web front-end (WFE) servers, but you may use 64-bit database servers in a farm with 32-bit WFE servers and application servers.

If you are upgrading an existing farm, or intend to deploy 64-bit servers only where necessary, we recommend that you prioritize the use of 64-bit servers as follows:

1. Computers running SQL Server

2. Application servers (in this order)

a. Index

b. Excel

c. Search

3. WFE servers

### Performance and capacity planning approach

There are many variables that impact performance and capacity planning. For this reason, it can be difficult to receive a crisp answer to a straightforward question. Consequently, the most common answer to a performance- or capacity-related question begins with, "It depends…".

The performance and capacity planning exercise provided in this chapter is designed to reduce the number of variables in consideration so that straightforward answers can be provided based on common scenarios. However, this chapter also includes the guidance for calculating your capacity and performance requirements based on your individual solution characteristics. This chapter includes two types of planning guidance:

 Recommendations for estimating performance and capacity requirements   A series of articles are provided based on targeted scenarios. Each article defines a typical usage profile and identifies the key characteristics that will impact capacity and performance for the scenario. Based on the profile and key characteristics, pre-canned data allows you to estimate capacity capabilities for your solution.

 Formulas and guidance for calculating specific performance and capacity requirements   Using this guidance, you can develop your own usage profile (or modify one of the scenario profiles) and calculate all of the variables that impact the capacity and performance of your solution.

### Performance and capacity planning process

Performance and capacity planning focuses on three aspects of a sizing your solution:

 Software boundaries   Each of the features that can be implemented and the objects that can be created have scale limitations. Planning for capacity boundaries ensures that your solution design fits within the scale recommendations of the software. Software boundaries and limits provided in this guide apply to all Office SharePoint Server 2007 and Windows SharePoint Services 3.0 environments.

 Throughput targets   Throughput is the number of operations per second that a server or server farm is able to process. Each type of action performed by a server farm introduces a performance load on the server hardware. Primary actions include user operations, indexing content, and operations tasks (such as backing up the databases). The use of specific features, such as Excel calculation services and content staging, also add a performance load. Developing throughput targets involves estimating or calculating the number of operations per second that a server farm will need to process in order to support the expected throughput load.

 Data capacity   Data capacity includes the expected volume of content databases and the configuration database. Each server role also has unique data requirements based on the solution, such as disk space for content indexes or for cached content.

Guidance for establishing throughput targets and data capacity is provided for each of the scenarios in the [Chapter overview: Estimate performance and capacity requirements [Office SharePoint Server]](#DSDOC_054526b9_417e_4140_b251_79b68e771c) section.

The recommended process includes the following steps:

 [Plan for software boundaries (Office SharePoint Server)](#DSDOC_6a13cd9f_4b44_40d6_85aa_c70a8e5c34)   Review the software boundaries and limits of the software against your solution design, and make adjustments to your design, if necessary.

 [Chapter overview: Estimate performance and capacity requirements [Office SharePoint Server]](#DSDOC_054526b9_417e_4140_b251_79b68e771c)   Identify the scenario that most closely matches your solution and review the guidance in the corresponding planning article. Use the article to identify the key performance and capacity characteristics for your environment, to estimate throughput and data capacity targets for your solution, and to evaluate your targets against the performance of several sample topologies and sizes of hardware.

 Plan scale actions based on performance and growth   After you understand the performance characteristics of your solution and you have determined the server hardware that is required to support your solution, you can plan scale actions for future growth.

 Test solution for your environment   After you have established a starting point topology, you can deploy a test environment based on your deployment plan. Use the test tools provided to establish actual performance and capacity data for your environment, and revise your deployment plan as required.

### Terminology

##### Availability

The percentage of time the system is able to respond to user requests. This can also be expressed in the equation (total time – downtime)/(total time). Typical availability requirements for mission-critical systems are 99.99% (less than 2 hours of downtime per year) to 99.999% (less than 5 minutes of downtime per year).

##### Common operation

A user operation that is performed frequently, such as accessing a SharePoint library or opening a document from the SharePoint server.

##### Long-running operation

A user operation with a long expected duration, such as creating a new Web application. A long-running operation is generally accompanied by a progress indicator.

##### Scalability

A measure of how well a computer, service, or application can grow to meet increasing performance demands. For server farms, the ability to incrementally add one or more computers to an existing farm when the overall load exceeds the current farm's capabilities.

##### Throughput

The number of operations per second that a server or server farm is able to process.

##### Rare operation

A user operation that is performed infrequently, such as changing a service account password.

##### RPS

Requests per second. This is a measurement of how many requests per second the system can process.

##### Uncommon operation

A user operation that is performed regularly, but at infrequent intervals. An example of an uncommon operation is adding a content type or upgrading a form template.

##### User Response Time

For the purposes of this guide, user response time can be defined as the length of time that a user perceives to occur between an event, such as clicking on a link to view a document library, and the completion of the resultant process. User response time is determined by a wide variety of factors, including memory usage, processor availability, disk access speed, and network bandwidth.

# Plan for software boundaries (Office SharePoint Server)

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [Test environment](#DSDOC_section16a13cd9f_4b44_40d6_85aa_c7)



 [Guidelines for acceptable performance](#DSDOC_section36a13cd9f_4b44_40d6_85aa_c7)

The test results and guidelines provided in this article apply to a single installation of Microsoft Office SharePoint Server 2007. Adding servers to the installation does not increase the capacity limits of the site objects listed in the table below. However, increasing the number of server computers increases the throughput of a server farm, which might be necessary to achieve acceptable performance with large numbers of objects. In some cases, the requirements for high numbers of objects within a solution might require the use of more than one server farm.

There are very few hard limits. Most of the scale guidelines are determined by performance. In other words, you can exceed the guidelines provided, but as you increase the scale, you may experience reduced performance.

Note that there are many factors that can affect performance in a given environment, and each of these factors may affect performance in different areas. Some of the test results and recommendations in this guide may be related to features or user operations that may not exist in your environment, and therefore may not apply to your solution. Only thorough testing can provide you with exact data related to your own environment.

See the section [Additional performance and capacity planning factors (Office SharePoint Server)](#DSDOC_9f3cfe3f_01b5_406e_8615_04735ae422) in this guide for more information on other factors that can affect performance and capacity but were not part of the testing process for this guide.

## Test environment

The following table lists the specifications of the computers in the test environment.

|  |  |
| --- | --- |
| Role | Specifications |
| Stand-alone computer | 1 dual core Intel Xeon 2.8 gigahertz (GHz) 64-bit processor, 2GB RAM |
| Web server computer | 2 dual core Intel Xeon 2.8 GHz 64-bit processors, 4 gigabytes (GB) RAM |
| Database computer running Microsoft SQL Server | 4 dual core Intel Xeon 2.8 GHz 64-bit processors, 3 2GB RAM |
| Client computers | Pentium III 1.2 GHz processor, 1 GB RAM |

A gigabit Ethernet network (one billion bits/sec) was used between the farm computers.

Testing was performed against the configurations listed in the following table.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Database server | 1 Web server | 2 Web servers | 3 Web servers | 4 Web servers | 5 Web servers | 6 Web servers | 7 Web servers | 8 Web servers |
| 0 | X |  |  |  |  |  |  |  |
| 1 | X | X | X | X | X | X | X | X |

Environment-specific testing was also performed against several farm configurations. See the scenario articles in the [Chapter overview: Estimate performance and capacity requirements [Office SharePoint Server]](#DSDOC_054526b9_417e_4140_b251_79b68e771c) section for information about environment-specific configuration testing.

## Test results

The following charts, graphs and tables show how the test environment performed given a certain set of parameters, user operations, and load conditions. These tests were all conducted on an 8x1 Office SharePoint Server 2007 farm. Results provided apply to all Office SharePoint Server 2007 environments.

note_ddNote:

Additional configurations will be tested in the future. Test results will be published as they become available.

Performance metrics for different operations depend on how site collections are used. For example, a single site collection can have thousands of subsites, but user response times for operations that enumerate the container begin to increase as the number of site collections increases. Other operations that do not enumerate the container will continue to perform acceptably.

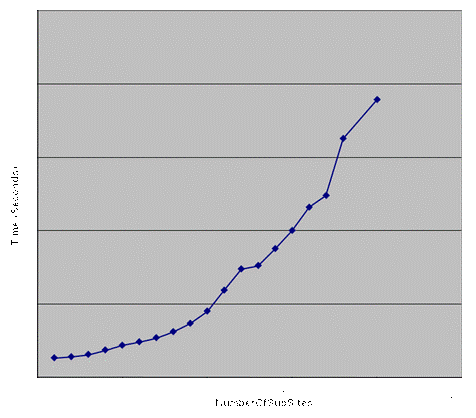
The subsites created for the tests break down as shown in the following table.

|  |  |
| --- | --- |
| Type of subsite | Percent of total |
| Team sites | 55% |
| Document workspace | 20% |
| Meeting workspace | 10% |
| Blog | 10% |
| Wiki | 5% |

### Throughput changes when creating a site vs. enumerating sites as the number of sites increases

User response time for certain operations increases with the number of sites in a site collection.

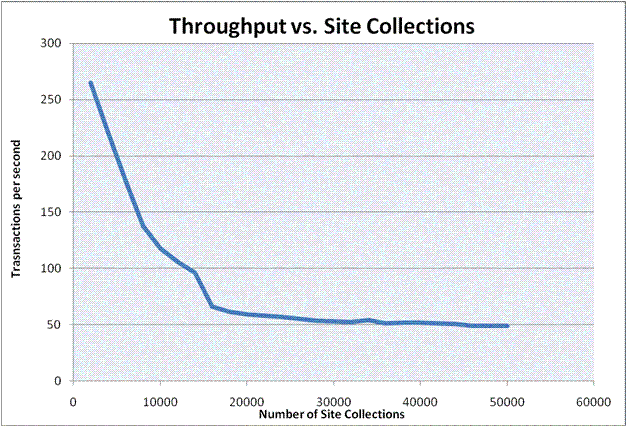
This graph shows the user response time when enumerating the sites in a site collection and when creating a new site as the number of existing sites increases.



