

Configuring Microsoft SharePoint Hybrid Capabilities



Jeremy Taylor, Neil Hodgkinson, and Manas Biswas

Forewords by Jeff Teper, Corporate Vice President, Microsoft OneDrive and SharePoint
and Seshadri Mani, Principal Program Manager, Microsoft Office 365 OneDrive and SharePoint

PUBLISHED BY
Microsoft Press
A division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Copyright © 2016 by Microsoft Corporation

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

ISBN: 978-1-5093-0243-7

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Support at mspinput@microsoft.com. Please tell us what you think of this book at <http://aka.ms/tellpress>.

This book is provided “as-is” and expresses the author’s views and opinions. The views, opinions and information expressed in this book, including URL and other Internet website references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

Microsoft and the trademarks listed at <http://www.microsoft.com> on the "Trademarks" webpage are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

Acquisitions and Developmental Editor:

Rosemary Caperton

Editorial Production: Dianne Russell, Octal Publishing, Inc.

Copyeditor: Bob Russell, Octal Publishing, Inc.

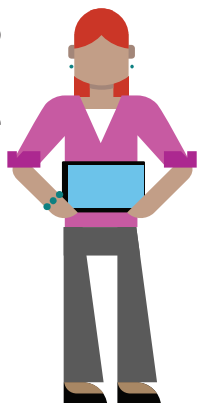
Technical Reviewers: Jeremy Taylor, Neil Hodgkinson, and Manas Biswas; Technical Review services provided by Content Master, a member of CM Group, Ltd.

Cover: Twist Creative • Seattle

Visit us today at

MicrosoftPressStore.com

- **Hundreds of titles available** – Books, eBooks, and online resources from industry experts
- **Free U.S. shipping**
- **eBooks in multiple formats** – Read on your computer, tablet, mobile device, or e-reader
- **Print & eBook Best Value Packs**
- **eBook Deal of the Week** – Save up to 60% on featured titles
- **Newsletter and special offers** – Be the first to hear about new releases, specials, and more
- **Register your book** – Get additional benefits



Dedications

Jeremy Taylor

To my wife, Sylvia, and two daughters, Nasia and Amarissa. Thanks for providing a supportive environment for me to keep focused, which helped me type away at my portions of this book every evening, night, and weekend for two months. I owe you heaps of fun-filled evenings, nights, and weekends now!

Neil Hodgkinson

I would like to dedicate my contribution to this book to my family. To my wife, Julie, whose love and dedication to our family provided me with the evenings and weekends to spend time writing. To our children, Luke, Cerys, and James who inspire me to so many things with their fantastic outlook on life and how they always see the best in everything. Without the support of my family, my work on this book would have been quite the burden; instead, they helped to make it a fabulous adventure.

Manas Biswas

My contribution is dedicated to my family. To my son, Manab, who sacrificed his play time for me, and to my wife, Sabita, who gave up family time, making it possible for me to work on this book. To my mom and dad, who put endless efforts into raising me, giving me the opportunities to pursue my career path, and providing me everything that I could ever ask for. Only with the unlimited love, support, and encouragement of my entire family was I able to fulfil my parts of this book.

Contents

Forewords xvi

By Jeff Teper, corporate vice president,
Microsoft OneDrive and SharePoint.....xvi

By Seshadri Mani, principal program
manager, Office 365 SharePoint,
Microsoft Corporation.....xix

Introduction xxii

Acknowledgments..... xxiv

From us all.....xxiv

Jeremy Taylor.....xxiv

Neil Hodgkinson.....xxv

Manas Biswas.....xxvi

Free ebooks from Microsoft Press xxviii

Errata, updates, & book support xxviii

We want to hear from you xxix

Stay in touch.....xxx

Chapter 1: Introduction and prerequisites 1

Introduction 2

Overview of SharePoint hybrid solutions..... 4

Hybrid search.....	4
Hybrid Business Connectivity Services	5
Hybrid OneDrive for Business	5
Hybrid Sites Features.....	6
Delve	8
Extranet sharing	8
Technology components overview.....	9
Active Directory and Azure Active Directory	9
IdFix directory synchronization error remediation tool.....	10
Azure AD Connect	10
Federation service.....	11
Reverse proxy	11
Certificates	12
SharePoint On-Premises	14
ULS Viewer	17
Microsoft Visual Studio.....	17
Prerequisites for hybrid scenarios.....	17
Modules for hybrid with Windows PowerShell	19
S2S trust.....	21

S2S trust setup—certificate management.....	22
Configuring the ACS trust.....	27

Chapter 2: SharePoint Server hybrid search 31

The importance of search.....	31
Hybrid search overview	33
Infrastructure requirements for classic hybrid search deployments	37
Configuring outbound hybrid search	43
SharePoint on-premises configuration	44
Configuring inbound hybrid search	56
Publishing the SharePoint on-premises web application by using client certificate preauthentication.....	58
Configuring the SharePoint Online Secure Store Target application	62
SharePoint Online search configuration	65
Configuring bidirectional hybrid search	67
Configuring Cloud Search Service Application	69
Configuring the Cloud Search Service Application	75

Creating a Cloud Search Service Application via Central Administration.....	76
Creating a Cloud Search Service Application via Windows PowerShell.....	78
Search Content Service	83
Completing the onboarding process	85
Searching from Office 365 with the Cloud Search Service Application.....	90
Configuring content sources on-premises	91
Configuring outbound query federation on the Cloud Search Service Application ...	92
Managed property for hybrid search results.....	93
Summary	96

Chapter 3: Business Connectivity Services hybrid 98

Overview of Business Connectivity Services hybrid.....	99
BCS hybrid flow.....	102
Prerequisite Steps for Configuring SharePoint BCS hybrid	106
Configuring SharePoint BCS hybrid.....	112
Validation steps for BCS hybrid.....	143

Chapter 4: Additional hybrid solutions..... 146

Overview of additional hybrid capabilities ..	147
OneDrive for Business.....	148
OneDrive for Business hybrid.....	149
OneDrive for Business synchronization client.....	152
Hybrid Sites features	154
Hybrid site following.....	154
Hybrid profiles.....	157
Delve in a hybrid deployment.....	161
Extensible hybrid app launcher	165
Overview of configuring additional hybrid capabilities	169
Configuring by using the Hybrid Picker tool	171
Hybrid Picker prerequisites	171
Running the Hybrid Picker	173
Configuring by using Central Administration	175
Configuration prerequisites via central administration	176
Configuration in Central Administration.....	177

Verification	179
OneDrive for Business verification	179
Hybrid Sites features verification	181
Site following verification	181
Hybrid profiles verification	182

Chapter 5: Microsoft Office 365 hybrid extranet and advanced sharing 184

Introduction	185
External sharing features of SharePoint Online	189
Configuring external sharing	192
Using the Restricted Domains sharing feature for SharePoint Online business-to-business extranet sites and OneDrive for Business	195
Planning for external sharing	198
Managing external users and invitations	201
Partner-facing extranet scenario	204
SharePoint Online B2B collaboration features	206
Example B2B scenario using hybrid extranet features	209
Summary	212

Chapter 6: Troubleshooting Microsoft SharePoint hybrid issues.....	214
Introduction	215
Troubleshooting approach.....	216
Getting the basics right.....	217
Validating directory synchronization	217
Validating the Azure Access Control Services server-to-server trust	224
Certificate validation in isolation	230
Validating the Active Directory Federation Services infrastructure.....	233
Hybrid workload troubleshooting.....	234
Troubleshooting account.....	234
Troubleshooting hybrid search federation.....	237
Troubleshooting query federation by using the SharePoint ULS logs	244
Scenario-based troubleshooting.....	249
Expired STS certificate	249
Search Service Application proxy in partitioned mode	251
Inbound hybrid user rehydration fails	253

Mismatched certificates on inbound configuration	256
Outbound proxy authentication	258
OneDrive and site redirection issues.....	260
Microsoft Support Assistance with Cloud Search Service Application.....	268
Summary	269

Chapter 7: Administering Microsoft SharePoint hybrid by using Windows PowerShell 271

Introduction	272
Getting started with Windows PowerShell and Office 365 administration	275
Installing Azure Active Directory module for Windows PowerShell	275
Connecting to Office 365.....	279
Managing identity in Office 365 and Azure Active Directory	282
Adding a new Active Directory domain to Office 365	282
Managing Office 365 users and groups....	286
Managing SharePoint Online by using Windows PowerShell.....	293

Installing the SharePoint Online Windows PowerShell module	294
Managing hybrid workloads by using Office 365 and SharePoint Online Windows PowerShell	298
Hybrid administration	299
Managing the hybrid workloads by using Windows PowerShell	308
Administering Microsoft OneDrive for Business.....	308
Administering Cloud Search Service Application.....	311
Summary	321
Chapter 8: Microsoft SharePoint hybrid deployment recommended practices.....	322
Introduction	323
Performance management	324
Network and connectivity.....	325
Microsoft OneDrive for Business and OneDrive Sync Client.....	332
Security	335
Certificate planning and ongoing management.....	337
User life cycle management	342

Hybrid identity management tasks.....	343
Synchronization management.....	346
Microsoft Identity Manager 2016.....	348
Search.....	350
Search verticals	350
Cloud Search Service Application.....	353
Auditing and transparency.....	362
Auditing content access	364
Auditing identity management	366
Scalability	367
Scaling identity management	368
Scaling for content	371
Supportability.....	374
OneDrive for Business.....	375
Hybrid Sites and following	375
Hybrid profiles.....	377
Hybrid search.....	378
Summary	380

Chapter 9: Microsoft SharePoint hybrid and cybersecurity..... 382

Overview.....	384

What is cybersecurity?	386
What is a threat.....	387
What is identity theft	387
What is risk management	388
What is data encryption	389
What is compliance	389
Office 365 security.....	390
Defense-in-depth.....	392
SharePoint Online encryption	395
Other encryption tools.....	399
Customer Lockbox.....	403
SharePoint Insights.....	405
Security & Compliance Center.....	406
Government accessing your data	417
Secure Identity Management.....	419
Privileged Access Management	419
Securing Microsoft Identity Manager 2016 and PAM	420
Relevant threats and risks	422
Social engineering	422
Pass-the-Hash attacks.....	424

Man-in-the-middle attacks	425
Address Resolution Protocol poisoning.....	427
Malware	428
LAN viruses	429
Sniffing	430
Cross-Site Scripting.....	430
Wildcard certificate risks	431
Device theft	431
Threat detection tools.....	432
Office 365 Advanced Security Management.....	433
Microsoft Advanced Threat Analytics	434
Risk-mitigation strategy.....	434
Risk remediation	438
Technical solutions	438
Office 365 Solutions.....	445
Personnel solutions	449

SSL security	452
Self-signed certificate security.....	453
Client preauthentication certificate security	454
Additional security reading resources.....	456
About the Authors.....	458

Forewords

By Jeff Teper, corporate vice president, Microsoft OneDrive and SharePoint

In spring of 2016, Microsoft announced the general availability of SharePoint Server 2016, which includes new hybrid capabilities that make it possible for on-premises customers to tap into the innovation the company is delivering in Microsoft Office 365.

For more than a decade, Microsoft's customers have relied on SharePoint to power teamwork, to automate business processes, to create business applications, and to build company-wide intranets. As a core part of Office 365, SharePoint provides content management and collaboration capabilities that are seamlessly integrated with the other applications people use every day to create and coauthor documents, meet and work with their teams, brainstorm, analyze, and make decisions. SharePoint is also integrated with the powerful cross-suite capabilities of Office 365, such as Office 365 Groups, the Office Graph, and

governance controls for security, privacy, and compliance.

Our vision for SharePoint Online in the cloud and SharePoint Server on-premises extends into a connected extensible hybrid experience in which users can take advantage of the powerful features of both SharePoint Server on-premises and the innovation we are delivering in SharePoint Online. Device-independent collaboration and file sharing through Microsoft OneDrive for Business, coupled with intelligent intranets driven by modern team sites, publishing and business applications on your desktop, and mobile device lead the charge in providing new ways to work.

SharePoint Server also delivers cloud-born innovation through hybrid capabilities and experiences that span, integrate, and unify on-premises farms and Office 365. With hybrid search, we have delivered an improved user experience that unifies the index, query results, and search experience across Office 365 and on-premises farms running SharePoint 2016, SharePoint 2013, and even SharePoint 2010. Hybrid search also makes on-premises content available within Office Graph-powered applications such as Delve.

Hybrid OneDrive provides businesses with a stepping stone into the Office 365 experience, paving the way for the gradual migration of personal sites to SharePoint online. With the Hybrid Sites feature, you can connect users to their favorite teamsites, whether on-premises or cloud based. External sharing policies provide granular control of the sharing experience, providing businesses with the ability to securely collaborate with partners. IT professionals can also use hybrid configurations to unify compliance policies and auditing.

With these and other integrated, unified, and hybrid experiences and services, you can take advantage of innovation and capabilities in Office 365 while maintaining workloads on-premises that are not suited to Office 365. You can move workloads to Office 365 at your own pace, based on your own requirements, and still take advantage of Office 365 where it best meets your needs. Additionally, the SharePoint mobile app will support both on-premises and Office 365 sites for hybrid customers.

This ebook draws together the SharePoint Server and Office 365 hybrid workloads and user experiences in one place, providing solid guidance to meet business needs and achieve

productivity goals in the cloud-enabled workplace.

**By Seshadri Mani, principal
program manager, Office 365
SharePoint, Microsoft
Corporation**

Working at Microsoft, I get to see our work empowering millions of users and thousands of enterprises to achieve more, which drives our passion for more innovation. At Microsoft, we strive for a cloud-first/mobile-first vision, and now, today, more and more enterprises and small businesses have begun to realize the benefits of cloud computing to meet their modern productivity needs. We also have strong on-premises server products, as on-premises deployments continue to have their own merits, even in the era of cloud computing. Many customers prefer to keep some of their data on-premises for a variety of reasons, ranging from regulatory controls to richer on-premises customizations.

But, the millennial era demands modern productivity needs from IT, such as access anywhere from any devices. These needs are efficiently satisfied by cloud deployments;

however, as just mentioned, there is an ongoing business need to maintain some parts on-premises. How do we reconcile this? The clear answer is *hybrid*.