### Throughput vs. number of site collections

Throughput, measured in RPS, decreases as the number of site collections in a farm increases.

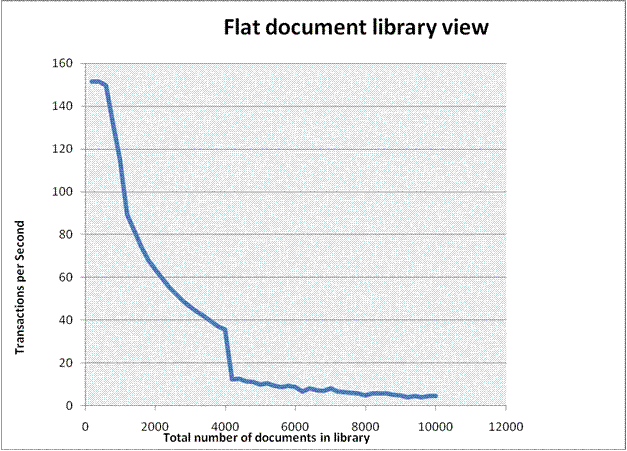
The following figure shows the decrease in throughput when browsing to the home page of different site collections as the number of site collections in a single content database increases. Throughput decreases quickly as the total number of site collections increases from 2000 (RPS=265) to 16,000 (RPS=66), then RPS remains approximately 50 as the total number of site collections increases to 50,000.



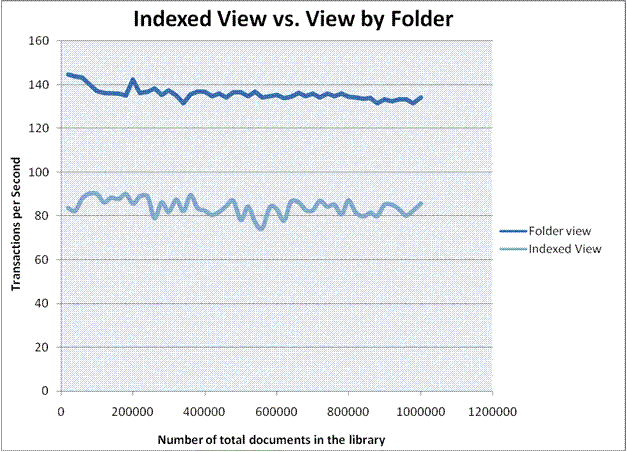
### Throughput differences between flat document library vs. document library with folders

Throughput for certain operations decreases as the number of items in a folder increases.

The following figure shows the difference in throughput between viewing all items in a document library with and without the effective use of folders, which is critical for scaling. As shown in the graph below, throughput performance degrades as the number of documents increases when flat library storage is used. The quickest drop in throughput occurs when the total number of documents is less than 2,000, from 151 RPS (at 200 documents) to 63 RPS (at 2,000 documents). At 4,000 documents, throughput decreases to about 13 RPS, or an overall throughput decrease of over 90% from an empty library.



The following figure shows the relative performance between folder views when folders are used to store and organize documents, and an indexed view of a flat library structure. Each folder contains 500 documents created by different users. In this scenario, there is no significant throughput degradation up to 1 million documents for either scenario, provided that the number of items in the view does not exceed the performance threshold for your system. However, performance is better when folders are used.



As the number of items in a folder increases, folder view performance will gradually degrade. Note that the above results are estimates based on our testing, and results may vary in your environment.

## Guidelines for acceptable performance

Capacity is directly affected by scalability. This article lists the objects that can compose a solution and provides guidelines for acceptable performance for each type of object. Use the guidelines in this article to review your overall solution plans.

If your solution plans exceed the recommended guidelines for one or more objects, take one or more of the following actions:

 Evaluate the solution to ensure that compensations are made in other areas.

 Flag these areas for testing and monitoring as you build and deploy your solution.

 Re-design the solution to ensure that you do not exceed capacity guidelines.

The following tables list the objects by category and include recommended guidelines for acceptable performance. Acceptable performance means that the system can support that number of objects, but that the number cannot be exceeded without some performance degradation. An asterisk (\*) indicates a hard limit; no asterisk indicates a tested or supported limit.

The following table lists the recommended guidelines for site objects.

|  |  |  |  |
| --- | --- | --- | --- |
| Site object | Guidelines for acceptable performance | Notes | Scope of impact when performance degrades |
| Site collection | 50,000 per Web application | Total farm throughput degrades as the number of site collections increases. | Farm |
| Web site | 250,000 per site collection | You can create a very large total number of Web sites by nesting the subsites. For example, 100 sites, each with 1000 subsites, is 100,000 Web sites. The maximum recommended number of sites and subsites is 125 sites with 2,000 subsites each, for a total of 250,000 sites. | Site collection |
| Subsite | 2,000 per Web site | The interface for enumerating subsites of a given Web site does not perform well as the number of subsites surpasses 2,000. | Site view |
| Document | 5 million per library | You can create very large document libraries by nesting folders, using standard views and site hierarchy. This value may vary depending on how documents and folders are organized, and by the type and size of documents stored. | Library |
| Item | 2,000 per view | Testing indicates a reduction in performance beyond two thousand items. Using indexing on a flat folder view can improve performance. | List view |
| Document file size | 50MB (2GB max\*) | File save performance is proportional to the size of the file. The default maximum is 50 MB. This maximum is enforced by the system, but you can change it to any value up to 2 GB. | Library, file save performance |
| List | 2,000 per Web site | Testing indicates a reduction in list view performance beyond two thousand entries. | List view |
| Field type | 256 per list | This is not a hard limit, but you may experience list view performance degradation as the number of field types in a list increases. | List view |
| Web Part | 100 per page | This figure is an estimate based on simple Web Parts. The complexity of the Web Parts dictates how many Web Parts can be used on a page before performance is affected. | Page |

The following table lists the recommended guidelines for people objects.

|  |  |  |
| --- | --- | --- |
| People object | Guidelines for acceptable performance | Notes |
| Users in groups | 2 million per Web site | You can add millions of people to your Web site by using Microsoft Windows security groups to manage security instead of using individual users. |
| User profile | 5 million per farm | This number represents the number of profiles which can be imported from a directory service, such as Active Directory, into the people profile store. |
| Security principal | 2,000 per Web site | The size of the access control list is limited to a few thousand security principals (users and groups in the Web site). |

The following table lists the recommended guidelines for search objects.

|  |  |  |
| --- | --- | --- |
| Search object | Guidelines for acceptable performance | Notes |
| Search indexes | 1 per query server |  |
| Indexed document | 50 million per search index | 50 million documents per index server are supported, and one search index per index server. This means that the effective limit of documents per index server is 50 million. |

The following table lists the recommended guidelines for logical architecture objects.

|  |  |  |
| --- | --- | --- |
| Logical architecture object | Guidelines for acceptable performance | Notes |
| Shared Services Provider (SSP) | 3 per farm (20 per farm maximum) |  |
| Zone | 5\* per farm | The number of zones defined for a farm is hard coded to 5. |
| Web application | 99 per SSP | This limit includes the number of Web applications on child farms consuming resources on this SSP. |
| Internet Information Services (IIS) application pool | 8 per Web server | Maximum number is determined by hardware capabilities. |
| Site collection | 50,000 per Web application |  |
| Content database | 100 per Web application |  |
| Site collection | 50,000 per database |  |

The following table lists the recommended guidelines for physical objects.

|  |  |  |
| --- | --- | --- |
| Physical object | Guidelines for acceptable performance | Notes |
| Index servers | 1 per SSP\* |  |
| Application servers running Excel Calculation Services | No limit |  |
| Query servers | No limit | Because 100 content databases are supported for each query server, the number of query servers required per farm is based on the number of content databases in the farm. For example, if there are 500 content databases in your farm, you will need at least 5 query servers. |
| Web server/database server ratio | 8\* Web servers per database server | The scale out factor is dependent upon the mix of operations. |
| Web server/Domain Controller ratio | 3 Web servers per Domain Controller | Depending on how much authentication traffic is generated, your environment may support a greater number of Web servers per domain controller. |

### Throughput vs. number of Web servers

In our test environment, farm throughput reached a plateau at 5 Web servers per database server, and did not change substantially when additional Web servers were added. Although you can deploy up to 8 Web servers per database server, you may not realize substantial throughput gains after 5 Web servers. This is because as the number of Web servers making calls against a single database server increases, the database server eventually reaches 100% capacity. Results in your environment may vary according to the performance characteristics of your database server. You will need to conduct your own testing to determine the optimum number of Web servers in your farm environment.

Adding more Web servers to a farm after optimum throughput has been achieved may be desirable for other reasons—for example, if a substantial portion of Web server CPU utilization is consumed by user authentication. In such a case, you should conduct testing to determine the correct solution.

### User response times

The following table provides guidelines for acceptable user response times for four types of user operations. Note that your business requirements may allow longer or shorter response times than suggested.

The testing goal was to provide sub-second response time for all end-user operations. However, this is not possible in all cases, so the guidelines in the following table were used.

|  |  |  |
| --- | --- | --- |
| Type of operation | Examples | Acceptable user response time |
| Common operation |  Browsing to the home page   Browsing to a document library | <3 seconds |
| Uncommon operation |  Creating a subsite Creating a list   Uploading a document to a document library | <5 seconds |
| Rare operation |  Backing up a site   Creating a site collection | <7 seconds |
| Long-running operation |  Indexing a site | Varies with operation and system configuration. All long running operations will have either an information or status page. |

# A Estimate performance and capacity requirements (Office SharePoint Server)

Insert introduction here.

## Subhead

Insert section body here.

### Subhead

Insert section body here.

# Chapter overview: Estimate performance and capacity requirements [Office SharePoint Server]

This content is preliminary content. It might be incomplete and is subject to change.

In order to provide specific guidance, several configurations were tested that cover the most common usage scenarios for Microsoft Office SharePoint Server 2007 and Microsoft Windows SharePoint Services 3.0. These articles include:

 [Windows SharePoint Services collaboration environments (Office SharePoint Server)](#DSDOC_0a7b2b45_f633_46d2_a4fd_78691d4b8f)

 [Portal collaboration environments](#DSDOC_a76963dc_1cd0_4aff_ae9c_3736d89c42)

 [Excel Services environments](#DSDOC_f0ff6cc9_2f84_4d73_8ac2_390bbcb08c)

 [Document repository environments](#DSDOC_3a693e2d_44a7_4c1a_8b8f_425ab57d8e)

 [Internet environments](#DSDOC_45997bad_da15_4442_8727_78e0f2dc5a)

 [ISP hosting environments](#DSDOC_007e4665_5bad_4591_8fe4_11eae89986)

 [Corporate hosting environments](#DSDOC_e517fe63_c9c1_4388_a27f_fee04cc706)

Each of these environment-specific articles provides the following information:

 Key characteristics – General characteristics of the scenario, such as system security, varieties of common user operations, and how the system will grow over time. Assumptions for system architecture, user authentication methods, user response times, and concurrency.

 Test environment – The design parameters used for testing, including number of users, user operation mix, number of sites, views, indexing, and number of documents per library.

 Usage profile – Details about the percentage of system resources consumed by user operations, throughput data, and the impact of scale increases on system performance.

 Recommendations – Recommendations on hardware requirements, throughput, data capacity, performance monitoring, and environment-specific factors.

# Windows SharePoint Services collaboration environments (Office SharePoint Server)

In this article:

 [Key characteristics](#DSDOC_section10a7b2b45_f633_46d2_a4fd_78)

 [Test environment](#DSDOC_section20a7b2b45_f633_46d2_a4fd_78)

 [Usage profile](#DSDOC_section30a7b2b45_f633_46d2_a4fd_78)

 [Recommendations](#DSDOC_section40a7b2b45_f633_46d2_a4fd_78)

This performance and capacity planning scenario incorporates a single Microsoft Windows SharePoint Services 3.0 farm used for collaboration and document management in an enterprise environment.

## Key characteristics

Key characteristics describe environmental factors, usage characteristics, and other considerations common to the scenario.

The key characteristics for this scenario include:

 Authentication/authorization — Typically users are authenticated and sites and content are secured either by using security groups or by granting access to individual users based on their user account. Integrated Windows authentication is used in this scenario.

 Both common (read) and complex (read/write) user operations — In a collaboration environment, users view and contribute to content. Throughput targets for this scenario are designed to ensure reasonable response times for complex user operations, such as uploading or downloading a document.

 Data and site growth over time — In addition to estimating the initial data volume, a Windows SharePoint Services 3.0 collaboration environment must also allow for data and site growth over time. A server farm that is sized only for the initial data volume can quickly be outgrown.

 User response times — Target user response times for common, uncommon, long-running, and rare operation are listed in the User response time table at the end of the Plan for software boundaries [Windows SharePoint Services] section, are targeted. Some organizations might tolerate slower user response times or might require faster user response times. The expected user response time is a key factor that determines overall throughput targets. (Throughput is defined as how many requests the server farm can process per second). A greater number of users requires a higher throughput target to achieve the same user response time.

 User concurrency — A concurrency rate of 10% is assumed, with 1% of concurrent users making requests at a given moment. In other words, for 10,000 users, the assumption is that 1,000 users will be actively using the solution at the same time, and that 100 users will be actively making requests.

 Long-running asynchronous tasks — Tasks such as indexing content and backing up databases add a performance load to the server farm. The general performance characteristics of sample topologies assume that these tasks are running during off-peak hours, such as overnight. Thus, user response rates during business hours are not affected.

## Test environment

Testing for this scenario was designed to help develop estimates of how different farm configurations respond to changes in a variety of factors, including number of concurrent users, user operations, and the number of objects such as site collections, sites, libraries, and lists.

It is important to note that although certain conclusions can be drawn from the test results, the specific capacity and performance figures in this section will vary in real-world environments. These results are intended to provide a starting point for the design of a properly scaled environment. After you have completed your initial system design, test the configuration to determine if your system will support the factors inherent in your environment.

For more information about testing your deployment, see Tools for performance and capacity planning (Windows SharePoint Services).

### Assumptions

 64-bit architecture – Only 64-bit servers were used in the test environment.

### Lab Topology

In order to provide a high level of test-result detail, several farm configurations were used for testing, ranging from a stand-alone computer to eight Web servers with single and clustered computers running Microsoft SQL Server 2003. Testing was performed with eight client computers simulating from 32 through 256 user connections.

The following table lists the specific hardware used for testing.

|  |  |
| --- | --- |
| Computer role | Hardware |
| Web server | 2 dual-core Intel Xeon 2.8 gigahertz (GHz) processors  4 gigabytes (GB) RAM |
| Database server | 4 dual-core Intel Xeon 2.8 GHz processors  32 GB RAM |
| Client computer | 1 Pentium 3 1.2 GHz processor  1 GB RAM |

A gigabit (1 billion bits/sec) network was used in the test environment.

## Usage profile

The following table shows the usage profile for the   collaboration test environment. Note that the usage profile for the Windows SharePoint Services 3.0 collaboration scenario assumes that the majority of user actions are within team sites.

Search within Windows SharePoint Services is scoped to a site collection. Consequently, search actions do not substantially affect throughput.

The following table shows the percentage of throughput consumed by each listed type of user operation in the test environment.

|  |  |
| --- | --- |
| Operation | Percentage of throughput |
| Get home page | 15.00 |
| Get cached document | 15.00 |
| Get static document | 15.00 |
| Get list page (HTML) | 10.00 |
| Get list page (grid) | 10.00 |
| Get list form | 7.00 |
| 404 errors | 5.00 |
| Insert list item | 2.00 |
| Edit list item | 2.00 |
| Delete list item | 2.00 |
| Insert document | 2.00 |
| Synchronize with Outlook | 2.00 |
| Delete document | 2.00 |
| List URLs | 2.00 |
| DAV Open document for edit | 1.00 |
| DAV Save document | 1.00 |
| FPRPC Open document for edit | 1.00 |
| FPRPC Save document | 1.00 |
| Short-term check-out | 1.00 |
| Incoming e-mail | 1.00 |
| RSS | 1.00 |
| Start workflow | 0.75 |
| Workflow task completion | 0.75 |
| Add/remove user | 0.50 |

## Recommendations

This section provides general performance and capacity recommendations. Use these recommendations to determine the capacity and performance characteristics of the starting topology that you created in Plan for availability (Windows SharePoint Services) article) and to determine whether you need to scale the starting topology out or up.

### Hardware recommendations

The following table lists the recommended hardware for Web servers and database servers. For more information about minimum and recommended system requirements, see Determine hardware and software requirements (Windows SharePoint Services).

|  |  |
| --- | --- |
| Computer role | Recommended hardware |
| Web server | Dual 2.5 GHz or faster processors (3 GHz or faster recommended)  1 GB RAM, 2 GB recommended  3 GB of available disk space  DVD drive, local or network accessible  1024x768 or higher resolution monitor |
| Database server | Dual 2.5 GHz or faster processors (3 GHz or faster recommended)  2 GB RAM, 4 GB recommended  Hard disk space based on a 1:1.2 ratio of content to database capacity. That is, if you plan for 100 GB of content, you need at least 120 GB of available disk space, plus additional space for transaction logs.  DVD Drive, local or network accessible  1024x768 or higher resolution monitor |

### Starting-point topologies

You can estimate the performance of your starting-point topology by comparing your topology to the starting-point topologies that are provided in Plan for availability (Windows SharePoint Services). So doing can help you quickly determine if you need to scale your starting-point topology to meet your performance and capacity goals.

#### Capacity and performance of scaled-out topologies

To increase the capacity and performance of one of the starting-point topologies, either scale up by implementing server computers with greater capacity or scale out by adding additional servers to the topology. This section describes the general performance characteristics of several scaled-out topologies. The sample topologies represent the following common ways to scale a topology for the collaboration scenario:

 To accommodate greater user load, add Web server computers.

 To accommodate greater data load, add capacity to the database server role by increasing the capacity of a single (clustered or mirrored) server, by upgrading to a 64-bit server, or by adding clustered or mirrored servers.

 Maintain a ratio of no greater than eight Web server computers to 1 (clustered or mirrored) database server computer.

### Estimating throughput targets

Throughput is the number of operations that a server farm can perform per second. Ideally the number of operations that are requested per second is lower than the number that can be performed. If the number of operations that is requested exceeds the number that can be performed, user actions and other operations take longer to complete.

Throughput is measured in requests per second (RPS). RPS measurements can be converted to the total number of users by using a model of typical end-user behavior. Like many human behaviors, there is a broad range of "typical" behavior. The user model for Windows SharePoint Services 3.0 has the following two variables:

1. Concurrency - The percentage of users that are using the system simultaneously.

2. Request rate — The average number of requests per hour that an active user generates. Four levels of user behavior are shown in the following table.