As it relates specifically to Microsoft Office 365 SharePoint and OneDrive for Business, we wanted to bring cloud innovations to SharePoint on-premises customers while at the same time lessening the burden on these customers to maintain massive on-premises infrastructure. Hybrid scenarios and experiences is leading us to achieve that goal. Hybrid is about the “best of both worlds—connected”, it is not strictly about migrating all on-premises content to the cloud simply to reap cloud benefits.

Over the past few years, Microsoft has invested heavily in SharePoint hybrid connected experiences. We looked at the core business values and modern productivity needs that confront SharePoint on-premises customers and picked key scenarios to light up in hybrid experience. To name a few, hybrid OneDrive for Business is connecting to OneDrive for Business in the Office 365 cloud from within your SharePoint on-premises, opening massive cloud storage to your end users; Hybrid search experience that spans across your on-premises and online content; and extranet business-to-

business (B2B) sites in the cloud where you can work collaboratively with partners and stop opening your firewall to external users, while still keeping your on-premises team and portal sites. With hybrid extensible app launcher, you can connect your end users to Office 365 video service from within the SharePoint on-premises sites.

This ebook provides a deep dive on various SharePoint hybrid capabilities, how to configure them, and considerations to take into account. There is a perception that hybrid deployments are very complex; this book proves that wrong, especially with the highlight on hybrid scenarios picker which provides a few clicks configuration wizard. I have known Neil and Manas for many years now, and Jeremy just recently: they are all highly passionate about SharePoint hybrid, and hence this book was born. In the ebook, they cover nitty-gritty details to the extent that you will be fully prepared for SharePoint hybrid.

I keep this book as a reference for details on configuring hybrid capabilities. I encourage you, too, to read this book and adapt SharePoint hybrid scenarios and use this book as your reference guide.

Have a nice hybrid Journey! I'm sure it will be fun learning for you.

Introduction

Microsoft SharePoint hybrid consists of a growing list of advanced hybrid solutions that empowers organizations to consume benefits of the cloud and maintain their on-premises investments. This book is the second in a series of SharePoint hybrid books in which we show you how to configure, troubleshoot, and manage a SharePoint hybrid environment.

As you move toward configuring a SharePoint hybrid environment, you will soon realize the need for a go-to manual to ensure a successful implementation. This book does exactly that! It contains step-by-step instructions to help you with configuring and managing SharePoint hybrid. Although, it is aimed primarily for a technical audience, it also addresses business benefits that you might need to present to your management.

This book covers configuring these SharePoint hybrid capabilities in detail, along with scenario-based troubleshooting and recommended practices.

Operating a SharePoint hybrid environment requires experience in both on-premises

SharePoint as well as Microsoft Office 365 products, such as SharePoint Online and Microsoft OneDrive for Business.

With hybrid capabilities such as search, business connectivity services, OneDrive for Business, sites, profiles, and advanced extranet sharing, you will find yourself surrounded by recommended practices and resources that will help you along the way.

One of the most important capabilities—hybrid search—is the glue that binds the on-premises and cloud data together, making it possible for your users to collaborate and access valuable data and information, whether it resides on-premises or in the cloud. You can choose to securely handle and expose line-of-business application data on SharePoint Online by configuring business connectivity services hybrid. Additional hybrid features such as enhanced profiles, sites, and OneDrive for Business, combined with Delve enhance the collaboration experiences in a SharePoint hybrid environment.

It is our aim to get you started to consider cybersecurity in your SharePoint hybrid roadmap. Cybersecurity is a topic of growing concern and we believe it is necessary for a SharePoint hybrid workforce to be security aware as they collaborate in real time across various

regions of the world. We have handpicked topics in cybersecurity to raise your awareness of the risks so that you have a great start to factor these risks and create your risk mitigation plan for a secure and well-performing SharePoint hybrid deployment.

Acknowledgments

From us all

A big thanks to Rosemary Caperton from Microsoft Press who supported and guided this project throughout its journey and all assistance to make this book series a success!

To Bob Russell and Dianne Russell from Octal Publishing, Inc., we appreciate your effort to make it such a smooth experience for all of us.

Jeremy Taylor

To my coauthors, Neil Hodgkinson and Manas Biswas from Microsoft, it was a fantastic experience collaborating with you throughout this book. You guys are so knowledgeable, and I am honored to work with you.

I appreciate all those who helped me directly or indirectly to make creating this book an easier experience for me. In particular, thanks to Matt Swann from Microsoft for providing me with your expert advice on cybersecurity.

Special thanks to Gunter Staes from Microsoft as well as my colleagues Michael Chiu and Phil Smith.

Thanks to all of my colleagues, clients, and customers who have given me countless opportunities to design, build, and support SharePoint capabilities over the past decade.

Neil Hodgkinson

First, let me acknowledge my coauthors: Jeremy Taylor, who is the inspiration behind this book and brought a first-class level of knowledge and experience with his contribution; and Manas Biswas, my good friend and colleague, who is truly my Sensei when it comes to SharePoint and Office 365 hybrid technologies. Without your support and teachings, I would not be in a position to write this book.

I would also like to extend a heartfelt *grazie* to Luca Bandinelli, who brought me into the Office 365 Customer Advisory Team (CAT) and opened

up the SharePoint engineering world to me in his own unique way.

To Jeff Wilkes my current manager in CAT, thanks for taking on a grumpy Mancunian from England and giving me all the opportunities to grow and develop in my role at Microsoft.

Finally, I want to express my thanks to several close friends who inspire me in so many different ways.

To Tony Bewley, my Karate instructor, who is one of the strongest and most patient people I know and someone I consider a true friend and Kyoshi.

To Spence Harbar and Bob Fox, my brothers-in-arms, who keep my feet on the ground, always tell me the truth even when it might hurt, and most of all never fail to help and support me when I need it the most.

Manas Biswas

I would take this opportunity to acknowledge and thank the efforts of few key people in my life without which this would not been possible.

Firstly, A big thank you to Neil!! You are way beyond my cowriter in this book. Thank you, my friend, for all the sync-up and work we do

together. I'm lucky to have a friend like you and thank you for your contributions and support throughout this book.

Thank you Jeremy, for being a coauthor and for all the valuable inputs and interactions during the course of writing this book.

Thank you Phil Cohen and Soon Chong, for having faith in me and giving me my first opportunity in the Office365 Service Engineering organization at Microsoft.

Thank you Luca Bandinelli, for being a mentor and always a call away, helping me solving some complex career decisions in life.

Thank you Roberta Vork, for your incredible drive and passion for hybrid. You have always been there to support me in technical challenges and in helping guide my career.

Thank you Renukanth J P for even making me believe that I should think of writing a book.

I would also like to thank a few people who has been great inspiration for me: Dr Amith Ellur, for all your guidance during my time in Microsoft CSS; Brian Lewis, for being a great manager and all the work we did in BETA testing; Bob Fox, for being a great friend and standing by when I need any support.

Finally, to all my good friends and colleagues in White Glove Engineering Team and Microsoft India; there are too many of you to mention each of you individually. Thank you for the help and support over the years we have worked together.

Free ebooks from Microsoft Press

From technical overviews to in-depth information on special topics, the free ebooks from Microsoft Press cover a wide range of topics. These ebooks are available in PDF, EPUB, and Mobi for Kindle formats, ready for you to download at:

<http://aka.ms/mspressfree>

Check back often to see what is new!

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

<http://aka.ms/ConfiguringSharePointHybrid/errata>

If you discover an error that is not already listed, please submit it to us at the same page.

If you need additional support, email Microsoft Press Book Support at mspinput@microsoft.com.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to <http://support.microsoft.com>.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable

asset. Please tell us what you think of this book at:

<http://aka.ms/tellpress>

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: <http://twitter.com/MicrosoftPress>.

Introduction and prerequisites

This e-book is the second of a series on Microsoft SharePoint hybrid. This chapter presents an overview of the configuration areas essential for a SharePoint hybrid environment and provides a list of requirements for configuring its capabilities. In this chapter is a summary of all the technology components and tools that you can use as a refresher if you need, or a great list for if you simply want to further your knowledge regarding the skills required to configure and

operate a SharePoint hybrid environment. It also details the steps required to configure a server-to-server (S2S) authentication trust with Microsoft Azure Access Control Service (ACS). The ACS trust is a base requirement for most SharePoint hybrid capabilities.

Introduction

SharePoint hybrid brings your organization the best of both worlds: a cloud-powered SharePoint on-premises farm. Users in your organization will be able to reap the benefits of the investments Microsoft has made in Office 365 and Azure Active Directory, such as increased productivity in collaboration and communication as your business requires.

The list of SharePoint hybrid solutions is growing in number, bringing you the most advanced

productivity tools that you can consume and rollout to your users at your own pace.

This book is aimed at providing a technical audience with a guide on how to configure SharePoint hybrid solutions such as search, Business Connectivity Services, Microsoft OneDrive for Business, profiles, and extranet sharing. You will gain insights into the benefits of each of the hybrid solutions covered in this book along with technical steps on how to configure, troubleshoot, and manage a SharePoint hybrid environment.

It is necessary for you and your administration team to understand the intricacies involved in configuring a SharePoint hybrid environment.

The first book in this series, *Planning and Preparing for Microsoft SharePoint Hybrid*, which you can download from https://blogs.msdn.microsoft.com/microsoft_press/2016/04/26/free-ebook-planning-and-preparing-for-microsoft-sharepoint-hybrid, covers the essential building blocks for connecting your on-premises directory to Azure Active Directory, synchronizing users, and managing the underlying tools and infrastructure around it. This book builds upon what you have configured by following the steps provided in that first book.

Overview of SharePoint hybrid solutions

There are a number of SharePoint hybrid solutions that are available to enhance your existing investments in SharePoint on-premises. In this e-book, we will focus on most hybrid solutions available for SharePoint hybrid. Some solutions, such as SharePoint hybrid Insights (currently in preview) and Yammer, are not covered here. The following subsections provide a brief summary of the solutions covered in this book.

Hybrid search

With Query federation–based hybrid search, users are able to search for content residing in both SharePoint Online and SharePoint on-premises from within the corporate network. This is known as *outbound search*. Users outside of the corporate network and in Office 365 are also able to search SharePoint Online and SharePoint on-premises content. This is known as *inbound search*. If both of these approaches are configured, it is referred to as a *two-way search*. These search topologies represent what is referred to as the classic approach to SharePoint hybrid search in this book.

In late 2015, the hybrid cloud search service application was released, with which users can search across SharePoint Online and SharePoint on-premises, with the indexing performed and hosted in SharePoint Online. The hybrid Cloud Search Service Application can crawl content sources such as other SharePoint farms, websites, and file shares.

Hybrid Business Connectivity Services

Hybrid Business Connectivity Services (BCS) makes it possible for users to access and interact with data from a non-SharePoint business system, but it is done via an external list or app through the on-premises SharePoint farm or through Azure SQL Database. These non-SharePoint business systems could be your organization's human resources or Enterprise Resource Planning (ERP) systems, which in this e-book we refer to as Line-of-Business (LOB) systems.

Hybrid OneDrive for Business

With hybrid OneDrive for Business, users work-related files are stored in OneDrive for Business in Office 365, giving them new ways of

collaborating with others. SharePoint administrators who are familiar with on-premises OneDrive for Business storage will know that it is basically the users document libraries in their personal sites via the My Site host. OneDrive for Business in Office 365 essentially replaces the requirement for your organization to host the on-premises OneDrive for Business storage offered with the personal sites. Similar names but different destination. Office 365 accommodates 1 TB of storage per user. When activated, users can click the OneDrive link in SharePoint on-premises, at which point they are redirected automatically to their OneDrive for Business in Office 365.

Hybrid Sites Features

Hybrid Sites Features is a bundle of features that you can turn on for your SharePoint on-premises farm. With this comes, site following, hybrid profiles, and extensible app launcher (SharePoint Server 2016 only). Many of these SharePoint hybrid features make use of a technique called *redirection*. With redirection, when users attempt to access a service in SharePoint server using site navigation, they are automatically redirected to the equivalent service in Office 365.

Hybrid site following

Followed sites from both on-premises SharePoint and SharePoint Online locations are consolidated in the SharePoint Online followed sites list. When a user accessing an on-premises SharePoint site clicks the Sites link, he will be redirected to his consolidated followed site page in SharePoint Online

Hybrid profiles

When you turn on hybrid Sites Features, hybrid profiles are in effect. This means that users will have a single Delve-powered profile where their profile information is displayed for organizational collaboration purposes. Hybrid profiles is a redirection of hybrid users to their own profile in Office 365 instead of the on-premises My Sites user profile.

Hybrid extensible app launcher

A SharePoint Server 2016–only solution, you can use the extensible hybrid app launcher to offer new apps that hyperlink to sites or web applications with their own custom icon. This makes it possible for users to pin any of these apps as tiles to their app launcher for quick access. When users pin these to their app

launcher, they automatically appear in the on-premises SharePoint Server 2016 app launcher.

Delve

In a SharePoint hybrid environment, the Delve experience can be augmented with some on-premises content based on managed properties processed by the Cloud Search Service Application and trimmed to match the user's permissions to that content.

Extranet sharing

Extranet sites give you the means to provide secure collaboration between business partners and your organization. Sending documents back and forth by email are a thing of the past, because all content is kept in one place and each business partner has access to only their content. Traditionally, deploying a SharePoint on-premises extranet site involves complex configuration to establish security measures and governance, including granting access to inside the corporate firewall, and expensive initial and on-going cost. But with Office 365 SharePoint Online, partners connect directly to a members-only site in Office 365, without access to the corporate on-premises environment or any other

Office 365 site. You can access Office 365 extranet sites from anywhere.

Technology components overview

If you are concerned about the skills required to configure a SharePoint hybrid environment, there are a number of Microsoft tools and technology components with which you need to be familiar. Although this book series has clearly laid out the planning, preparation, and configuration how-to's for you, the ongoing management of a SharePoint hybrid is not a trivial task. You will need to be well versed across a range of technologies and tools to configure and manage a SharePoint hybrid environment. The following subsections present an overview of what you'll need to know.