You can calculate a rough throughput guideline in the following way:

Number of users\*percentage of users who are active/request rate

For example, for 1,000 users, the following values result:

Simultaneous users = 1,000 \* 10% = 100

The following table describes the response to four levels of load.

|  |  |
| --- | --- |
| Load | Requests per hour |
| Light | 20 requests per hour. An active user will generate a request every 180 seconds. Each response per second of throughput supports 180 simultaneous users and 1,800 total users. |
| Typical | 36 requests per hour. An active user will generate a request every 100 seconds. Each response per second of throughput supports 100 simultaneous users and 1,000 total users. |
| Heavy | 60 requests per hour. An active user will generate a request every 60 seconds. Each response per second of throughput supports 60 simultaneous users and 600 total users. |
| Peak | 120 requests per hour. An active user will generate a request every 30 seconds. Each response per second of throughput supports 30 simultaneous users and 300 total users. |

If your organization has an existing collaboration solution, you can view the IIS logs to determine the usage patterns and trends in your current environment. For more information about parsing IIS logs, see [Analyzing Log Files (IIS 6.0)](http://go.microsoft.com/fwlink/?LinkId=78825&clcid=0x409)http://go.microsoft.com/fwlink/?LinkId=78825&clcid=0x409.

If your organization is planning a new collaboration solution deployment, use the information in the following section to estimate your usage patterns.

#### Estimate throughput targets

The estimated throughput performance of the server farms presented in the previous section is based on the following assumptions:

 User response rate of <1 second for common operations

 User concurrency rate of 10%

 Indexing operations running within an overnight time window of 12 hours

Use the information in this section to change the value of these assumptions to accommodate your organization’s characteristics. The result might be a different throughput target for your organization.

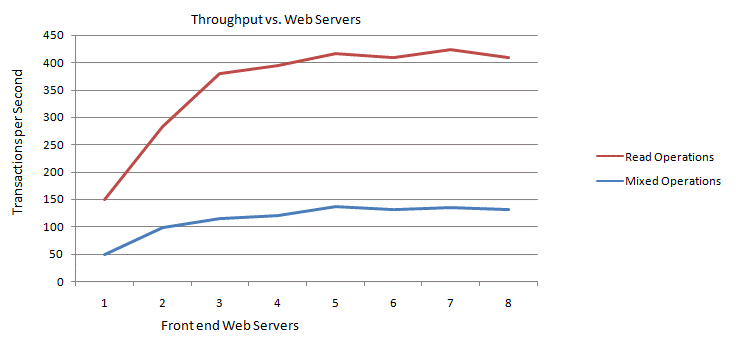
##### Test results: Throughput by farm configuration

The table in this section shows test results for a variety of user operation profiles using the hardware listed in [Test environments](#DSDOC_section20a7b2b45_f633_46d2_a4fd_78) earlier in this article. The number of user connections is a fixed parameter that was used during testing.

The following table shows test results for both read-write mix and read-only user operations.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Farm configuration | RPS |  | Total number of user connections |  |  |  |  |  |  |  |
|  |  |  | Light usage |  | Typical usage |  | Heavy usage |  | Extreme usage |  |
|  | Mix | Read | Mix | Read | Mix | Read | Mix | Read | Mix | Read |
| 1 by 1 | 50 | 100 | 90,000 | 180,000 | 50,000 | 100,000 | 30,000 | 60,000 | 15,000 | 30,000 |
| 2 by 1 | 99 | 185 | 178,200 | 333,000 | 99,000 | 185,000 | 59,400 | 111,000 | 29,700 | 55,500 |
| 3 by 1 | 115 | 265 | 207,000 | 477,000 | 115,000 | 265,000 | 69,000 | 159,000 | 34,500 | 79,500 |
| 4 by 1 | 120 | 275 | 216,000 | 495,000 | 120,000 | 275,000 | 72,000 | 165,000 | 36,000 | 82,500 |
| 5 by 1 | 136 | 280 | 244,800 | 504,000 | 136,000 | 280,000 | 81,600 | 168,000 | 40,800 | 84,000 |
| 6 by 1 | 130 | 280 | 234,000 | 504,000 | 130,000 | 280,000 | 78,000 | 168,000 | 39,000 | 84,000 |
| 7 by 1 | 134 | 290 | 241,200 | 522,000 | 134,000 | 290,000 | 80,400 | 174,000 | 40,200 | 87,000 |
| 8 by 1 | 130 | 280 | 234,000 | 504,000 | 130,000 | 280,000 | 78,000 | 168,000 | 39,000 | 84,000 |

The following graph shows changes in throughput for both read-write and read-only operations when the number of front-end Web servers changes.



##### Estimate user response time

First, determine if your organization can tolerate a slower user response time or if your organization demands a faster user response time. Response times are categorized in the following way:

 Slow (3-5 seconds)   User response times can slow to this rate without causing alarm.

 Recommended (1-2 seconds)   The average user response time target.

 Fast (<1 second)   For organizations whose businesses demand speed.

Based on the user response time that most closely matches your organization’s requirements, determine the throughput target based on the number of users. Because a single-server deployment can capably serve up to 1,000 users, 500 users is the fewest listed.

The following table lists throughput targets based on user response times.

|  |  |  |  |
| --- | --- | --- | --- |
| Total users | Slow (RPS) | Recommended (RPS) | Fast (RPS) |
| 500 | .4 | .5 | .7 |
| 1,000 | .7 | 1.0 | 1.2 |
| 5,000 | 4.0 | 5.0 | 6.0 |
| 10,000 | 9.0 | 10.0 | 12.0 |
| 20,000 | 18.0 | 20.0 | 24.0 |
| 50,000 | 40.0 | 50.0 | 60.0 |
| 100,000 | 90.0 | 100.0 | 120.0 |

After you have identified the throughput target that is appropriate for your organization, re-evaluate the test data for the sample topologies to validate your choice of topology and hardware.

##### Estimate concurrency rate

Next, estimate your organization’s concurrency rate. Concurrency rate is the percentage of users that are using the solution at the same time. Use the concurrency rate that you expect during peak hours. The following table recommends throughput targets based on the total number of users and the concurrency rate.

The following table lists throughput targets in RPS at various concurrency rates.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Total users | 5% concurrency rate | 10% | 15% | 25% | 50% | 75% | 100% |
| 500 | .25 | .5 | .75 | 1.25 | 2.5 | 3.75 | 5.0 |
| 1000 | .5 | 1.0 | 1.5 | 2.5 | 5.0 | 7.5 | 10.0 |
| 5,000 | 2.5 | 5.0 | 7.5 | 12.5 | 25.0 | 37.5 | 50.0 |
| 10,000 | 5.0 | 10.0 | 15.0 | 25.0 | 50.0 | 75.0 | 100.0 |
| 20,000 | 10.0 | 20.0 | 30.0 | 50.0 | 100.0 | 150.0 | 200.0 |
| 50,000 | 25.0 | 50.0 | 75.0 | 125.0 | 250.0 | 375.0 | 500.0 |
| 100,000 | 50.0 | 100.0 | 150.0 | 250.0 | 500.0 | 750.0 | 1,000.0 |

After you have identified the throughput target that is appropriate for you organization based on your expected concurrency rate, re-evaluate the test data for the sample topologies to validate your choice of topology and hardware.

##### Estimate indexing window

Finally, verify that indexing jobs can be contained within an overnight window of 12 hours. In a Windows SharePoint Services 3.0 collaboration environment, indexing jobs typically represent the longest-running operation that is not initiated by users. You will need to perform testing in your own environment to determine the duration of indexing jobs, and whether the throughput consumed by indexing jobs interferes with your target user response times.

### Estimating disk space requirements

This section provides tables that can help you estimate disk space requirements for the collaboration scenario. Disk space requirements for your hardware will vary greatly by server role and scenario, and are dependent upon data to be stored in the content database, caching requirements, and external content crawled by search. Where possible in the following discussion, numbers are filled into the formulas based on disk space requirements that can be predicted (such as the size of installation files).

First, estimate your disk space requirements by server role. Then, based on your planned topology, add up the requirements where server roles will share the same physical server computer. Finally, ensure that your hardware is appropriately sized to accommodate your disk space requirements.

Additionally, best practices for SQL Server storage should be applied to database servers. For more information, see [Physical Database Storage Design](http://go.microsoft.com/fwlink/?LinkId=78853&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=78853&clcid=0x409).If more than one database server is implemented, apply the SQL disk space factor separately for each search server.

note_ddNote:

Operating system and program files should stored separately from data files on a separate drive or a Redundant Array of Independent Disks (RAID).

#### Database server disk space requirements

Use the following table to calculate disk space requirements for database servers in your farm. If more than one database server is implemented, calculate this sum separately for each search server.

|  |  |  |
| --- | --- | --- |
| Category | Description | Number |
| Operating system files | Disk space required for Windows Server 2003 Setup and system files. For more information, see [Choosing a File System for the Installation Partition](http://go.microsoft.com/fwlink/?LinkId=78866&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=78866&clcid=0x409). | 4 GB |
| Swap file | The swap file size will be the same as the physical memory size, by default. |  |
| SQL Server installation files | Disk space required for SQL Server Setup and program files. For more information, see SQL Server 2005 Standard Edition System Requirements (http://go.microsoft.com/fwlink/?LinkId=78870&clcid=0x409). | 425 megabytes (MB) |
| Database log files | Disk space for log files will vary based on log settings and the number of databases. For more information, see [Physical Database Storage Design](http://go.microsoft.com/fwlink/?LinkId=78853&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=78853&clcid=0x409). |  |
| Configuration database | The configuration database will not grow past this size. | 1.5 GB |
| Content databases | Estimate the initial volume of content that will be stored in content databases. Consider the following factors:   Multiply the size of initial content by 1.3 for the size of stored content in a SQL database.   If versioning is used for documents, a copy of each version is stored in the database. |  |
| Future growth | Future growth is a key characteristic of the collaboration scenario. You should plan for twice the amount of data that you initially plan to experience. Enter a number that is appropriate for your environment. |  |
| Free space | Leave at least 25% free space for each hard disk or volume. |  |
|  | Total |  |

#### Search server disk space requirements

Use the following table to calculate disk space requirements for search servers in your farm. If more than one Windows SharePoint Services 3.0 search server is implemented, calculate this sum separately for each search server.

|  |  |  |
| --- | --- | --- |
| Category | Description | Number |
| Operating system files | Disk space required for Windows Server 2003 setup and system files. For more information, see [Choosing a File System for the Installation Partition](http://go.microsoft.com/fwlink/?LinkId=78866&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=78866&clcid=0x409). | 4 GB |
| Paging file | The paging file size will be the same as the physical memory size, by default. |  |
| Windows SharePoint Services 3.0 installation files | This number is an approximation based on a full installation. | 1.3 GB |
| The Microsoft .NET Framework version 3.0 |  | 60 MB |
| Content index | Add the amount of content in content databases that will be indexed by the index server. Divide this amount by 2. The resulting number is the estimated size of the content index. |  |
| Free space | Leave at least 25% free space for each hard disk or volume. |  |
|  | Total |  |

#### Web server disk space requirements

Use the following table to calculate disk space requirements for Web servers in your farm.

|  |  |  |
| --- | --- | --- |
| Category | Description | Number |
| Operating system files | Disk space required for Windows Server 2003 setup and system files. For more information, see [Choosing a File System for the Installation Partition](http://go.microsoft.com/fwlink/?LinkId=78866&clcid=0x409) (http://go.microsoft.com/fwlink/?LinkId=78866&clcid=0x409). | 4 GB |
| Swap file | The swap file size will be the same as the physical memory size, by default. |  |
| Windows SharePoint Services 3.0 installation files |  | 1.3 GB |
| The .NET Framework version 3.0 |  | 60 MB |
| Free space | Leave at least 25% free space for each hard disk or volume. |  |
|  | Total |  |

### Performance monitoring

Using performance counters to monitor the health of your system is an important factor in determining when you need to scale your system up or out. Use the information in the following tables to determine what performance counters to monitor, and to which process the performance counters should be applied.

#### Web server

The following table shows performance counters and processes to monitor for Web servers in your farm.

|  |  |  |
| --- | --- | --- |
| Performance counter | Apply to process | Notes |
| % Processor time | Total | Shows the percentage of elapsed time that this thread used the processor to execute instructions. |
| % Memory utilization | Application pool | Shows the average utilization of system memory for the application pool. You need to identify the appropriate application pool to monitor. The basic guideline is to identify peak memory utilization, and assign that number plus 10% to the application pool. |

#### Database server

The following table shows performance counters and processes to monitor for database servers in your farm.

|  |  |  |
| --- | --- | --- |
| Performance counter | Apply to process | Notes |
| % Processor time | Total | Shows the percentage of elapsed time that this thread used the processor to execute instructions. |
| % Memory utilization | Total | Shows the average utilization of system memory. |

# Portal collaboration environments

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

This content is preliminary content. It might be incomplete and is subject to change.

# Excel Services environments

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Document repository environments

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Internet environments

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# ISP hosting environments

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Corporate hosting environments

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Additional performance and capacity planning factors (Office SharePoint Server)

This section describes additional factors which you should consider when planning your deployment.

[MOSS feature areas](#DSDOC_MOSS_features9f3cfe3f_01b5_406e_86)

[Client integration](#DSDOC_Client9f3cfe3f_01b5_406e_8615_0473)

[Shipped features](#DSDOC_Shipped9f3cfe3f_01b5_406e_8615_047)

[Environmental factors](#DSDOC_Environment9f3cfe3f_01b5_406e_8615)

## MOSS feature areas

The subsections below describe additional performance and capacity factors for feature areas within Microsoft Office SharePoint Server 2007, including test data specific to each feature area.

[Search](#DSDOC_Search9f3cfe3f_01b5_406e_8615_0473)

[Excel Calculation Services](#DSDOC_Excel9f3cfe3f_01b5_406e_8615_04735)

[InfoPath Forms Services](#DSDOC_IPFS9f3cfe3f_01b5_406e_8615_04735a)

### Search

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

### Excel Calculation Services

See the article [Excel Services environments](#DSDOC_f0ff6cc9_2f84_4d73_8ac2_390bbcb08c) for more information on capacity and performance planning factors.

### IPFS

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

## Client integration

This section provides information about how 2007 Microsoft Office system client applications may impact the performance and capacity requirements of Office SharePoint Server 2007.

[Outlook client integration](#DSDOC_Outlook9f3cfe3f_01b5_406e_8615_047)

InfoPath client integration#InfoPath

### Outlook

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

### InfoPath client integration

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

## Shipped features

[Caching](#DSDOC_Caching9f3cfe3f_01b5_406e_8615_047)

[Content Query Web part](#DSDOC_Content_query9f3cfe3f_01b5_406e_86)

### Caching

Microsoft Office SharePoint Server ships with advanced caching capabilities to maximize the performance of the Web sites.

[Object caching](#DSDOC_Object_caching9f3cfe3f_01b5_406e_8)

[Disk-based caching for Binary Large Objects (BLOBs)](#DSDOC_BLOB_caching9f3cfe3f_01b5_406e_861)

The table below shows the available types of caching and where they are implemented.

|  |  |  |
| --- | --- | --- |
| Use this type of caching… | At the… | Notes |
| Output caching and cache profiles | Individual page level | Ideal for heavily accessed Web sites that do not need to present new content frequently. |
| Object caching | Individual Web Part control, field control, and content level | Includes cross-list query caching and navigation caching |
| Disk-based caching for Binary Large Objects (BLOBs) | Individual BLOB level and caches images, sound, movies, and code | Supports .gif, .jpg, .js, .css, and other image, sound, and code files that are stored as binary large objects |

#### Output Caching

Office SharePoint Server 2007 uses output caching technology native to ASP.NET 2.0 to manage when and how page content is served. When output caching is used properly, it can improve the throughput and user response time significantly.

If a site is enabled with ASP.NET, the HTML markup generated at run-time by each Web page is cached by ASP.NET output cache based on the specified cache profile. On a heavily accessed Web site, caching frequently accessed pages for even a minute at a time can result in substantial throughput gains. While a page is cached by the output cache, subsequent requests for that page by the users with similar permissions are served from the output cache without executing the code or control that created it for the specified duration of the cache.

For more information about enabling output caching, see the article at <http://msdn2.microsoft.com/en-us/library/aa661294.aspx>.

##### Output Caching Considerations

Before choosing to use output caching to improve the performance of page and page-item rendering, consider benefits and drawbacks of a potential output caching implementation.

Output caching is ideal for Web sites that do not require content update every minute. In this environment, the cached output can be shown to the different users without accessing the backend database, or executing the code/controls that created the HTML markup of the Web page initially.

Output caching can be used for anonymous and authenticated users, but it is most effective when the access is anonymous. Therefore, enable anonymous user access whenever it is appropriate and feasible for the entire or a part of the Web site.

However, before deciding to implement output caching, you may want to consider the following limitations:

 Output caching consumes additional memory to cache the HTML markup for each cached page. Be sure to install sufficient amount of physical memory to avoid system paging or other memory issues.

 When used with two or more front-end Web servers, output caching may affect consistency. You can configure a cache profile not to check for updates for each request and, for example, instruct it to ignore changes to the version of the Web page in the output cache until 60 seconds after the original page is updated. If you have two front-end Web servers in your topology, and depending on the load balancer used to route the user's request, a reader of site content could see inconsistency if the page is rendered by one server and then a subsequent request is routed to a second server within that 60-second window. If checking for changes is enabled in the caching profile, it will reduce the effectiveness of the output caching.

 If output caching is enabled for users with write permission in any items in the site collection, these users may not see the most up-to-date data on the Web pages until the output cached pages have expired. Usually, this does not affect the content directly on a Web page that the user is currently changing or viewing, but it may affects roll-up data from a list or a library, such as the data presented from a document library Web part. Therefore, you should only enable output caching for readers only if you have concerns about providing the up-to-date information for users with write permissions.

Output caching behavior

The behavior of Output caching can be specified at 3 levels:

 Site collection

 Site

 Page layout

A system administrator can apply different caching profiles to each level to optimize the caching behavior. For example, the home page of your site may be accessed most often, and one may use a unique page layout for the home page so that you can apply a special cache profile to that unique page layout and override the caching behavior of the entire site collection. The cache profile of the page layout may be configured with a longer cache duration. This allows you to trade off timeliness of data against performance only for the home page where you can afford this trade-off. For the other pages in the system, you can use a different cache profile with a shorter cached duration.

Search result caching

In an environment employing user authentication, you should never cache search results. Doing so can permit disclosure of privileged information to the wrong users. Normally, search query filters its result set to show only information available to the current user. By caching the results, the code which filters the result set is bypassed, thus can result in a user seeing results to which they should not have access. In an anonymous environment, this is not an issue because all search results are the result of unauthenticated requests.