Active Directory and Azure Active Directory

Active Directory is your store of users and groups in your Windows directory on-premises. Azure Active Directory is a store of users and groups in the cloud, hosted by Microsoft, in Microsoft's data centers. Azure Active Directory

is a securely partitioned multitenant directory service, where one tenant cannot access another tenant's information. You typically "master" users in Active Directory on-premises and then synchronize them with Azure Active Directory.

IdFix directory synchronization error remediation tool

This is the tool required to scan and report issues with identities in your on-premises directory service that might have synchronization issues with Azure AD. You can fix these identities either manually or from within the IdFix tool. It is essential to run this tool and remediate any issues before configuring the Azure Active Directory Connect (AD Connect) tool.

Azure AD Connect

Azure AD Connect is the preferred tool to synchronize your on-premises users and groups to Azure Active Directory. This core functionality of directory synchronization is also referred to as *DirSync*. Azure AD Connect supersedes several older tools, providing an improved configuration wizard and more granular options for synchronization of your user identities. This tool

is absolutely essential for a SharePoint hybrid environment.

You have two options when it comes to synchronizing user identities to Azure Active Directory:

- Synchronized identities with password hash synchronized to Azure Active Directory.
- Federated identities that authenticate to a federation service such as Active Directory Federation Services (AD FS). This is a requirement for a single sign-on (SSO) experience for your users.

Federation service

There are a few options available here, but throughout the e-books in this series, we have based our federation service on AD FS. It is possible to use other federation services for SSO capabilities, such as Shibboleth.

Reverse proxy

This is the device that is used to publish the SharePoint on-premises site for hybrid search as well as hybrid BCS. In our examples in the SharePoint hybrid series, we have used Microsoft's reverse proxy called the Web

Application Proxy. The Web Application Proxy also has an AD FS proxy service that we often refer to in the first book. The AD FS proxy service is required to securely publish the AD FS service in a perimeter network. You also can use the Web Application Proxy to publish Office Online Server or Office Web Apps server required to generate previews for on-premises content with federated search.

Certificates

There are a number of certificates that you need to acquire and maintain when you are working with SharePoint hybrid.

Federation service certificates

If you do decide to configure federated identities for SSO in your organization, there are three certificates that you must manage:

- Service communication certificate
- Token signing certificate
- Token decryption certificate

This is discussed in detail in, [*Planning and Preparing for Microsoft SharePoint Hybrid*](#), Chapter 6, in the section "Secure Sockets Layer certificates."

S2S ACS trust certificate

The last part of this chapter walks you through the steps on how to configure the S2S trust with ACS. You must have a certificate that is used to sign the authentication tokens issued on behalf of the users. This is discussed in more detail in the section “S2S Trust” later in this chapter.

SharePoint site publishing certificate

This is a certificate required to publish the SharePoint site (either a web application or a host-named site collection). In our examples, we have published <https://intranet.contoso.com> via the Web Application Proxy service. Chapter 2 discusses this in detail and has hyperlink references to Microsoft sources that we created.

Client authentication certificate

For security reasons, it is recommended to have this certificate as a separate certificate to the SharePoint site publishing certificate. This certificate is used for client authentication where requests that are sent from Office 365 reaches the reverse proxy device (Web Application Proxy in our examples) on which the on-premises web application has been published and configured with client preauthentication.

To learn more, refer to the section “Publishing the SharePoint on-premises web application by using client certificate preauthentication” in Chapter 2.

SharePoint On-Premises

Most testing and screenshots in this SharePoint hybrid book series have been done by using SharePoint Server 2016. However, SharePoint Server 2013 has most of the cloud-capabilities available to it except for a few like the extensible app launcher and SharePoint hybrid insights (currently in preview). If you have an opportunity to build a SharePoint hybrid environment from the ground up, I recommend that you consider SharePoint Server 2016 as your on-premises SharePoint farm version. If you currently have a SharePoint Server 2013 farm in operation, I recommend that you test all hybrid configuration in a non-live environment including your directory services, utilizing test users. SharePoint Server 2013 foundation does not have the necessary service applications to be able to work in a SharePoint hybrid environment; for example, it does not have a user profile service.

Let's go through some of the SharePoint on-premises services you will need to implement.

User profile service application

This is the service application that synchronizes users from Active Directory to SharePoint and maintains its own store of all the profiles of users. As a SharePoint farm administrator, you have the ability to configure the Active Directory attribute mapping for users in this service application.

My Site host and personal sites

Using the My Site host, you can use a designated site to host personal sites for your users in SharePoint on-premises. With personal sites, each user will be the site collection administrator of their personal site, and the document library of their personal site is only available for each user's work files. This document library is labelled as OneDrive for Business. (More about this in Chapter 4.)

Search Service Application

This service application is responsible for crawling on-premises content sources that can be SharePoint sites across your organization, websites, file shares, and other LoB system data. You must have the Search Center configured in

order to use hybrid search. Chapter 2 covers the configuration of the Cloud Search Service Application. This application is responsible for crawling on-premises content sources and it also acts as a query processor in the query federation based–search model.

Secure Store Service

The Secure Store Service (SSS) holds credentials in a secure manner and are referred to by an application ID name that you specify. This SSS application ID can be used by services like BCS to connect to servers and remote systems. We will be creating and using SSS application IDs in Chapter 2 and Chapter 3.

Business Connectivity Services

The Business Connectivity Services (BCS) is a service in SharePoint that facilitates connecting remote data sources and presenting them in SharePoint through either an external list or an add-in. BCS was also known as Business Data Connectivity services in SharePoint 2007, so you might see references such as BDC when you are working with BCS. In this book, we work with external lists for BCS hybrid.

ULS Viewer

The Unified Logging Service (ULS) Viewer is a tool for viewing SharePoint on-premises logs. It is an essential tool to troubleshoot SharePoint issues.

Microsoft Visual Studio

This is the development tool referred to and used in Chapter 3 in this book. We used Visual Studio to create an OData endpoint required for hybrid BCS. In this book, we demonstrate how to use Visual Studio to work with the BCS External Content Types (ECTs).

Prerequisites for hybrid scenarios

Because there are a number of infrastructure components that are required as a whole for SharePoint hybrid, not all of these technology components are required for all of the hybrid scenarios. The following table will help you plan what components you need for each of the hybrid scenarios and capabilities you are planning for your organization.

Scenario	AADSync/ DirSync	SSO/ AD FS	ACS trust	Reverse proxy	Comments
OneDrive for Business	Y	O	O	N	
Sites features	Y	O	Y	N	
Extranet	Y	O	O	N	
Profile	Y	O	O	N	
BCS	Y	O	Y	Y	
Search					
Outbound Federation	Y	O	Y	N	
Inbound Federation	Y	O	Y	Y	Reverse proxy (RP) for access to on-premises web application. RP for publishing Office Web Apps or Office Online server.
Cloud SSA	Y	O	Y	O	RP for publishing Office Web Apps or Office Online server.

Y = Yes (required); O = Optional; N = Not required

We cover each of the above scenarios in subsequent chapters in this book.

Modules for hybrid with Windows PowerShell

There are a few prerequisites that you must install to configure and manage your hybrid environment. Office 365 and Azure come with their own set of Windows PowerShell commands that are required in operations such as creating the S2S trust manually. Office 365 Windows PowerShell lets you manage your Office 365 Admin Center settings from the command line.

Microsoft Online Services Sign-In Assistant for IT Professionals

You need to install the Microsoft Online Services Sign-In Assistant for IT Professionals RTW from the Microsoft Download Center at <http://go.microsoft.com/fwlink/?LinkID=286152>.

The Microsoft Online Services Sign-In Assistant provides end-user sign-in capabilities to Microsoft Online Services, such as Office 365 and

Azure. It installs client components that allow common applications, such as Microsoft Outlook and Lync, to authenticate to Microsoft Online Services.

Azure Active Directory Module for Windows PowerShell

You also need to install the Azure Active Directory Module for Windows PowerShell (64-bit version) by downloading and running it from <http://go.microsoft.com/fwlink/p/?linkid=236297>

You should be able to launch the Windows Azure Active Directory Module for Windows PowerShell window because it will be installed as part of the aforementioned installation. Upon launching the Windows Azure Active Directory Module for Windows PowerShell, your Windows PowerShell will have a preloaded collection of Microsoft Azure-related commands.

Connect to Azure Active Directory and Office 365

You will need to connect to Azure Active Directory and Office 365 to run Windows PowerShell commands to configure components such as the S2S ACS trust used by SharePoint hybrid functionality. To do so, run the connect-

msolservice cmdlet at the Windows PowerShell command prompt. You will then be prompted for your credentials. If you want, you can supply your credentials in advance; for example:

```
$msolcred = get-credential
```

In the Windows PowerShell Credential Request dialog box that opens, type your Office 365 Global Administrator user name and password, and then click OK.

```
connect-msolservice -credential $msolcred
```

More info To read more about Office 365 Windows PowerShell, go to <https://technet.microsoft.com/library/dn975125.aspx>.

S2S trust

S2S authentication configuration for SharePoint hybrid environments consists of establishing a trust between SharePoint on-premises and ACS. ACS is then the trust broker for both SharePoint on-premises and SharePoint Online. When S2S trust is fully configured, each server farm trusts the security tokens that are issued by ACS and are used for authenticating access to resources on behalf of the identified user.

S2S trust setup—certificate management

To begin, we need to consider the trust element of the communication between the on-premises SharePoint server farm and the Office 365 tenant. As already mentioned, this trust is “brokered” by Azure ACS, and to configure the trust, you must obtain a certificate that is trusted by both parties and can be used to sign the authentication tokens issued on behalf of the users. The administrator has a number of options available to obtain this certificate, each offering different advantages:

- Obtain a publically signed Secure Sockets Layer (SSL) certificate from a trusted certificate signing authority.
- Create a new self-signed certificate specifically for this purpose.
- Extract the built-in self-signed certificate deployed on each farm server and used as the Secure Token Service (STS) signing certificate for inter server communication across the on-premises SharePoint farm.

Many companies will not allow self-signed certificates to be used for production applications, especially applications that

communicate over untrusted network segments such as the Internet. For this reason, obtaining a publically signed and trusted certificate is a recommended practice, and for many companies will be a requirement to comply with their own security regulations or standards.

More info Obtaining a public-signed SSL certificate is a common task, and we will not detail the steps here. However, obtaining a self-signed SSL certificate is different. You can find the details on how to do this at [https://technet.microsoft.com/library/cc753127\(v=ws.11\).aspx](https://technet.microsoft.com/library/cc753127(v=ws.11).aspx).

We should also note that if the built-in STS certificate is not chosen as the certificate for creating the trust, it must be replaced with the newly obtained certificate as the farm STS certificate. This means the certificate needs to be deployed to every server in the farm and configured as the STS Token Signing certificate by using Windows PowerShell.

Replacing the STS Token signing certificate is a disruptive operation requiring an Internet Information Server (IIS) recycle and a SharePoint Timer Service recycle. This operation should be conducted during non-business hours. Also consider that if you're using a self-signed or

publically signed SSL certificate, they do have an expiration date and must be replaced before the date is reached to avoid breaking the hybrid workloads.

When using a new self-signed or a public-signed certificate, you need two versions of the certificate: one in the .pfx format, which will be used to replace the original farm STS certificate, and a second in the .cer format, which will be used to generate a credential value for configuring the ACS trust.

To convert a .pfx certificate to a .cer format, you can use the following Windows PowerShell script:

```
Get-PfxCertificate -FilePath c:\certs\mystscert.pfx  
| Export-Certificate -FilePath  
c:\certs\mystscert.cer -Type CERT
```

The mechanism to replace the farm STS is as follows:

1. Copy the .pfx formation of the certificate to a farm server; for example, c:\certs\mystscert.pfx where you will run the Windows PowerShell to configure the trust.
2. Run the Windows PowerShell script:

```
# Variables for the script cmdlets  
$stscertpfx="c:\certs\mystscert.pfx"  
$stscertpassword="password"
```

```
# Create the new certificate object
$pxCertificate=New-Object
System.Security.Cryptography.X509Certificates.X5
09Certificate2 $stscertpx, $stscertpassword, 20

# Update the Certificate on the STS
Set-SPSecurityTokenServiceConfig -
ImportSigningCertificate $pxCertificate
```

You must recycle the SharePoint Timer Service and run IISRESET on every machine in the farm after running this script so that the new STS certificate is loaded.

The final certificate option, extracting the built-in STS certificate, is more complicated but can be carried out by using Windows PowerShell as follows:

1. Obtain the signing certificate:

```
$SPSigningCert = (Get-
SPSecurityTokenServiceConfig).LocalLoginProvider
.SigningCertificate
```

2. Run the following to get the STS certificate thumbprint:

```
$thumb = $SPSigningCert.Thumbprint
```

3. Create a password for the certificate as a secure string by using the following Windows PowerShell command:

```
$mypwd = ConvertTo-SecureString -String
"password" -Force -AsPlainText
```

4. Define the location and filename for the certificate:

```
$mypfxcertpath = "c:\certs\mystscert.pfx"  
$mycercertpath = "c:\certs\mystscert.cer"
```

5. Export the SharePoint STS certificate to the filesystem as .pfx and .cer formats by using the following Windows PowerShell:

```
Export-PfxCertificate  
cert:\localmachine\sharepoint\$Thumb -Password  
$mypwd -FilePath $mypfxcertpath  
Export-Certificate -Cert  
cert:\localmachine\sharepoint\$Thumb -Type CERT  
-FilePath $mycercertpath
```

There is no need to recycle services if you choose this option.

Note When we use the built-in STS certificate, there is no need to obtain it in both .pfx and .cer formats; only .cer is required. The export of .pfx included in the preceding example for completeness only and to allow the administrator to take a backup of the .pfx sts certificate.

At this point we are now in a position to begin configuring the core hybrid setup.

Configuring the ACS trust

Regardless of the certificate type selected, the ACS trust configuration includes identical steps and involves the .cer version of the certificate only.