If you have output caching enabled on the site collection, you can disable the search result page layout by performing the following procedure:

procedure_ddDisable search results page layout

|  |
| --- |
| 1. On the Site collection output cache settings page, check the Page Layouts can use a different page output cache profile checkbox.  2. On the Master page gallery page, in the SearchResult.aspx page layout section, disable the Authenticated Cache Profile property.  3. Check in and approve the page layout item to take effect for all users.  Search results using that particular page layout will no longer be cached. |

In addition, one can disable the entire search center sub-site to disable output cache if you have other pages in that sub-site that are sensitive with the same potential security issue. To disable the output cache for the search center sub-site, follow these steps:

procedure_ddDisable output cache for Search Center

|  |
| --- |
| 1. On the Site collection output cache settings page, check the Publishing sites can use a different page output cache profile checkbox.  2. On the Site settings page for the Search Center sub-site, In the Site administration section, click Site output cache.  3. On the Publishing site output cache settings page, change the inheritance property to the setting that disables the authenticated cache profile. |

ASP.NET private byte limit

If output caching is enabled, you may want to extend the default ASP.NET 2.0 limit on private bytes. This limit instructs ASP.NET when flushing of its output cache should occur. Premature flushing will cause unnecessary performance degradation. See this article for details: <http://msdn2.microsoft.com/en-us/library/ms228248.aspx>

Cached page versions

Certain Web pages may show slightly different versions based on the users or other business logic. Output caching can be extended via the supported programmable API to accommodate the need to cache the items differently. See the article <http://msdn2.microsoft.com/en-us/library/ms550239.aspx> for more information.

##### Output caching and the Content Query Web part RSS feeds

The Content Query Web part offers the option of providing RSS feeds of the results that it displays. This RSS feed is generated by an .aspx page on the server, which produces the RSS feed XML based on the same results that the Content Query Web part displays.

Because RSS clients often request an RSS feed from the server on a periodic basis, such as every 30 minutes, it is important that the RSS feed generation is performant. As such, the RSS feed .aspx page implements output caching. In the source of the .aspx file, you will see the following line:

<%@ OutputCache Duration="300" VaryByParam="xsl;web;page;wp" VaryByCustom="rights;feedresults"%>

This means that, out of the box, Content Query RSS feeds will be cached for 5 minutes, will cache unique versions of the RSS feeds for each different Content Query Web part, and will cache unique versions of the RSS feeds for users with different rights and different feed results.

If you wish to customize this output caching, you can create your own feed .aspx page that implements the same logic, but has different output cache settings. Then, Content Query Web parts can reference your custom feed .aspx page instead of the out-of-box page.

#### Object Caching

Office SharePoint Server 2007 supports caching of certain page items, such as navigation data and data accessed through cross-list queries. Caching page items reduces the need to retrieve field data from the database each time a page is rendered. The caching system also caches complete field data for a page, excluding data for any Web Part controls on the page.

##### Object Cache Tuning

The size of the object caching is set at 100MB per site collection by default, but this setting can be modified for each site collection to fit the characteristics of the Web site. There is a set of performance counters you can use to tune the size of the object cache. The name of the performance counter object is SharePoint Publishing Cache Object. Based on the Cache Hit Ratio and the change in Object Discard counters, you can set the object cache size accordingly. Consider the following items when you are setting this limit:

 Start with a low value (such as 200MB) and monitor the cache hit ratio and object discard counter. Hit ratio over 90% and a low object discard rate are generally good sign that you current size is big enough. However, you should also measure user response time for key operations to adjust this setting.

 If you set the size too big, you may waste valuable memory for the other caches, such as the ASP.NET output cache if used. Certain Web parts, such as the Content By Query Web part, stores their XSLT stylesheet in output cache. If the object cache size is set too big, ASP.NET may flush output cache memory to make room for it. CPU usage may increase after the flushing. This is particular important for system running on 32-bits OS because each worker process is limited to 2GB application memory space. If you set the object cache size limit too big, the IIS worker process (w3wp) may actually run out of memory.

##### Cross-List Query Caching

The object cache is also used to cache items that are retrieved as part of cross-list queries. These queries aggregate items from various lists and sites in your site collection. The most common usage of these queries is in the Content Query Web part. Each use of the cross-list query requires a SQL round trip. By using the object cache, you can greatly reduce the number of round trips required to serve up cross-list queries, thereby improving the performance of features like the Content Query Web part that present cross-list query results.

Checking for updates

There are two ways that the cross-list query cache will check for updates, and conditionally refresh the cache:

 By checking for changes made in the site collection. If no changes were made, the cached results are used.

 By waiting for a period of time, during which the cached results will be used, and after which a query will be issued to refresh the cache.

The first setting is useful in cases where there are frequent changes to content in the site collection that the cross-list query displays, and where it is important that the query displays the latest information. An example of this case is a divisional intranet portal site, which is displaying a cross-list query of the latest documents in the site. In this site, many users are contributors, and it may be important to see the latest documents that users have published.

The second setting is useful in cases where there are not frequent changes to the content in the site collection, and where it is less important that the cross-list query displays up-to-date information. An example of this case is a public Internet site, which is displaying a cross-list query of the latest article pages that have been published in the site. In this site, most users are anonymous users, or are authenticated users with read-only rights. In this case, a few minutes delay of the latest articles is not critical.

procedure_ddConfigure the cross-list query cache

|  |
| --- |
| 1. From the home page of your site, click on the Site Actions menu.  2. From the Site Settings drop-down menu, select Modify all site settings.  3. On the Site settings page, in the Site collection administration section, click Site collection object cache.  4. In the Cross list query cache changes section, select the appropriate radio button, depending on how you want the cross-list query cache to update. If you select the second radio button, you will also need to enter a value in the text box, representing the number of seconds the cache will wait before refreshing.  5. Click OK to save your changes. |

Number of items to retrieve

The cross-list query results multiplier setting controls the number of items that are retrieved and cached. Because cross-list queries can retrieve items for a variety of users with different permissions, it is important to retrieve enough items from the query so that all users see the correct items. To ensure that all users see the correct items in the query results after security trimming, the cross-list query cache must pull more results than originally requested. This setting requires an integer that reflects the multiple of the number of items that the cross-list query cache should retrieve.

 Setting the multiplier to a larger number will retrieve more items, and will consume more memory. A larger number is appropriate in a Web site where many users have unique permissions on different lists and items.

 Setting the multiplier to a smaller number will retrieve fewer items, and will consume less memory. A smaller number is appropriate in a Web site where users have the same security, such as anonymous users on an Internet site.

procedure_ddConfigure the cross-list query results multiplier

|  |
| --- |
| 1. From the home page of your site, click on the Site Actions menu.  2. From the Site Settings drop-down menu, select Modify all site settings.  3. On the Site settings page, in the Site collection administration section, click Site collection object cache.  4. In the Cross-list query results multiplier box, enter a number that represents the multiple of items the cross-list query will retrieve.  5. Click OK to save your changes. |

#### Disk-based Caching for Binary Large Objects (BLOBs)

Disk-based caching controls caching for binary large objects (BLOBs) such as image, sound, and video files, as well as code fragments. Disk-based caching reduces the need for database round trips for accessing the BLOBs. BLOBs are retrieved from the database once and stored on the WFEs. Further requests are served from the disk-based cache and trimmed based on security.

##### Considerations

 The size of the disk-based cache can be configured for each Web application. The minimum is 1 GB, and you may increase the size in multiples of gigabytes. Make sure that you have enough disk space for your application.

 There are a number of settings you can set on the disk-based cache. Two settings are of particular note:

 Max-age specifies the maximum amount of time in seconds that the client browser caches BLOBs downloaded to the client computer. If the downloaded items have not expired since the last download, the same items are NOT re-requested until the cache expires. The max-age attribute is set by default to 86400 seconds (that is, 24 hours), but it can be set to a time period of 0 or greater. The longer you set this value, the longer it takes for the browser to get the updated items.

 Path specifies in the form of a regular expression which files are cached based on the file extension. By default, the file extension includes: gif, jpg, png, css, and js. If you have special ones that your Web pages may referenced, you must store them in the cache.

 Disk-based caching only applies to items in a document library. If you store resources outside of a document library, such as a folder underneath a site, the items are not managed by the disk-based cache even if you enable it for the entire Web application. This is important if you want to control the max-age setting of the blob resources downloaded to the client browser. By default, the max-age of all items stored in Office SharePoint Server is set to zero.

### Content Query Web part

The Content Query Web part utilizes the Windows SharePoint Services cross-list querying mechanism to retrieve content from a SharePoint site collection.  If the Web part is configured to issue a query that involves a large number of lists, the cross-list query mechanism may raise an exception.

By default, cross-list queries have a list limit of 1,000.  This means that if you configure the Content Query Web part with a query that includes more than 1,000 lists, the cross-list query will not complete, and the Web part will not show any content.  The reason for this throttling is to avoid overburdening SQL Server 2005.  The more lists the cross-list query includes, the longer it takes for the database server to return the content the query is asking for.  For very large numbers of lists, this could cause the database server to disproportionately process cross-list queries at the expense of other requests.

If your requirements involve querying for more than 1,000 lists, you can increase the list limit if the database load that the operations require is acceptable.  You can do this by adding a MaxListLimit attribute to the ListsOverride property of the Web part.  For example, if you wanted to raise the list limit to 2000, you would set the ListsOverride property as:

 <Lists ServerTemplate="850" MaxListLimit="2000">

## Environmental factors

[Network considerations](#DSDOC_Network_config9f3cfe3f_01b5_406e_8)

[Network security](#DSDOC_Network_security9f3cfe3f_01b5_406e)

[Authentication](#DSDOC_AuthN9f3cfe3f_01b5_406e_8615_04735)

[Developing custom code](#DSDOC_Code9f3cfe3f_01b5_406e_8615_04735a)

### Network configuration

Network configuration is critical to the performance of your Office SharePoint Server or Windows SharePoint Services installation. Common network components which can affect your performance include:

 Network Interface Card (NIC)

 NIC settings: Where possible, you should always use Gigabit network cards. If you have self-switching cards (100 MB / 1 GB), you should always set the over-ride to use 1 Gigabit.

 Inbound/Outbound: For scenarios where you expect high traffic, we recommend you have separate NICs to handle inbound and outbound traffic.

 Switches: If you run your network through a switch, ensure that you are using a GB switch and that you have the same number of inbound/outbound channels.

 Routers: Ensure your routers are configured on a GB infrastructure.

 Domain controllers: It is possible for authentication to become a performance bottleneck in your SharePoint environment if the domain controller (DC) receives requests more quickly than it can respond. For environments using user authentication such as NTLM, we recommend a ratio of 3 WFEs per DC. If your tests indicate that the authentication load at 3 WFEs per DC is acceptable, you can add one more WFE per DC for a supported limit of 4 WFEs per DC.

Keep in mind that network configuration should be planned and tested thoroughly prior to moving a system to a production environment.

### Network security

See [Plan for secure communication within a server farm [Office SharePoint Server]](#DSDOC_a29ecba7_813e_4815_bdc7_ca1e3517e4) for more information on network security.

### Authentication

The authentication mechanism used in your environment has an incremental effect on the overall performance of the system. Factors which contribute to authentication performance include:

 The number and speed of round trips to the authentication provider

 Authentication provider processing performance

Microsoft tests indicate that the order of authentication mechanisms, from fastest to slowest, are as follows:

1. Anonymous

2. Kerberos

3. NTLM

4. Basic

5. Forms

If you choose to write an authentication provider to use with Office SharePoint Server or Windows SharePoint Services, you should follow the best practices guidelines at <http://msdn.microsoft.com/library/en-us/dnbda/html/authaspdotnet.asp>.

### Developing custom code

The most common cause of poor performance in earlier releases of SharePoint Server is the development and deployment of inefficient custom features on top of the SharePoint platform. When developing customer features for SharePoint, there are a number of performance metrics you should monitor. These include, but are not limited to:

 SQL Server round trips. For core pages, we recommend no more than 2-3 SQL round trips. Excessive round trips have the following deleterious effect on performance:

 Increased end user response time due to greater server-side processing time

 Reduced overall system throughput due to additional load on the SQL server.

 SQL server CPU utilization. In order for your MOSS system to remain healthy, it is important that CPU utilization on the SQL server(s) remains relatively low. If SQL server CPU usage averages more than 60%, performance will be adversely affected. Steps you can take to reduce SQL CPU utilization include:

 Implement a caching strategy – this reduces the overall number of calls from the WFE(s) to SQL Server.

 Optimize custom code to use object methods which return your desired data in the most efficient manner (e.g. introduce indexes on lists, etc.)

 Distribute your SQL databases across multiple physical SQL servers

 Page download size. Keep code size to a minimum. A relatively small increase in page size can have a significant impact on performance if that page is accessed by a large number of people every day, especially during peak hours.

 Client-side code efficiency. Approximately 50% of end user response time is comprised of client side processing of returned code. If your custom solution increases any of these, you can expect an adverse effect on end user response time.

 AJAX callbacks. For AJAX parts, the number of callbacks, and the payload for each callback. For example, each KPI makes 3 calls in order to return the result. Make sure you test page performance when you introduce multiple KPIs or other custom code into a page.

# Tools for performance and capacity planning [Office SharePoint Server]

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

This article contains information about test tools available for Microsoft Office SharePoint Server 2007.

In this article:

 [About the SharePoint test data load tool](#DSDOC_section1301ed832_95da_4251_b266_7b)

 [Constructing a SharePoint test data load configuration file](#DSDOC_section2301ed832_95da_4251_b266_7b)

 [Deleting SharePoint test data](#DSDOC_section3301ed832_95da_4251_b266_7b)

## About the SharePoint test data load tool

The SharePoint test data load tool (WSSDW.exe) is a performance testing tool that populates data for testing deployments of Office SharePoint Server 2007. The SharePoint test data load tool is available as a command-line executable program that accepts an XML configuration file that specifies the objects to be populated. The SharePoint test data load application calls a Microsoft .NET assembly (WSSDWLib.dll). WSSDWLib.dll can also be called from other applications.

When you run the SharePoint test data load tool, the tool extracts information about how to populate the server from an XML configuration file. This file must be specified in the command as shown in the following examples.

 Populate a server   To populate a server with data, run the following command where myfile.xml is the name of your configuration file, as shown in the following example:

wssdw.exe myfile.xml

 Delete SharePoint test data   To delete data created by the SharePoint test data load tool, run the same command that you used to load test data, but add a –d command-line switch before the name of your configuration file, as shown in the following example:

wssdw.exe –d myfile.xml

 Specify a URL   If you are running the SharePoint test data load tool on a server that has multiple virtual servers, specify the absolute URL to the site as a second argument, where myserver is the name of the specified server, as shown in the following example:

wssdw.exe myfile.xml http://myserver

 Specify a path to plug-in assemblies   If your plug-in assemblies are not located in the same directory as the SharePoint test data load tool, load the assemblies by specifying a path to them, as shown in the following example:

wssdw.exe myfile.xml –p <path to directory>

 View supported tags   To view a list of tags that are supported by the SharePoint test data load tool, run the SharePoint test data load tool command and add the –h command-line switch, as shown in the following example:

wssdw.exe –h

 Improve SharePoint test data load tool performance   To improve performance while loading assemblies, the SharePoint test data load tool maintains a list of known plug-in assemblies. When you run the SharePoint test data load tool, the tool looks for and loads these known plug-in assemblies. If your plug-in assembly is not on the list, you can direct the SharePoint test data load tool to load your assembly by using one of the following procedures.

 Run the following command to direct the SharePoint test data load tool to ignore the list of known plug-in assemblies and load all available assemblies, where myfile.xml is the name of your configuration file, as shown in the following example:

wssdw.exe myfile.xml –loadall

 Include the following file in the same directory from which you are running the SharePoint test data load tool. Populate this file with a list of all the new plug-in assemblies you want to load, separated by newline characters, as shown in the following example:

dwlib\_knowndllstoload.txt

## Constructing a SharePoint test data load configuration file

Before you can use the SharePoint test data load tool, you must construct an XML configuration file. The SharePoint test data load tool will use this file to create objects on the SharePoint server that you are testing. The configuration file should be placed in the same folder as the SharePoint test data load tool. The basic format is shown in the following example.

<WSSDWLib>

<Object parameter="value" …>

</WSSDWLib>

In the following example, the XML configuration file creates 10 Webs in Windows SharePoint Services 3.0 (subweb1 through subweb10). Each Web has 50 list items added to the list named "Announcements."

<WSSDWLib>

<Webs num="10" name="subweb" >

</WSSDWLib>

A list of the objects that are supported by the SharePoint test data load tool — along with known parameters, usage, and legal placement within the XML structure — is provided in the SharePoint Test Data Load Tool Software Development Kit (SDK) (WSSDW.chm).

## Deleting SharePoint test data

The SharePoint test data load tool supports deletion of content by using the same XML configuration file that was used to create the content. To perform this deletion, run the SharePoint test data load tool command and add the –d command-line switch to the command, as shown in the following example:

wssdw.exe –d myfile.xml

The SharePoint test data load tool deletes XML objects recursively, deleting the XML children before it deletes the XML parent. If you want to override this behavior for a given XML node, add the following attribute to the node in the configuration file:

quickdelete="true"

Adding this attribute deletes the entire node without deleting the child nodes independently.

note_ddNote:

Using the quickdelete attribute speeds up the deletion process, but it might not remove all data from the content database.

# XVIII Plan for and design database storage and management

In this chapter:

 [TBD Chapter overview: Plan for and design database storage and management](#DSDOC_ebbd99e2_98e8_478f_87f3_12f195741b)

 Gather content requirements

 Develop database design

 Plan for scaling out content databases

 [Plan for backup and restore [Office SharePoint Server]](#DSDOC_054c3d6d_a0d3_448a_864b_93db6283d7)

 Plan for database hardware and software requirements

 Plan SQL Server configuration settings

 Plan DNS names and IP addresses

# TBD Chapter overview: Plan for and design database storage and management

note_ddNote:

This topic is a placeholder for future content. It is included in this preliminary documentation to illustrate the proposed structure of the final content.

# Plan for backup and restore [Office SharePoint Server]

note_ddNote:

This content is preliminary content. It might be incomplete and is subject to change.

In this article:

 [Plan for tools](#DSDOC_section1054c3d6d_a0d3_448a_864b_93)

 [Backup Strategies](#DSDOC_section2054c3d6d_a0d3_448a_864b_93)

 [Plan for backup types and schedules](#DSDOC_section3054c3d6d_a0d3_448a_864b_93)

Backups are a necessity in today's workplace as protection for any unforeseen event or circumstances that may warrant a database restore or complete disaster recovery. Developing plans and procedures for recovering from failures before they occur is critical in minimizing lost productivity in the event of a server crash, database corruption, or any other form of data loss. An effective disaster recovery plan should reflect a thorough data protection strategy based on your specific data protection requirements.

After reading this article, you will be able to define the backup strategy that is best for your environment.

## Plan for tools

This section provides an overview of the tools that can be used for backups and content retrieval at various levels of granularity:

 SQL Server Backup and Restore

 SharePoint Products and Technologies Backup and Restore Utility

 stsadm Utility

 Recycle Bin

### SharePoint Products and Technologies Backup and Restore Utility

Microsoft Office SharePoint Server 2007 includes a backup and restore tool. This tool is available from the Central Administration site or by using the STSADM command-line tool. This tool is the preferred method of backing up and restoring SharePoint solutions and can be used in a variety of ways:

 Run backup or restore jobs directly from Central Administration.

 Manage backup and restore jobs remotely.

 Schedule backup jobs using a batch script.