To create the ACS trust, you first need to convert the .cer certificate to a base-64 encoded version. The base-64 encoded version is required because you cannot upload the certificate directly to Office 365; instead, you need to configure it as a new service principal credential for the Office 365 SharePoint Online AppId. You can do this by running the following Windows PowerShell script:

1. Create the certificate object and import the .cer file.

```
$stscertcer = "C:\Certs\mystscert.cer"  
$cerCertificate = New-Object  
System.Security.Cryptography.X509Certificates.X5  
09Certificate2  
$cerCertificate.Import($stscertcer)
```

2. Create the credential by base-64 encoding the raw certificate data.

```
$cerCertificateBin =  
$cerCertificate.GetRawCertData()  
$credValue =  
[System.Convert]::ToBase64String($cerCertificate  
Bin)
```

3. Import the Microsoft Online Windows PowerShell Modules.

```
Import-Module MSOnline -force -verbose  
Import-Module MSOnlineExtended -force -verbose
```

4. Connect to Microsoft Online as an administrator.

```
$cred=Get-Credential  
Connect-MsolService -Credential $cred
```

5. Register the On-Premise STS as Service Principal in Office 365 by running the Windows PowerShell script that follows. In our example, we have chosen <https://on-premises.contoso.com> for our on-premises SharePoint site. Update this with your on-premises site.

```
$spoappid = "00000001-0000-0000-c000-  
000000000000"  
$spcn="*.contoso.com"  
$spsite=https://onpremises.contoso.com  
  
New-MsolServicePrincipalCredential -  
AppPrincipalId $spoappid -Type asymmetric -Usage  
Verify -Value $credValue
```

6. Configure the Service Principal for the on-premises domain by running the following in Windows PowerShell:

```
$SharePoint = Get-MsolServicePrincipal -  
AppPrincipalId $spoappid  
$spns = $SharePoint.ServicePrincipalNames  
$spns.Add("$spoappid/$spcn")
```

```
Set-MsolServicePrincipal -AppPrincipalId  
$spoappid -ServicePrincipalNames $spns
```

7. Register the Office 365 AppID as an App Principal in the on-premises farm and set the authentication realm to match the Office 365 tenant context.

```
$spocontextID = (Get-  
MsolCompanyInformation).ObjectID  
$spoappprincipalID = (Get-MsolServicePrincipal -  
ServicePrincipalName $spoappid).ObjectID  
$sponameidentifier =  
"$spoappprincipalID@$spocontextID"  
$site=Get-Spsite "$spsite"
```

```
$appPrincipal = Register-SPAppPrincipal -site  
$site.rootweb -nameIdentifier $sponameidentifier  
-displayName "SharePoint Online"
```

```
Set-SPAAuthenticationRealm -realm $spocontextID
```

8. Create the Azure Access Control Services Service Application Proxy Connection by using the following:

```
New-SPAzureAccessControlServiceApplicationProxy  
-Name "ACS" -MetadataServiceEndpointUri  
"https://accounts.accesscontrol.windows.net/meta  
data/json/1/" -DefaultProxyGroup
```

9. Create a new Trusted Security Token Issuer for the ACS endpoint:

```
New-SPTrustedSecurityTokenIssuer -  
MetadataEndpoint  
"https://accounts.accesscontrol.windows.net/meta  
data/json/1/" -IsTrustBroker -Name "ACS"
```

At this point, the trust is in place between the on-premises farm and ACS, which complements the existing trust between ACS and Office 365 to allow authentication tokens to flow between Office 365 and SharePoint on-premises utilizing ACS as the trust broker.

Validating the trust configuration and also how to remove the trust is covered in Chapter 7.

After you have the ACS trust set up, you are now in a position to configure the outbound search experience that is covered in Chapter 2.

SharePoint Server hybrid search

This chapter focuses on the search workload of SharePoint on-premises and SharePoint Online. It covers both simple and complex federation scenarios that have been around for a number of years now. It concludes with the latest search hybrid feature, the hybrid Cloud Search Service Application.

The importance of search

When considering the multiple workloads that SharePoint can handle, enterprise search comes

right at the top of the list because of the breadth of features and capabilities it offers. From the simplest search solution that you can achieve by just deploying an Enterprise Search Service Application in the on-premises farm and using it to locate content saved within the various libraries on the same farm, all the way through to complex search-driven publishing sites, driving the user experience and e-discovery solutions assisting with regulatory compliancy and records management.

Hybrid search is important for SharePoint Online customers. Migration to the cloud is not an overnight exercise and, in fact, many enterprise customers might not move 100 percent of their infrastructure and content to the cloud; instead, they might opt for a perpetual hybrid state. Here are some key objectives of hybrid deployment:

- Reduce operation cost
- Use hybrid to take advantage of advanced cloud functionalities
- Use hybrid as short- and mid-term migration to cloud strategy

Migration from SharePoint on-premises will typically take a long time for enterprise customers. No one will migrate everything to

cloud in one shot. Therefore, during migration, some content will definitely live on-premises and some will be migrated to the cloud. If a company is going to be in the “mid” state for an extended period of time, there is a risk that end users will become confused about what content resides where. That is when hybrid comes in to play; users can search for content and get search results irrespective of where the content resides.

Hybrid search overview

The power of search in enhancing the user experience in hybrid scenarios cannot be stressed too highly. It is the key workload that unifies both the on-premises deployment and the Microsoft Office 365 SharePoint Online environment, making it possible for users to discover and access content in either environment, regardless of the location of the end user. As you will see, the experience of the end user depends largely on what is known as the *Authentication Topology* and the choice of hybrid implementation.

There are four possible deployment strategies for hybrid search:

- **Outbound search** (most common)
Outbound from the customer’s network

(SharePoint on-premises) to SharePoint Online. A user in the corporate network searches from on-premises. There is an outbound request to SharePoint Online to return results. Results from both verticals are shown on the results page.

- **Inbound search** Inbound from SharePoint Online to a customer's network (SharePoint on-premises). A user who is not on the corporate network but signed into SharePoint Online carries out a search. There is an inbound request to the SharePoint on-premises located on the corporate network to return results. Results from both verticals are shown on the results page.
- **Two-way search** Search is set up both inbound and outbound, as just described. Both scenarios are supported in that case—whether the user is on-premises on the corporate network, or signed in only to SharePoint Online.
- **Cloud Search Service Application** The on-premises Search Service Application is configured to feed the Office 365 search index to provide a true unified search experience for end users. Outbound search is commonly used alongside the Cloud Search

Service Application to provide search results to on-premises users.

The first three of these scenarios are based on the *Query* model, whereby the search results presented to the user are generated by a federation model at query time and displayed as separate “blocks” of results controlled by query rules. Each block contains search results from different search indexes. This type of hybrid search experience is often referred to as *classic hybrid search*.

The last scenario represents a very different approach, and in this case the user hybrid experience is driven by a *Crawl* model, whereby all the results presented to the user are generated from a single search index.

To support these hybrid solutions, SharePoint on-premises and Sharepoint Online need to be configured to support Server-to-Server (S2S) authentication. This provides the ability to support identity delegation across environments such as SharePoint on-premises and SharePoint Online, utilizing the OAuth authentication protocol.

In the same way that SharePoint add-ins use OAuth to access SharePoint data, so hybrid search works based on an OAuth layer. The

primary goal of hybrid search experiences is for users to be able to find items regardless of where SharePoint, or indeed the user resides; that is, on-premises or online. Hybrid search gives the ability to run a query and get the most relevant results from SharePoint Online and SharePoint on-premises. In the query federation hybrid scenarios in SharePoint Server 2013 and 2016, we use OAuth and Remote SharePoint Index to give a user in one farm the ability to submit a query to another SharePoint farm. Of primary concern when searching for content is that the permissions on crawled objects or Access Control Lists (ACLs) are respected so that the user gets search results that are appropriately security trimmed. To do this, the user identity needs to be refreshed in the remote SharePoint farm. S2S authentication and related communication is a prime requirement for hybrid search to work.

We will look closely at the different models and how to configure them.

Infrastructure requirements for classic hybrid search deployments

At this point, we are ready to look at the infrastructure components that you need to set up your hybrid scenarios. Hybrid search, like other hybrid solutions, depends on the core identity elements defined in book one of this series, [*Planning and Preparing for Microsoft SharePoint Hybrid*](#). Figure 2-1 provides an overview.

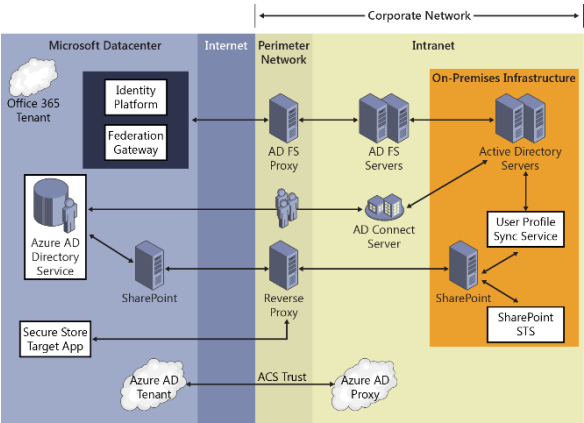


Figure 2-1: Schematic diagram of connectivity between on-premises and Office 365 SharePoint Online showing perimeter network components and identity data flow as well as search query flow.

We can begin by examining the on-premises infrastructure needed to support the implementation. At its most basic, we require a SharePoint 2013 SP1 or 2016 Server farm configured with an Enterprise Search Service Application. The SharePoint farm must be deployed into an Active Directory domain of at least 2008 functional level and support Windows Claims as the authentication model for end-user access.

In the SharePoint on-premises farm, it is critical that the User Profile Service Application (UPA) is turned on and running. The UPA must also be populated with current data from Active Directory. UPA on the local farm is used to determine what rights users have, what claims they have, what groups they belong to, and so on. With a hybrid solution, anyone to whom you grant rights needs to be in the profile system. Post hybrid configuration, when a search is issued from the local search center to the remote farm, the user's UserPrincipalName (UPN) is sent along with the query. Upon receiving the request, the remote farm will perform a UPA lookup for a user profile that matches the

attribute that was sent. The match can be on UPN, email, or SIP Address, and this is the reason you would want those values to be populated in the UPA.

Also in the on-premises farm, the Subscription Settings Service and App Management Service Applications are required to support the SharePoint Apps infrastructure and are a prerequisite for SharePoint Online to be a registered as a high-trust app in SharePoint Server 2013.

In the Microsoft datacenter, the components needed to support search-based hybrid scenarios with SharePoint on-premises are the Office 365 tenancy including SharePoint Online and the Microsoft Azure Active Directory service. For some hybrid search functionality, an Enterprise subscription will be required for the Office 365 tenant.

There are several other components that come into play when deploying a search-based hybrid experience.

- **Azure Active Directory Connect (AD Connect)** This is deployed on a member server in the on-premises domain and is used to synchronize users and groups to the Azure Active Directory service to support the

user authentication and the rehydration process.

- **Trust broker** A Trust must be configured between the on-premises farm and Azure Access Control Services (ACS) to make it possible for ACS to act as a trust broker to validate an outbound request from the on-premises farm. This is generally referred to as an S2S trust. Azure Active Directory Access Control is a cloud-based federation service that provides an easy way to authenticate users against identity providers and, most important of all, Azure Active Directory. An Azure service is used to establish and broker trusted connections between two endpoints. ACS, in very simple terms, can be referred to as an authorization server. Office 365 already has a trust with ACS. However, for the on-premises SharePoint farm, you need to configure an ACS trust. ACS as an Azure service does provide Identity provider services (Idp); However, for a hybrid search deployment, ACS acts purely as an “invisible” trust broker for applications.
- **Active Directory Federation Services (AD FS)** The AD FS infrastructure provides the federation services to make single sign-

on (SSO) possible for users in the Office 365 tenancy. This is an optional component of a hybrid deployment when Password Sync has been turned on in Azure AD Connect but is recommended for a seamless user experience.

- **Reverse proxy component** Last, but by no means least, is the reverse proxy component, which has two key roles to play. In the inbound search scenario, it provides a route for the call from SharePoint Online to be routed to the on-premises search service. It is also used to ensure that the incoming request is from a trusted source by validating the certificate used to authenticate the query.

The following table shows the required and optional components for each of the four hybrid search scenarios:

Component	Outbound	Inbound	Bi-directional	Cloud SSA
AD FS	Optional	Optional	Optional	Optional
Azure AD Connect	Required	Required	Required	Required
ACS trust	Required	Required	Required	Required
Reverse proxy	Not required	Required	Required	Not Required

For all of the scenarios in this chapter, we assume the following:

- The company's on-premises domain has been added to the Office 365 tenant.
- Azure AD Connect has been configured with or without password synchronization.
- If password synchronization has not been turned on, AD FS has been deployed to support user sign-in to Office 365.
- An S2S trust has been set up between SharePoint on-premises and Office 365, using Azure ACS as the trust broker. You can configure this trust manually as detailed in Chapter 1, or it might already be in place if you have used the SharePoint Online Hybrid picker to deploy OneDrive or Hybrid Sites features, which is covered later in Chapter 4.

All other deployment requirements for each hybrid search scenario will be discussed in the relevant section.

Configuring outbound hybrid search

Configuring outbound hybrid search is very often perceived as the simplest method of achieving a hybrid search experience for your users, and in many ways it is. The critical step is in configuring the S2S trust which is the baseline for all hybrid scenarios. We discuss setting up the S2S trust in Chapter 1, so here we will focus on using that trust to provide outbound search for your users.

The query flow for an outbound hybrid search experience begins with the user submitting his query in the local search center. The on-premises Query Processor takes the user's identity claims plus his search query and forwards these on to the SharePoint Online search index where they are processed. Returned results are displayed as a result block or *search vertical* in the on-premises search center. To facilitate this experience, we need to carry some configuration of the search settings in the on-premises farm.

SharePoint on-premises configuration

After the trust is established, you need to carry out additional configuration steps for SharePoint Online search results to show up on a SharePoint on-premises search results page. As a rule of thumb, the configuration always needs to be done in the environment that should display the results from the other “remote” location. In this case, you are looking at displaying the SharePoint Online results within SharePoint on-premises search center. *To use this approach, you must deploy a search center in the on-premises farm because the site and lists search results page, `osssearchresults.aspx` cannot provide the hybrid experience.*

You need to carry out two administrative steps to configure hybrid search:

- Create a result source
- Create a query rule

Administrative permission is needed at the location where you intend to create these objects.

Result source

A result source is a definition that specifies the source from which to get search results. Result sources limit searches to certain content or to a subset of search results. In earlier versions of SharePoint (prior to SharePoint Server 2013), these were referred to as search scopes. The preconfigured default result source is Local SharePoint Results. However, you can always configure additional result sources; in this case, you need to define a new result source for SharePoint Online search results.

You can configure this on two different levels:

- Global, in the Search Service Application
- Local, per site collection or per site level

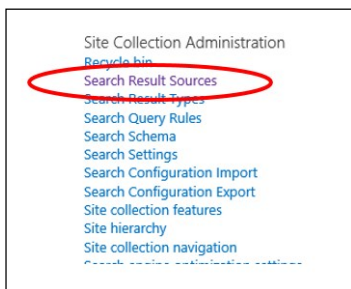
You can create a result source for a Search Service Application, a site collection, or a site. The following table shows the permissions that are required to create a result source at each level, and where the result source can be used.

When you create a result source at this level...	You must have this permission...	The result source can be used in...
Search service application	Search service application administrator	All site collections in web

		applications that consume the Search service application
Site collection	Site collection administrator	All sites in the site collection
Site	Site owner	The site

To perform the configuration at the on-premises site-collection level, follow these steps:

1. Go to the site where the result source is to be created.
2. In Site Settings, in the Site Collection Administration section, click Search Result Sources.



3. On the Manage Result Sources page, click New Result Source.

4. On the Add Result Sources page, do the following:
 - a. In the Name box, type a name for the new result source (for example, SharePoint Online).
 - b. For the Protocol, select Remote SharePoint.
 - c. For the Remote Service URL, type the address of the root site collection of the Office 365 SharePoint Online tenant whose results should be included (for example, <https://contoso.sharepoint.com>).

EDIT LINKS

Site Collection Administration · Add Result Source

Note: This result source will be available to all sites in the site collection. To make one for just this site, use [site result source](#).

General Information
Names must be unique at each administrative level. For example, two result sources in a site cannot share a name, but one in a site and one provided by the site collection can.
Descriptions are shown as tooltips when selecting result sources in other configuration pages.

Name
SharePoint Online

Description
Search results from the Contoso SharePoint Online Tenancy

Protocol
Select Local SharePoint for results from the index of this Search Service.
Select OpenSearch 1.0/1.1 for results from a search engine that uses that protocol.
Select Exchange for results from an exchange source.
Select Remote SharePoint for results from the index of a search service hosted in another farm.

☐ Local SharePoint
☒ Remote SharePoint
☐ OpenSearch 1.0/1.1
☐ Exchange

Remote Service URL
Type the address of the root site collection of the remote SharePoint farm.
<https://contoso.sharepoint.com>

- d. For the Type, select SharePoint Search Results.

- e. Leave the default setting for Query Transform, which is {searchTerms}.

More info A complex explanation of Query Transforms is beyond the scope of this book, but you can find a thorough discussion at <https://technet.microsoft.com/library/jj219620.aspx>.

- f. Leave the default option for Credentials Information (Default Authentication).

The screenshot shows a configuration window for a search result source. It has three main sections: 'Type', 'Query Transform', and 'Credentials Information'. In the 'Type' section, 'SharePoint Search Results' is selected with a radio button. In the 'Query Transform' section, there is a text box containing '{searchTerms}' and a 'Launch Query Builder' button. In the 'Credentials Information' section, 'Default Authentication' is selected with a radio button. There are also links for 'Learn more about query transforms' and 'Launch Query Builder'.

Type

Select SharePoint Search Results to search over the entire index.

Select People Search Results to enable query processing specific to People Search, such as phonetic name matching or nickname matching. Only people profiles will be returned from a People Search source.

Query Transform

Change incoming queries to use this new query text instead. Include the incoming query in the new text by using the query variable "{searchTerms}".

Use this to scope results. For example, to only return OneNote items, set the new text to "{searchTerms} fileextension=one". Then, an incoming query "sharepoint" becomes "sharepoint fileextension=one". Launch the Query Builder for additional options.

Credentials Information

If you are connecting to your intranet through a reverse proxy, please select and enter the SSO Id of the Single Sign On entry which stores the certificate used to authenticate against the reverse proxy. Else use the Default Authentication to authenticate against the remote SharePoint location.

☒ SharePoint Search Results
☐ People Search Results

☒ Default Authentication
☐ SSO Id

{searchTerms} Launch Query Builder

[Learn more about query transforms.](#)

- g. Click OK to save the new result source.

Note When SharePoint Server 2013 or 2016 is configured to include results from SharePoint Online, Credentials Information is Default Authentication. Default Authentication will pass the user's UPN as the identity claim alongside the search query for this result source.

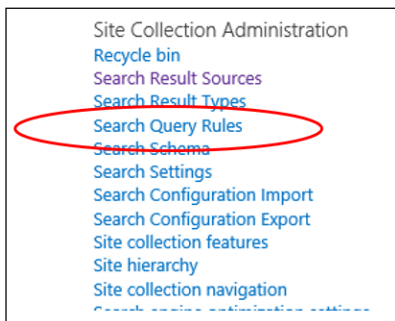
However, this will change in the section “Configuring inbound hybrid search,” in which we explain the importance of the SSO Application ID.

Now that you have a result source configured, you need to define the conditions under which a query is submitted to the result source from the on-premises search center.

Query rule

Whereas the result source defines where exactly to get the search results from, the query rule defines whether the result source is actually processed.

1. In Site Settings, in the Site Collection Administration section, click Search Query Rules.



2. In the For What Context Do You Want To Configure Rules? list box, select Local SharePoint Results (System) Content Source.

This is the source for which you want searches to trigger your hybrid outbound query.

3. Click New Query Rule.

EDIT LINKS

Site Collection Administration · Manage Query Rules

Use query rules to conditionally promote important results, show blocks of additional results, and even tune ranking. Changes may take several minutes to take effect. Note that dictionaries may take several minutes to update. [Learn more about query rules.](#)

For what context do you want to configure rules?

Local SharePoint Results (System) All User Segments All Topic Categories

New Query Rule | Order Selected Rules

Test a Query... find rules that fire for a query

Name	Modified	Conditions

4. In the General Information section, in the Rule Name box, type a name for the new query rule (for example, SharePoint Online Query Rule).
5. Click the Context link to expand the options.
6. In the Context section, do the following:
 - a. In the Query Is Performed On These Sources section, select either All Sources or select One Of These Sources. If you select One Of These Sources, make sure that you select the result source that you will search

on from the source site. The default is Local SharePoint Results (System).

- b. In the Query Is Performed From These Categories and Query Is Performed By These User Segments sections, leave the defaults for both.

The screenshot shows the 'Add Query Rule' page in Site Collection Administration. At the top, there is a note: 'Note: This query rule will apply to all sites in the site collection. To make one for just this site, use [site query rules](#).' Below this, the 'General Information' section is visible. It includes a 'Rule name' field with the value 'SharePoint Online Query Rule'. The 'Context' section explains that the rule can be restricted by source, category, or user segment. Three sections follow, each with a radio button selection: 'Query is performed on these sources' (selected: All sources), 'Query is performed from these categories' (selected: All categories), and 'Query is performed by these user segments' (selected: All user segments). Each section has an 'Add' link and a 'remove' link for the selected option.

EDIT LINKS

Site Collection Administration · Add Query Rule

Note: This query rule will apply to all sites in the site collection. To make one for just this site, use [site query rules](#).

General Information

Rule name
SharePoint Online Query Rule

Context
You can restrict this rule to queries performed on a particular result source, from a particular category of topic page, or by a user matching a particular user segment. For instance, restrict a rule to the Local Video Results source so that it only fires in Video search.

Query is performed on these sources

- ☒ All sources
- ☐ One of these sources

Local SharePoint Results (System) [remove](#)

[Add Source](#)

Query is performed from these categories

- ☒ All categories
- ☐ One of these categories

[Add Category](#)

Query is performed by these user segments

- ☒ All user segments
- ☐ One of these user segments

[Add User Segment](#)

7. In the Query Conditions section, click Remove Condition so that the rule will run for every query.
8. In the Action section, under Result Blocks, click Add Result Block.

Query Conditions Define when a user's search box query makes this rule fire. You can specify multiple conditions of different types, or remove all conditions to fire for any query text. Every query condition becomes false if the query is not a simple keyword query, such as if it has quotes, property filters, parentheses, or special operators.	This rule fires on any query text. Add Condition
Actions When your rule fires, it can enhance search results in three ways. It can add promoted results above the ranked results. It can also add blocks of additional results. Like normal results, these blocks can be promoted to always appear above ranked results or ranked so they only appear if highly relevant. Finally, the rule can change ranked results, such as tuning their ordering.	Promoted Results Add Promoted Result Result Blocks Add Result Block Change ranked results by changing the query

9. In the Add Result Block dialog box, do the following:
 - a. Leave the default for the Query Variables and Block Title sections.
 - b. In the Query section, in the Search This Source list box, select the name of the result source that you created earlier (in the example, it's SharePoint Online) and specify the number of items to show up as maximum (the default is 2).
 - c. Click the Settings hyperlink.
 - d. In the Settings section, ensure that the option This block Is Always Shown Above Core Results is selected.

- e. Skip the Routing section and click OK to add the result block.

10. Back on the Add Query Rule page, click the Publishing hyperlink.

11. In the Publishing section, ensure that the Is Active check box is selected.

12. Click Save.

More info If you want to explore additional configuration options with SharePoint Server Search Query Rules, you can review the documentation at

<https://technet.microsoft.com/library/jj871676.aspx>.

Testing outbound hybrid search

In Chapter 6, we investigate some steps for validating each of the previous configuration stages so that you can break them down for testing. For now, let's assume that everything has gone well so that we can demonstrate outbound hybrid search.

1. Sign in to the Search Center where the Result Source and Query Rule were configured.
2. Type **SharePoint** as a search query.
3. Review the Search Results page for the Hybrid Results block from Office 365.

sharepoint

Everything People Conversations Videos

Preference for results in English ▼

Results for "sharepoint"

Contoso Bistro
 "The menu shines as ever with distinctive dishes ... Choose from the very best, the freshest and highest quality food whether it's an everyday dinner or a special occasion ..."
contoso.sharepoint.com

Contoso Team Site - Site Pages
 Home System Account 6/3/2014 4:34 PM System Account 6/2/2014 4:18 AM ...
 SharePoint Help ... Search help and community Looking for recommendations ... There is no recommended article for ...
contoso.sharepoint.com/SitePages/Forms/AllPages.aspx

Contoso Team Site - MicroFeed
 SharePoint Help ... Search help and community Looking for recommendations ... There is no recommended article for this page ... Can't find what you are looking for ...
contoso.sharepoint.com/Lists/PublishedFeed/AllItems.aspx

Home
 AIIM-IWR-SharePoint-Puzzle-2012 ... Email Management for MS Exchange 10.3 New Features ...
intranet.contoso.com

How To Use This Library
 information about using Microsoft SharePoint Foundation-based wiki libraries, click Help on any Microsoft SharePoint Foundation page ...
intranet.contoso.com/SitePages/HowToUseThisLibrary.aspx

AIIM-IWR-SharePoint-Puzzle-2012
 and is a qualified CIP, ECM P and SharePoint P. © 2012 AIIM - The Global Community of Information Professionals The SharePoint Puzzle - adding the missing pieces ...
intranet.contoso.com/~/AIIM-IWR-SharePoint-Puzzle-2012.pdf

Modified date

One Year Ago Today

All

The result block will show Search Results from Office 365, and the regular search results will be from the Local SharePoint Search Index.

Now that the simplest of the search hybrid configurations is set up, we can go on to review the more challenging inbound hybrid search configuration.

Configuring inbound hybrid search

It's time to take a look at the steps to configure the inbound hybrid search topology. Almost all of the configuration work that you did to configure the outbound hybrid search topology is required for the inbound hybrid search topology, with just a few additional items,

We should assume that the on-premises environment will always be secured behind a firewall. To set up query federation from Office 365, the on-premises web application needs to be exposed to the Internet via a reverse proxy. You need to confirm that the connection through the reverse proxy is secured using a client signing certificate.

The query flow for inbound hybrid search is a little different to outbound hybrid search. After the user submits a search query in the SharePoint Online search center, it is passed to the SharePoint Online Query Processor, which evaluates the query rules and other search configuration elements. When the query rule for the on-premises result source is run, it initiates an additional request for search results from the on-premises search index. This request first

reaches the reverse proxy device on which the on-premises web application has been published and is configured with client certificate preauthentication. The result source in SharePoint Online has been configured with an SSO Application ID, which maps to a client authentication certificate for this exact reason. This certificate is returned in response to the authentication challenge from the reverse proxy. If the certificate matches the expected response, the query is allowed to proceed to the on-premises web application, and from there to the Search Service Application. We will look deeper into the configuration elements for this scenario in this chapter.

The following steps assume that one-way hybrid search is working and SharePoint on-premises is returning search results from SharePoint Online. The following steps are additional actions that are required to retrieve SharePoint on-premises search results when a user submits a query in a SharePoint Online search center:

1. Publish the SharePoint on-premises web application using client certificate preauthentication.
2. Secure store service application configuration.

After you complete these two steps, you need to repeat the results source and query rule configuration for inbound hybrid search.

Publishing the SharePoint on-premises web application by using client certificate preauthentication

For inbound hybrid search, the Microsoft SharePoint engineering teams have validated a number of reverse proxy solutions, including dedicated appliances and software-based options. For specific configuration guidelines, go to

<https://technet.microsoft.com/library/dn607304.aspx>.

In this chapter, we will focus on Microsoft Web Application Proxy as the reverse proxy solution. There are two schools of thought on the preferred way to configure this solution for hybrid scenarios. One such solution is documented on Microsoft TechNet at <https://technet.microsoft.com/library/dn551377.aspx> and uses a shared Secure Sockets Layer (SSL) certificate for the Web Application and the Secure Store. The authors prefer a dual certificate approach, as documented in their

blog article at <http://aka.ms/inboundhybridrp>, but you are encouraged to review both articles and choose the approach that best matches your requirements.