This tool provides the most comprehensive support for restoring Office SharePoint Server 2007 solutions:

 Restores all SharePoint web applications, content databases, and SSP databases.

 Automatically attaches databases when restoring.

 Restores the search index (or indexes).

For more information on using this tool, see Office SharePoint Server 2007 Backup and Restore.

### SQL Server Backup and Restore

SQL Server Backup and Restore is typically used by large organizations with SQL Server Tools already implemented, and by those with off-site datacenters. The person responsible for the databases, regardless of the application, is a Database Administrator (DBA), rather than the SharePoint Central Administrator.

Using SQL Server to backup your databases affords the following benefits:

 Ability to schedule backup tasks, automating the task.

 Provides backup (and restore) logs for the DBA to review the success or failure of a job.

### stsadm Utility

This utility can back up My Sites and divisional site collections in a single server farm configuration. By using this utility to back up My Sites and site collections, you can restore site collections without having to overwrite all the portal databases. You can back up an entire divisional site collection and all of the sites and content beneath it, but not an individual subsite. However, you can restore content and subsites within a site collection by restoring the site collection to a different site and manually copying the lost data to the original location. The backup file includes the following:

 Subsites

 Pages in the sites

 Files in document libraries or lists

 Security and permission settings

 Feature settings

Note Using an stsadm.exe backup script affects performance on the server farm, because the backup process takes up both memory and processing power. If you choose to schedule stsadm.exe backups in a script, be sure to run the script when server farm usage is light.

### Recycle Bin

The Recycle Bin functionality is similar to that of the Windows Recycle Bin. New to this version, the Recycle Bin provides two stages of file retrieval. The first stage is when an item is deleted, it is removed from its list and placed into the Recycle Bin. On the Recycle Bin page, you have the option to restore or permanently delete any item. Restoring a document will simply move the item from the Recycle Bin back into its original list, making sure that the file name doesn’t conflict with existing files. In addition to the basic Recycle Bin functionality, the site collection administrator has the option to automatically permanently delete items that have been deleted for a specified amount of time.

The second stage Recycle Bin stores items that end users have deleted from their Recycle Bin for easier restoration when needed. This second stage adds to space requirements, which can be enlarged by a specific percentage. When you enable the second-stage recycle bin for a Web application, you must designate how much disk space is available to the second stage recycle bin as a percentage of the quota allotted to the site. For example, if you have allotted 100 MB of space for the site, allotting a 50% quota for the second-stage recycle bin allots 50 MB for the second-stage recycle bin and 150 MB for the site as a whole. You may allot up to 100% for the second-stage recycle bin quota.

## Backup Strategies

There are several data stores in a SharePoint farm, and you may not have a need to back up every store as regularly, depending on the SLA you have outlined with stakeholders. This section provides an overview of recommended backup methodologies and the estimated amount of disk space required to support backup operations for each of the following areas:

 SharePoint databases

 Search Indexes

 Web Front End (WFE) servers

 Windows SharePoint Services sites

 Personal sites

### SharePoint Server Database Backups

The Office SharePoint Server databases and the Windows SharePoint Services databases are backed up by using the native Windows SharePoint Services Backup and Restore Utility. The utility backs up SQL Server databases for each portal. It creates an XML-based manifest file that lists all of the individual backup files for Office SharePoint Server 2007 and Windows SharePoint Services databases. The size of the Office SharePoint Server databases depends on your business requirements and usage.

### Search Index Backups

This version allows for the Search indexes to be backed up.

### Web Front End (WFE) Server Backups

Web front end server data includes custom assemblies, configuration files, add-in software, custom templates, the IIS metabase, and the Inetpub directory. The size of a WFE server backup depends how much customization is done on the WFEs. An estimate based on a medium server farm consisting of two WFE servers is approximately 50 MB for each server. You can estimate the maximum amount of hard disk space required for front-end Web server backups by using the following formula:

The number of WFE servers × 50 MB = estimated disk space required

For example, if you have 2 WFE servers at 50 MB, each, you need 100 MB of disk space to back up the WFE servers. You must also plan adequate space for backing up the IIS log files. You can estimate the space required by using the following formula:

The number of days of logging × daily log file size = estimated disk space required

For example, if you want to preserve 30 days of logs with an average daily log file size of 1 GB, you need 30 GB.

### My Sites Backups

By default, My Sites content is contained in the site database of the corporate portal. The database for the portal is backed up on a regular basis and the individual My Sites are backed up in a separate process using the Office SharePoint Server stsadm.exe command line utility. This process backs up the same data twice, but it allows for backing up and restoring individual My Sites as opposed to restoring the entire site database. The amount of disk space to back up My Sites depends on the following factors:

 The number of My Sites

 The amount of content in each My Site

 The amount of time that My Site backups are kept on disk before they are moved to a tape drive

You can estimate the maximum amount of disk space required for backing up the individual My Sites by using the following calculation:

The number of My Sites × disk quota= maximum disk space required

For example, if you have 2000 users, each with a My Site and 100 MB storage limit set on each My Site, the maximum amount of disk space required for the My Site backup is approximately 200 GB. This also means that the divisional portal site database, which also contains the My Site data, is equally impacted by the extra 200 GB of data. Keep in mind that most My Sites will not use disk space in amounts approaching the quota. Therefore, the average disk space required for My Sites will be much lower than the quota. Set the quota high enough to accommodate the occasional large My Site. Setting the quota too low could result in support calls from users needing more space.

### Windows SharePoint Services Site Backups

The Windows SharePoint Services site collection databases are backed up by the Office SharePoint Server Backup and Restore Utility in the same manner as the Office SharePoint Server databases. In addition, there are alternate prescribed methods for backing up and restoring site collections and My Site data at a more granular level. This means that the backup of some data is duplicated, and this increases the required hard disk space. The site collections are also backed up individually by using the stsadm.exe command line utility, so that individual site collections can be recovered without restoring the entire site collection database.

The amount of disk space required to back up each site collection depends on the amount of content within the site collection and how long the backups are kept on the disk before being moved to a tape drive. You can estimate the maximum amount of hard disk space required for site collection backups by using the following formula:

The number of site collections × disk quota = maximum disk space required

For example, if you have 10 site collections with the quotas set for 100 MB, you need 1000 MB of disk space for backing up site collections. This also means that the Windows SharePoint Services databases containing the site collections are impacted by 1000 MB.

## Plan for backup types and schedules

When developing your backup strategy, you must understand the supported backup types, and carefully plan when you will schedule the backup task. This section defines the types of backups you should perform, and recommends a schedule based on how large your databases are and the amount of time each one will take to be backed up.

### Backup Types

There are two types of backups supported: full and differential.

A full backup backs up the entire database, including all file groups and data files. The benefit of scheduling full backups is high data integrity. However, the process is very time consuming and once started, cannot be paused until the backup process is complete.

A differential backup backs up only data that has been modified or added sine the last backup (either full or differential). The process runs quickly, and requires much less disk space than the full backup. Restores can be time intensive for the

### Recommended Backup Schedules

It is generally recommended to schedule backups during times of low activity usage. You must also take into account how long each part of the backup will take. The following table shows the typical backup size and time needed for the four types of backups required. This section describes the recommended backup types, along with the recommended schedules.

Backup times

|  |  |  |  |
| --- | --- | --- | --- |
| Backup Type | Description | Size | Time |
| Web Front End Server | Custom assemblies, configuration files, add-in software, custom templates, the IIS metabase, and the Inetpub directory. | TBD | TBD |
| SQL Server – differential | Changes to the databases since the last backup (daily) | TBD | TBD |
| SQL Server – full | Complete databases (weekly) | TBD | TBD |
| SharePoint log files | See "TBD" for a list of logs (daily) | TBD | TBD |

### Archiving data for trend analysis

You can back up the data from Web front-end servers for future analysis and long-term off-line reference. The following log files can be backed up from these servers:

 Internet Information Services (IIS) logs C:\Winnt\System32\Logfiles\W3svc1\\*.log

 Usage analysis log C:\Windows\System32\LogFiles\STS\ if usage analysis is enabled

 Other Windows SharePoint Services logs STSAdm.log and OWSTimer.log from the C:\Documents and Settings\ Windows\_SharePoint\_Services\_Administrator\_Account \Local Settings\Temp directory.

# XIX Plan for server management and operations

In this chapter:

 Chapter overview: Plan for server management and operations

 Identify policies for ongoing site maintenance

 Develop monitoring plan for servers and applications

 Develop plan for updating servers and applications

 Plan for ongoing maintenance of servers and applications

# XX Plan for deployment rollout

In this chapter:

 Chapter overview: Plan for deployment rollout

 Plan for upgrade and migration

 Plan for rollout

 Plan the test environment

1. #section7 [↑](#footnote-ref-2)
2. #section5 [↑](#footnote-ref-3)
3. #section3 [↑](#footnote-ref-4)
4. #section6 [↑](#footnote-ref-5)
5. #section4 [↑](#footnote-ref-6)
6. #section7 [↑](#footnote-ref-7)
7. #section3 [↑](#footnote-ref-8)
8. #section2 [↑](#footnote-ref-9)
9. #section6 [↑](#footnote-ref-10)
10. #section3 [↑](#footnote-ref-11)
11. #section4 [↑](#footnote-ref-12)
12. #section3 [↑](#footnote-ref-13)
13. #section4 [↑](#footnote-ref-14)
14. #section6 [↑](#footnote-ref-15)
15. #section1 [↑](#footnote-ref-16)
16. #section4 [↑](#footnote-ref-17)
17. #section5 [↑](#footnote-ref-18)
18. #section7 [↑](#footnote-ref-19)
19. #section3 [↑](#footnote-ref-20)
20. #section3 [↑](#footnote-ref-21)