Regardless of the single- or dual-certificate approach, the SharePoint on-premises web application must be secured with an SSL certificate issued by a Public Certification Authority (PCA). This ensures that the identity of the web application can be trusted as well as being a requirement for publishing with Web Application Proxy. Additionally, a second certificate is required to act as the client preauthentication certificate. This certificate must also be issued by a PCA that is trusted by SharePoint Online. You need to install it on the reverse proxy and add it to a SharePoint Online Secure Store Service target application. The certificate can be one of the following types:

- Standard Domain certificate (Single name matching the external URL of the published SharePoint web application.)
- Multidomain certificate (SAN X.509 standard)
- Entire Domain certificate (Wildcard)

Each of these certificates must be of at least 2048-bit encryption.

Configuring Web Application Proxy

In our scenario, we will be using two different certificates, as per the guidance provided at <http://aka.ms/inboundhybridrp>. This guidance includes detailed step-by-step configuration details for installing and configuring WAP for inbound hybrid search.

The first certificate is a one acquired from a well-known PCA and is used to secure your externally published SharePoint web application `https://intranet.contoso.com`.

The second certificate is also acquired from a well-known PCA and is used for client preauthentication. It has the common name `userauth.contoso.com`.

Each of the certificates has been stored in the local computer account personal certificate store on the Web Application Proxy server and is also available on the file system at `C:\Certs`.

To publish a SharePoint web application using client certificate preauthentication, you must use Windows PowerShell. You can configure Web Application Proxy to only publish pass-through and AD FS secured web applications using the GUI.

By default, Web Application Proxy expects you to have identical BackendServerUrl and ExternalUrl. If you have configured different URLs for these parameters, you will need to disable URL translation for the publishing rule and add Alternate Access Mappings to the SharePoint web application. This is a more complex configuration, and you might want to take a visit to <https://technet.microsoft.com/library/dn528827.aspx> for more specific details.

To configure Web Application Proxy, use the following script, replacing certificate paths and URL names, as appropriate: (Note: the script will challenge for .pfx certificate passwords)

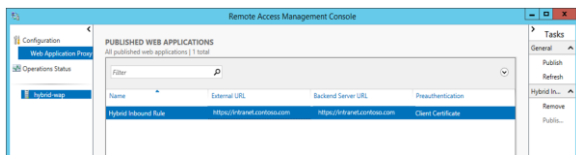
```
#Get the thumbprint of the external URL certificate
$externalcert = Get-pfxCertificate -FilePath
"c:\cert\internet_contoso_com.pfx"
$externalcert.Thumbprint

#Get the thumbprint of the client pre-
authentication certificate
$clientcert = Get-pfxCertificate -FilePath
"c:\cert\userauth_contoso_com.pfx"
$clientcert.Thumbprint

#Publish the Web Application
Add-WebApplicationProxyApplication `
-Name "Hybrid Inbound Rule" -BackendServerUrl
"https://intranet.contoso.com" `
-ExternalUrl "https://intranet.contoso.com" `
```

```
-ExternalCertificateThumbprint  
$externalcert.Thumbprint `  
-ExternalPreauthentication "ClientCertificate" `  
-ClientCertificatePreauthenticationThumbprint  
$clientcert.Thumbprint
```

After you complete this, the Remote Access Management Console on Windows Server 2012 R2 will show the Preauthentication status of the application as Client Certificate.



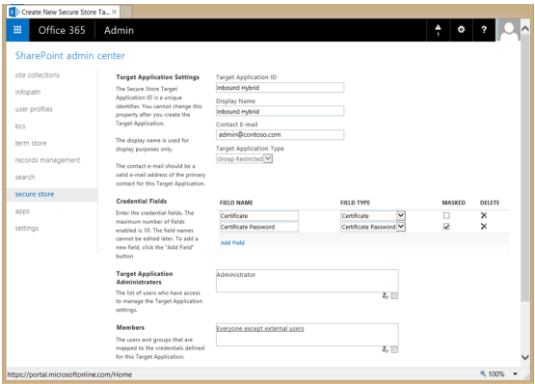
After the SharePoint web application has been securely published, the next step is to create the SharePoint Online secure store target application to support the client certificate preauthentication.

Configuring the SharePoint Online Secure Store Target application

To configure the secure store, you need to be a global administrator on the Office 365 tenancy and have access to the certificate used for the

client preauthentication on the Web Application Proxy server.

1. Sign in to the Office 365 Admin Center and open the SharePoint Admin Center site.
2. Go to the Secure Store Admin page and select New to create a new Secure Store Target Application.



3. Type a name for the new application and set the credential fields to match the following table:

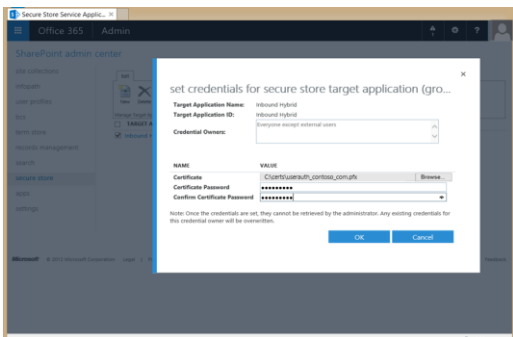
Field name	Field type
Certificate	Certificate
Certificate Password	Certificate Password

4. Complete the other fields for providing administrative control over this application and also specify the group(s) of users who are mapped to this identity.

The mapped users will be able to consume this secure store application from SharePoint Online. In this case, we are stating that all users of the tenancy except external users can call this application which will configure all users for searching.

5. Set the actual Certificate Information for the Secure Store Application. Highlight the new application on the Secure Store Admin page, and then select Set Credentials.

Browse to the same .pfx certificate file used for the client preauthentication when configuring the Web Application Proxy publishing rule and supply the password used to encrypt the file. Be aware that the password is not validated at this point, so be extra careful when typing it.



SharePoint Online search configuration

After the SharePoint web application has been securely published and the Secure Store Target application has been created and configured, the next step is to configure the user search experience in SharePoint Online. In a similar way to the on-premises approach, we use a Result Source to define the source of the search results and a Query Rule to determine when the result source is called. Because we have fully documented these steps for the outbound hybrid search experience, here we will focus on just the differences between the two configurations.

Result source

There are two elements that are different for the Result Source configuration. Again, as with on-premises, we can create result sources at the site, site collection, or tenant admin level, but the changes are the same in all cases.

The first change is to the Remote Service URL. For inbound hybrid search, you need to set this to match the published external SharePoint web application endpoint.

Remote Service URL	https://intranet.contoso.com
Type the address of the root site collection of the remote SharePoint farm.	

The second change is to the Credentials Information used to connect to the remote index location. We need to choose the Secure Store Target Application ID (SSO Id) for the reverse proxy certificate preauthentication. In our example, we named the SSO Id Inbound Hybrid.

Credentials Information

If you are connecting to your intranet through a reverse proxy, please select and enter the SSO Id of the Single Sign On entry which stores the certificate used to authenticate against the reverse proxy.
Else use the Default Authentication to authenticate against the remote SharePoint location.

☐ Default Authentication

☒ SSO Id

Reverse proxy certificate (Secure Store Id)

Inbound Hybrid

Query Rule

For the Query Rule configuration, nothing changes. When defining the Query Rule you select the On Premises results source to query against, but all other configurations remain the same.

Testing outbound search hybrid

Testing is the same as the inbound scenario. In this case, the result block should show the on-premises search results, and the main body will show the SharePoint Online search results.

Configuring bidirectional hybrid search

After you have configured both the outbound and inbound hybrid search scenarios, you are automatically placed in the third hybrid

topology: bidirectional, as illustrated in Figure 2-2.

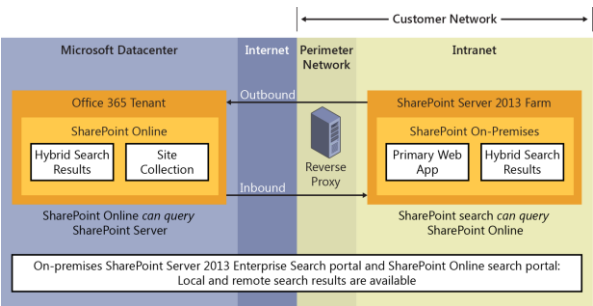


Figure 2-2: Representation of the two-way (bidirectional) hybrid search topology, showing both inbound and outbound query flows.

This means that there is no additional configuration required at this point to provide a rich search experience for your users. Wherever a user submits a search request, whether in SharePoint Online or in on-premises, she can get search results from both places in a single results page. The remote results are typically displayed in result blocks but you also can configure them as separate search verticals.

The main limitation of these query federation-based hybrid search experiences is the lack of a single unified result set, which can lead to a somewhat disjointed user experience. For example, the refinement pane is not driven by

search results from both local and remote indexes, and this can be confusing for the user. Also, there is no ranking across the two result sets; each set is ranked in accordance to the output from its own source index.

To address these gaps in the experience Microsoft embarked on developing a new Hybrid Search Experience, one which is based on a single unified search index and eliminates the need for separate results blocks or search verticals within the user experience.

Configuring Cloud Search Service Application

Hybrid search makes finding content easy, wherever the content lives. A company has a hybrid environment if its content and applications are spread across on-premises and Office 365. To complement the existing query federation–based hybrid search solution with SharePoint 2013 and Office 365, a new capability in the product has been introduced that makes it possible for customers to implement a crawl-based solution. By taking advantage of this new cloud hybrid search model, your users can

experience a more holistic joined-up search experience. Plus, as a business there are significant gains to be made in reducing the complexity, management, and operational overhead involved with running an on-premises SharePoint search service. Some of the benefits are highlighted here:

- Users of the search service will get a set of unified search results that includes ranking and refinement across the entire search corpus.
- Businesses can develop rich search-driven portals based on indexed content from multiple sources, including sources not normally available to SharePoint Online search, such as line-of-business (LoB) applications, by crawling the external content defined in the Business Connectivity Service model.
- The Cloud Search Service Application can support crawling of all existing SharePoint Server content sources.
- As Microsoft introduces new experiences in the SharePoint Online services, your users will automatically benefit without your organization having to update your on-premises SharePoint servers.

- As the search index is now located in the cloud, so the footprint of your SharePoint Server farm on-premises will be much smaller than earlier. The consequence of a smaller farm is significant reduction in the total cost of ownership for the search feature.
- Version to version migration of SharePoint server search on-premises involves migration plus recrawling all of the content. With the index now located in SharePoint Online, this complex procedure is no longer required, thereby reducing the operational cost of the on-premises deployment.
- As content is migrated from on-premises to Office 365, the search experience for that content will be seamless. The hybrid Cloud Search Service Application will automatically remove items as they are migrated out of the on-premises farm into SharePoint Online, where the Office 365 search service will automatically detect and index them. This provides an optimal search experience for the end user.
- The cloud hybrid search solution also influences what users can search for and see in Delve. In the preview version of cloud hybrid search, Delve will make it possible for

users to see search results from on-premises as well as Office 365. Gestures such as adding an item to a board will work just the same for on-premises content as for Office 365 content. On premises content from SharePoint will also show up as activity on the Me page or a person page in Delve.

Even though the existing query-based model of inbound and outbound hybrid search continues to be supported, this new hybrid solution brings numerous new capabilities into the hybrid sphere. The new hybrid solution takes away the complexities of incoming query via Reverse Proxy to SharePoint on-premises environment. As a result, this takes away the need for a second public SSL certificate, which was required for inbound authentication requests from Secure Store Applications in SharePoint Online. The infrastructure requirements for configuring cloud hybrid search are discussed later in this content. Figure 2-3 presents a representation describing the query and crawl flow in hybrid search. The figure also illustrates how you can use regular Search Service Application publishing and consumption to extend the reach of the hybrid Cloud Search Service Application to downstream SharePoint versions.

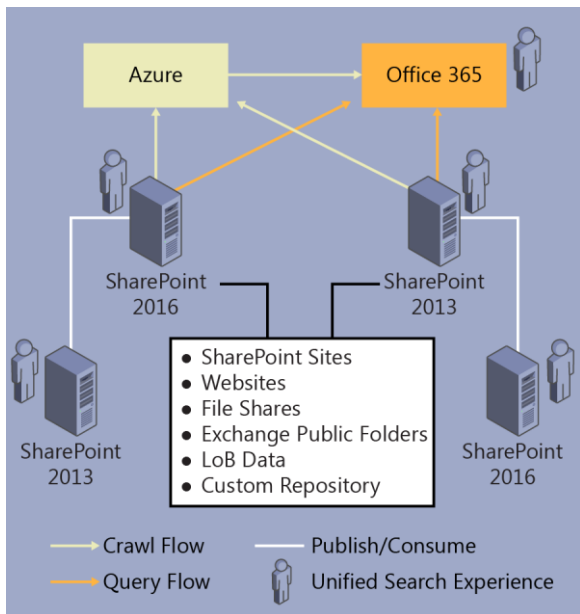


Figure 2-3: Representation of the Cloud Search Service Application experience showing crawl and query flow, search experience, and service application federation.

Cloud hybrid search is available with both of these solutions:

- In the August 2015 Public Update (PU) for SharePoint Server 2013
<http://support.microsoft.com/kb/3055009>

- In SharePoint 2016
<https://www.microsoft.com/download/details.aspx?id=51493>

The cloud hybrid search solution provides the ability to crawl and parse on-premises content. This parsed content is then processed and added to the search index in Office 365. When users query the search index in Office 365, they get search results from both on-premises and Office 365 content.

The crawling configuration, including that of the search service application, content sources, crawl rules, and so on is carried out in the on-premises environment. Modifications to search experiences—for examples search schema changes—are performed at the Office365 level.

By deploying the cloud hybrid search solution, customers can finally achieve the benefits of a unified index and search experience spanning on-premises and online content in a single result set.

You can review the roadmap for configuring hybrid capability at
<https://technet.microsoft.com/library/dn197168.aspx>.

Configuring the Cloud Search Service Application

As with the classic inbound and outbound hybrid solutions, the Cloud Search Service Application has a set of requirements that you must configure to achieve a successful implementation.

1. Synchronize users and groups from on-premises to Office 365 Azure Active Directory.
2. Install onboarding prerequisites.
3. Create Cloud Search Service Application.
4. Execute onboarding script.
5. Create on-premises content sources.
6. Configure outbound query federation.

It is assumed that you've already completed step 1 and that the Azure Active Directory associated with the SharePoint Online Tenant is correctly populated. There are some nuances to the relationship between crawling via the Cloud Search Service Application and the Directory

Synchronization process, which can trip up the administrators and cause some confusion among your users. These nuances will be examined in Chapter 8, but for now let's assume that everything is in place and the directory is fully synchronized before we begin crawling.

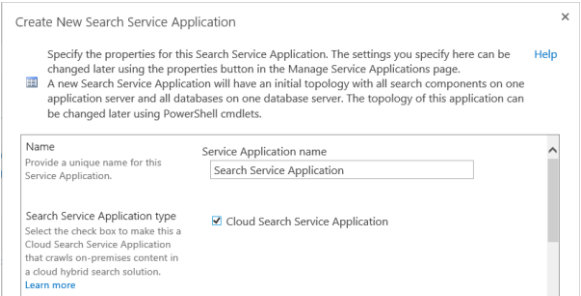
Step 2 is similar to the prerequisites installed for deploying Azure AD Connect; however, here the components are deployed to one of the SharePoint servers in the farm. The suggestion is that it is installed on the same server that hosts Central Administration to maintain all the administrative tools in the same place.

You can create a Cloud Search Service Application by using the Central Administration Search Service Application creation wizard, or you can create one by using Windows PowerShell.

Creating a Cloud Search Service Application via Central Administration

To create a Cloud Search Service Application, start the SharePoint Server on-premises Central Administration site, navigate to the Service Applications section, and then, on the ribbon,

select New. When the Create New Search Service Application page opens, select the Cloud Search Service Application type in the parameters interface.



Create New Search Service Application

Specify the properties for this Search Service Application. The settings you specify here can be changed later using the properties button in the Manage Service Applications page. [Help](#)

A new Search Service Application will have an initial topology with all search components on one application server and all databases on one database server. The topology of this application can be changed later using PowerShell cmdlets.

Name
Provide a unique name for this Service Application.

Service Application name
Search Service Application

Search Service Application type
Select the check box to make this a Cloud Search Service Application that crawls on-premises content in a cloud hybrid search solution. [Learn more](#)

☒ Cloud Search Service Application

A Cloud Search Service Application has a special property, CloudIndex. When you select the Cloud Search Service Application check box, it sets CloudIndex to true. CloudIndex is a read-only property of a deployed Search Service Application, and as such, you cannot set it post creation. By definition, this also implies that an existing regular Search Service Application cannot be converted to a Cloud Search Service Application after creation.

The property value for a Search Service Application can be checked by running the Windows PowerShell command (get-spenterprisesearchserviceapplication).cloudindex , as demonstrated here:

```
PS C:\> (get-spenterprisesearchserviceapplication).cloudindex  
True
```

```
PS C:\>
```

Creating a Cloud Search Service Application via Windows PowerShell

You can create a Cloud Search Service Application by executing a Search Service application creation Windows PowerShell script and setting the CloudIndex property to true. Later, when we connect the Cloud Search Service Application to the Office 365 Search Content Service, another property, the IsHybrid property is set to 1. This process is referred to as *onboarding*.

A sample Windows PowerShell cmdlet is shown here with the -CloudIndex property set:

```
New-SPEnterpriseSearchServiceApplication -Name  
$SearchServiceAppName -ApplicationPool $appPool  
-DatabaseServer $DatabaseServerName -CloudIndex  
$true
```

The two new properties serve two purposes:

- The CloudIndex property turns off the normal ContentPlugin

- The IsHybrid initializes AzurePlugin so that the content is batched in preparation to be pushed to Azure

SharePoint administrators are free to use their own script to generate the hybrid Cloud Search Service Application and scale-out as long as they set these properties. Microsoft has provided a sample set of scripts on the Microsoft Download center site at <https://www.microsoft.com/en-us/download/details.aspx?id=51490>.

After the Cloud Search Service Application has been created, the administrator is encouraged to validate the deployment by using a Windows PowerShell approach similar to the following script:

```
Add-PSSnapin Microsoft.SharePoint.Powershell

$ssaname = "Cloud Search Service Application"
$ssa = Get-SPEnterpriseSearchServiceApplication
$ssaname
Get-SPEnterpriseSearchTopology -Active -
SearchApplication $ssa
Get-SPEnterpriseSearchStatus -SearchApplication $ssa
-Text |ft Name, state,Partition,Host -AutoSize
$ssa.CloudIndex
```

The expected output is a list of Search Service Application components showing status online, and the CloudIndex property of the Search Service Application showing true.

```

TopologyId      : 38099df4-8da0-4c1a-9df8-ae727190f7b0
CreationDate    : 7/29/2015 12:23:00 AM
State           : Active
ComponentCount  : 6

Name           : IndexComponent1
State          : Active
Primary        : True
Partition      : 0
Host           : sp16

Name           : Cell:IndexComponent1-SP56859a39cc17I.0.0
State          : Active
Primary        : True
Partition      : 0

Name           : Partition:0
State          : Active

Name           : AdminComponent1
State          : Active
Host           : sp16

Name           : QueryProcessingComponent1
State          : Active
Host           : sp16

Name           : ContentProcessingComponent1
State          : Active
Host           : sp16

Name           : AnalyticsProcessingComponent1
State          : Active
Host           : sp16

Name           : CrawlComponent0
State          : Active
Host           : SP16

True

```

Note Only one Cloud Search Service Application is allowed per SharePoint Server Farm; however, you can have multiple non-Cloud Search Service Applications in the same SharePoint 2013 or 2016 farm. These Search

Service Applications should not share any topology services.

Here are some key considerations when deploying and scaling-out the Cloud Search Service Applications:

- To deploy the Cloud Search Service Application, at least one of each component is required, but not all are actually used.
- Deploying additional crawlers will provide high availability for the crawler function.
- Adding query processors will also provide high availability when the on-premises farm is configured to send search queries to Office 365.
- Content processing is performed in the Office 365 service, so there is no requirement for additional content processors on-premises.
- Regardless of the number of items crawled by the Cloud Search Service Application, there is no requirement for additional index components. The index is stored in the Office 365 search farms, which saves a significant amount of on-premises capacity and capital outlay for large corpuses.

- You must scale the on-premises crawl databases to match the number of items crawled because the Cloud Search Service Application must maintain an up-to-date crawl log of the items crawled.

Scaling-out employs the same processes as a regular Search Service Application; follow the steps at

[https://technet.microsoft.com/library/jj862356\(v=office.15\).aspx#Topology_ExampleDefaultSmall](https://technet.microsoft.com/library/jj862356(v=office.15).aspx#Topology_ExampleDefaultSmall).

After you have the Cloud Search Service Application configured the way you want it, the next step is to complete the onboarding process. This process wires up the connectivity between the on-premises farm and two services running in the Microsoft Cloud.

The first of these services is the Office 365 tenancy, and the onboarding process simply carries out the configuration steps that might have already been done if you have previously configured your on-premises farm with a hybrid workload.

The second service is the Search Content Service, and this is the feature that really drives this new world of hybrid search experiences

Search Content Service

Search Content Service is a service hosted in Azure, which provides storage for SharePoint content intended for use in Search and Graph scenarios. Search Content Service acts as an intermediary for several scenarios for which the number of sources and targets varies. Search Content Service is the core technology behind the Cloud Search Service Application and routes data from SharePoint crawlers, either in SharePoint Online or SharePoint on-premises, to either one or more SharePoint Online search farms and to the Office Graph.

Search Content Service was developed with the following goals:

- Clients submitting Content Insert/Update/Delete operations. Set of clients:
 - SharePoint Online crawlers.
 - On-premises SharePoint (Cloud Search Service Application in SharePoint Server 2013 and SharePoint Server 2016)
- Route data from SharePoint crawlers, either in SharePoint Online or on-premises to:

- One or more SharePoint Online search farms
- The Office Graph
- Provide ways to redistribute data based on capacity needs.
- Ability to refeed crawled content. Quick refeeding of content provides disaster recovery features and supports reprocessing when document processors or schema have changed.

At this point, it is worth reviewing a high-level architectural overview of the Search Content Service. Figure 2-4 shows that both SharePoint Online and SharePoint on-premises use the endpoints to feed batches of content into the indexing API which ultimately queues and processes the data before handing it off to the search farm for content processing. Content in the Search Content Service is stored in an encrypted format in Azure Blob Storage.

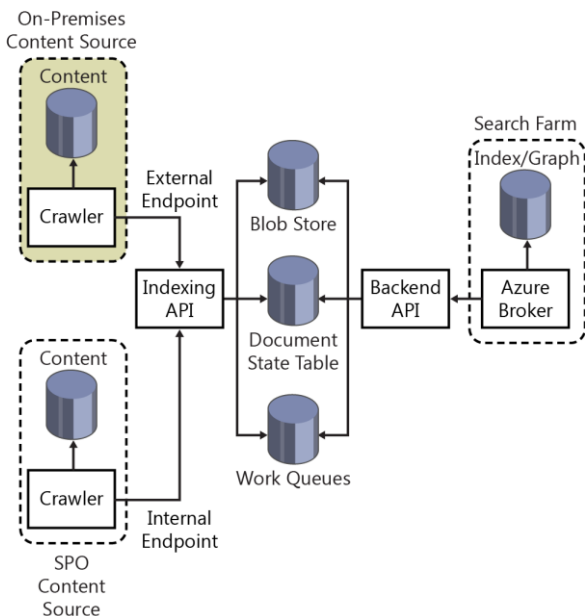


Figure 2-4: Schematic representation of the connections from content farms to the search content service and the Office 365 search farm.

Completing the onboarding process

Onboarding consists of several stages and is implemented by running the `OnBoardHybrid-Search.ps1` Windows PowerShell script on a SharePoint Server in the farm, supplying

parameters for the Tenant URL and optionally the Cloud Search Service Application name. The script is also available at

<https://www.microsoft.com/download/details.aspx?id=51490>.

Onboarding stages

There are four keys stages to the onboarding process

- **Get-HybridSSA** This stage validates that the Cloud Search Service Application name supplied as a parameter to the script execution is valid. If multiple Search Service Applications are found and no parameter is supplied, it attempts to validate a Search Service Application that has the IsHybrid property set to 1.
- **Prepare-Environment** This stage checks that the prerequisites for deployment are installed. It checks for MSOnline Single Sign-In Client and for Windows PowerShell. If either of these tools is missing, the script will exit with a prompt to install them.
- **Connect-SPFarmToAAD** This completes the OAuth trust configuration with Azure Access Control Services (ACS) and deploys the ACS Proxy. Additionally, it deploys a new

SPO connection proxy so that the farm can communicate with the external endpoint of the Azure Search Connector Service (SCS).

- **Add-ServicePrincipal** The final stage adds the Office 365 Service Principal ID to the local farm and sets the correct Service Principal Name in Azure Active Directory for the On Premises URL. This ensures that outbound query federation can succeed between the Office 365 tenant and the on-premises farm.

The process completes by settings some additional parameters on the Cloud Search Service Application.

Important Before running the Onboard-Hybridsearch.ps1 script, you should close all open Windows PowerShell sessions including PowerShell ISE and PowerShell cmd windows.

To run the onboarding process, run the following script:

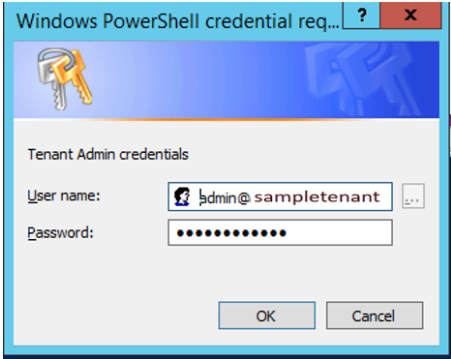
```
.\Onboard-CloudHybridSearch.ps1 -CloudSSAid "Cloud Search Service Application" -PortalUrl https://contoso.sharepoint.com
```

Output from executing the OnboardHybrid-Search.ps1 looks similar to the following: Note, that on a SharePoint 2016 minrole server the

SharePoint Server Search service may not be running on the same server where the script is executed, resulting in an error message. This can be safely ignored, however the SharePoint Server Search service should be restarted on the appropriate servers in the farm.

```
PS C:\scripts> .\Onboard-HybridSearch.ps1 -PortalUrl https://sampletenant1234.sharepoint.com
Configuring for SharePoint version 15.
Accessing Hybrid SSA...
Using SSA with id aa40e25b-909c-4e65-aa4d-cef5e5e69063.
Preparing environment...
Found Office Single Sign On Assistant!
Found AAD PowerShell!
Configuring Azure AD settings...
Restarting MSO IDCTL Service...
Service Restarted!
Connecting to O365...
```

When the message Connecting To O365 appears, you are prompted to sign in using a tenant Global Administrator account.



The next stage of execution shows connecting to the ACS Endpoint. If a message similar to the printscreen in the image that follows indicates that Signing Credential already exists, this means


```
Done connecting!
Connecting to content farm in SPD...
Preparing tenant for hybrid...
PreparePushTenant was successfully invoked!
Getting service info...
Registered hybrid configuration:

TenantId           : 53647484-fbd0-42e3-883c-66e552f81bd2
AuthenticationRealm : 53647484-fbd0-42e3-883c-66e552f81bd2
EndpointAddress    : https://msitfrontendexternal.search.msit.us:traffictmanager.net:443/

Configuring Service Principal...
Service Principal already registered, containing the correct SPN.
Configuring Hybrid SSA...
Restarting search service...
All done!

PS C:\scripts>
```

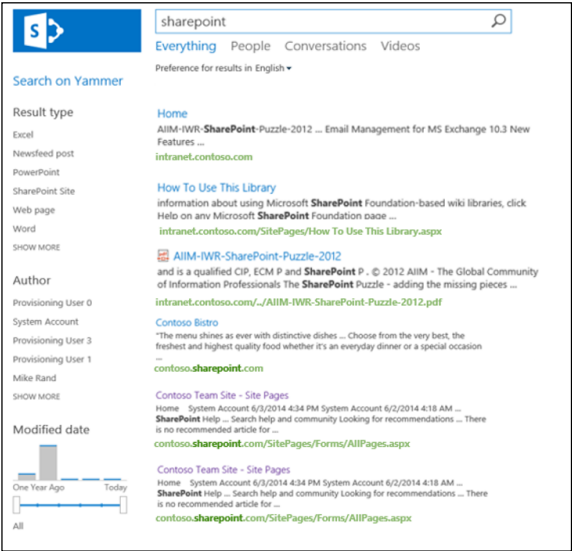
In the preceding screenshot you can see the TenantID, Authentication Realm, and the connected endpoint address.

At this point, onboarding is complete.

Searching from Office 365 with the Cloud Search Service Application

When onboarding is complete, of course the first thing to do is run a full crawl of the on-premises content in order to feed the search index. After this is done, the user can search from Office 365 and obtain search results from the SharePoint Online sites and the on-premises sites. The screenshot that follows shows just such a search results page with on-premises and SharePoint Online content mixed within the same set of

results. The ranking of the results and the refinement panel apply across the entire search corpus, leading to a much improved user experience.



Configuring content sources on-premises

Content sources in the Cloud Search Service Application are no different from content sources in a regular enterprise Search Service

Application. Follow the steps in <https://technet.microsoft.com/library/jj219808.aspx> to create and manage content sources in the Cloud Search Service Application. You can find additional information on good practices for configuration of content sources in Chapter 8.

Configuring outbound query federation on the Cloud Search Service Application

By default, deploying the Cloud Search Service Application only configures the crawling connection from SharePoint on-premises to SharePoint Online. This makes it possible for users in Office 365 SharePoint Online to see search results from both on-premises and SharePoint Online. For on-premises users to see the full set of search results, you must configure outbound hybrid search query Federation in the same way you did for the first hybrid search scenario described earlier in this chapter.

Managed property for hybrid search results

There is a new managed property that has been defined for all content passing through the Search Content Service. For non–SharePoint Online crawled content, the managed property `IsExternalContent` is set to 1, giving us the ability to use this property selectively to identify the externally crawled content.

PROPERTY NAME	TYPE	MULTI	QUERY	SEARCH	RETRIEVE	REFINE	SORT	SAFE	MAPPED CRAWLED PROPERTIES
<code>IsExternalContent</code>	Yes/No	-	Query	-	Retrieve	Refine	Sort	Safe	<code>IsExternalContent</code>

You can use the property to restrict a query for online/on-premises results, as a refiner or in a result source. For example, you can use the default result source using Local SharePoint results, but you can rename it to "Everything" in the Search Navigation configuration. It uses Local SharePoint results plus a filter on which sites to include in the search results.

This managed property becomes very important when considering the people crawl scenario. By default, all people in the SPO User Profile application will be indexed by the SharePoint Online search service. If you additionally crawl people from the on-premises Cloud Search Service Application, you will generate a duplicate set of indexed people content in the Office 365

Search Service. This will be confusing to users because searching for a person will return multiple results.

There are two ways to approach this problem today:

- Make Office 365 User Profile service the primary source of user information and let Office 365 search take care of the indexing and presentation. With this approach, you do not need to crawl people on-premises.
- Crawl the on-premises people profile store in addition to Office 365 crawling the tenant profile store. This will result in the described scenario of duplicate search results for each person; however, you can use query transformation to decide which results you want to display. Even providing the ability for users to choose between the different result sources at query time.

Businesses that have a richly populated on-premises profile store, perhaps with additional augmentation from LoB applications, might want to maintain their primary source of people information as this store. To avoid duplicate search results and to focus the results on the primary store, you must implement query transformation.

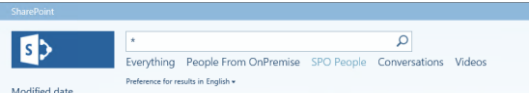
To utilize the on-premises profile store as the primary people search source, you should follow these steps:

1. Create a new result source or copy the existing people results source.
2. Edit the new result source and modify the Query Transformation box to include the Managed Property IsExternalContent, as shown here:

```
{?{searchTerms} ContentClass=urn:content-class:SPSPeople IsExternalContent:1}
```



3. Create a new search results page and configure the Core Search Results web part to consume this new search result source.
4. Complete the implementation by adding the new page to the search navigation settings. This will add the new page as a search vertical within the search center, as per the following screenshot:



To utilize the Office 365 profile store as the primary people search source, you should follow the same steps but use a slightly different query transformation at step two, as follows:

```
{?{searchTerms} ContentClass=urn:content-class:SPSPeople NOT IsExternalcontent:1}
```

Note The difference in the two transforms is the insertion of NOT before the managed property to force the exclusion of External content, i.e., non–Office 365 people results.

For people results transformation, you can make a copy of the built-in people result source and modify it to include the IsExternalContent managed property restriction for filtering against Online or on-premises people sources.

For on-premises people:

```
{?{searchTerms} ContentClass=urn:content-class:SPSPeople IsExternalcontent:1}
```

For Online people:

```
{?{searchTerms} ContentClass=urn:content-class:SPSPeople NOT IsExternalcontent:1}
```

Summary

This chapter presented a story of the evolution of SharePoint Server and Office 365 Search-driven hybrid scenarios. From simple query-driven federation in outbound hybrid search to the more complicated and infrastructure-dependent inbound hybrid search setup. Finally, settling on the newest member of the search hybrid family, the Cloud Search Service Application that finally gives users the single unified search index they have been seeking and the ability to deliver not just silos of search results on a page, but a truly holistic end-to-end search-driven experience from all the crawled content across multiple repositories, both online and on-premises.

Hear about it first.



Get the latest news from Microsoft Press sent to your inbox.

- New and upcoming books
- Special offers
- Free eBooks
- How-to articles

Sign up today at
MicrosoftPressStore.com/Newsletters



Business Connectivity Services hybrid

In this chapter, you will learn what Microsoft SharePoint Business Connectivity Services offers in a hybrid context, its usage scenarios, authentication flow, and configuration in a sample on-premises application. We cover what are the requirements for a BCS hybrid solution with step-by-step procedures on the configuration process. This chapter requires the use of Microsoft Visual

Studio, and adequate screenshots with explanation have been provided here—enough to get you right through the process of configuring BCS hybrid.

Overview of Business Connectivity Services hybrid

A Business Connectivity Services (BCS) hybrid solution makes it possible for organizations to securely publish internally hosted business application data, commonly referred to as line-of-business (LoB) data to SharePoint Online. Your mobile workers, traveling workforce, and external partner organizations can securely consume and interact with the data that resides on your internal corporate network without the need for you to migrate or replicate data across network boundaries.

Using BCS, your internal users can publish on-premises data to a list or application external in

SharePoint Online. With BCS hybrid, users can create, read, update, and delete items in an external list across both SharePoint Online and SharePoint on-premises. Your LoB data can exist in its current location without moving it out to a perimeter or external network. A requirement is that the on-premises SharePoint must have an existing BCS configuration set up.

BCS hybrid uses the on-premises BCS services to connect to the LoB data and then, through a reverse proxy, securely publish it through a Client-Side Object Model (CSOM) endpoint out to the BCS services in SharePoint Online. BCS hybrid currently only connects through an Open Data Protocol (OData) source. OData is an open web protocol for querying and manipulating data with Create, Read, Update, and Delete (CRUD) operations.

Simply put, BCS hybrid connects to the SharePoint on-premises farm and in turn, connects to the on-premises OData service URL that connects and exposes the LOB data with which users can interact.

Note Because an OData connection is a requirement for your BCS hybrid connection, it is not possible to reuse any Business Data Connectivity (BDC) connections that were established through SharePoint Designer.

SharePoint Designer does not have the capability of creating BDC models from an OData source. You will need to use tools like Visual Studio to create the OData service.

An OData client accesses data provided by an OData service by using standard HTTP. The OData protocol largely follows the conventions defined by REST, which define how you use HTTP verbs such as GET, POST, PUT, DELETE.

More info To read more about OData, go to <https://msdn.microsoft.com/data/hh237663>.

BCS hybrid with Microsoft Azure SQL

Some organizations that already have their data on Azure SQL, have the option of exposing this data directly to SharePoint Online. Microsoft has made it easy to set up the external content types between SharePoint Online and Azure SQL databases. This is done through SharePoint Designer's SQL Data source type without the need for using Visual Studio and working with OData. After all the permissions are set up correctly and the configurations made, you can add databases from Azure SQL as external lists on SharePoint Online.

More info To read more about how to configure an external list on SharePoint Online that consumes data from SQL Azure, go to <http://social.technet.microsoft.com/wiki/contents/articles/28286.office-365-sharepoint-online-bcs-with-azure-sql-server-database.aspx>.

BCS hybrid flow

To understand BCS hybrid, you need to go through the flow to see what it entails, such as authentication, presentation of data, and components involved in presenting that data, as illustrated in Figure 3-1. Understanding this will make BCS hybrid more meaningful and help in troubleshooting and administration.

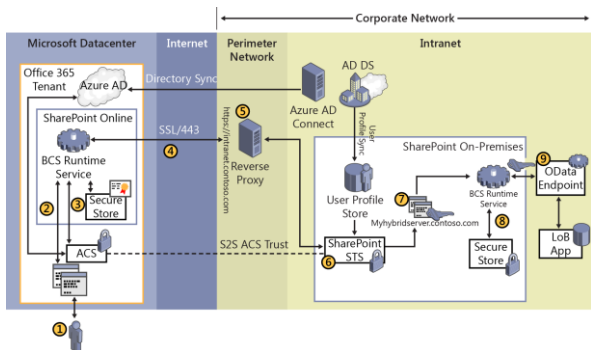


Figure 3-1: BCS hybrid flow diagram.

1. A user that requires content from the LoB application, signs in to SharePoint Online as a federated or synchronized user and opens an online app or external list on SharePoint Online.
2. The online app or external list sends a request to BCS online for the data. BCS determines the data source and credentials required by looking up its imported data models and connection settings. BCS online differs a little from BCS on-premises by the requirement to specify the OData connection settings in a separate setting within BCS online.
3. BCS retrieves the identification certificate with a purpose of client preauthentication against the reverse proxy from the online Secure Store Service. This certificate is configured when setting up the online Secure Store Service. This certificate is used for authentication from SharePoint Online back to the on-premises reverse proxy and SharePoint on-premises farm.

Additionally, BCS retrieves an OAuth token containing the user's credentials from the Azure Access Control Service (ACS) and is used for authenticating to the SharePoint on-premises farm.

4. BCS online sends a HTTPS request to the published endpoint for the data source. This HTTPS request contains the following:
 - The client authentication certificate from the online Secure Store Service for preauthentication purposes with the reverse proxy
 - The user's OAuth security token
 - A request for the data.
5. The reverse proxy authenticates the request by using the client certificate and forwards the HTTPS request to the CSOM pipeline of the SharePoint on-premises farm.
6. SharePoint on-premises retrieves the user's identity from the OAuth security token in the HTTPS request and attempts to match it to an identity in the on-premises User Profile Service. If a match exists, the user's on-premises credentials are returned to the HTTPS request. The matching process is performed on the user's security identifier (SID) first and then a soft match is performed on the user's User Principal Name (UPN), Simple Mail Transfer Protocol (SMTP), and Session Initiation Protocol (SIP) settings, if necessary.

Note When a user signs in to SharePoint Online, the user is authenticated by ACS. ACS issues an OAuth security token, which represents the user to all SharePoint Online processes and objects that the user tries to access. This security token is embedded in the request for external data and passed, along with the client authentication certificate, to the reverse proxy.

7. The user's on-premises credentials are used to authenticate to the SharePoint on-premises site that is configured for inbound hybrid requests and published by the reverse proxy; for example, <https://intranet.contoso.com>. The request is then passed to the SharePoint on-premises BCS service.

Note User's domain credentials is another security token that represents the user in the on-premises Active Directory domain. In a SharePoint BCS hybrid scenario, it is used to authenticate the user to SharePoint on-premises and to access all other on-premises resources as that user. This depends, of course, on the BCS Secure Store in play on the internal site. If you are using Secure Store group credentials or a fixed account, the content is

not accessed as the user, but as the group or the fixed account.

8. The SharePoint on-premises BCS retrieves the credentials in the form of a security token that are used to the Secure Store service application, which in turn provides credentials for access to the OData source.
9. The SharePoint on-premises BCS service passes the request for data along with the data access credentials to the OData endpoint, which then performs the desired operations on the external data. The request is authenticated by OData endpoint which, in our example, is Internet Information Services (IIS), and the results are returned to the SharePoint Online user.

Prerequisite Steps for Configuring SharePoint BCS hybrid

The following are the prerequisites that are required to be set up prior to configuring your SharePoint BCS hybrid environment.

For all the scenarios in this chapter, the following assumptions have been made.

1. The company's on-premises domain has been added to the O365 tenant.
2. Azure Active Directory Connect (Azure AD Connect) has been configured with or without password synchronization.
3. If password synchronization has not been enabled, then Active Directory Federation Services (AD FS) has been deployed to support user sign-in to Office 365.

More info You can find details for the preceding steps in the free eBook, *Planning and Preparing for Microsoft SharePoint Hybrid*.

To download the e-book, go to

https://blogs.msdn.microsoft.com/microsoft_press/2016/04/26/free-ebook-planning-and-preparing-for-microsoft-sharepoint-hybrid.

4. An S2S trust has been set up between SharePoint Server on-premises and Microsoft Office 365, using Azure ACS as the trust broker. You can configure this trust either manually as detailed in Chapter 1, or it might already be in place if you have used the SharePoint Online Hybrid picker to deploy Microsoft OneDrive or Hybrid Sites features.

5. A SharePoint site collection has been chosen and is published via a reverse proxy. This is identical to what hybrid search requires. The choice of reverse proxies might differ from one organization to another, but Microsoft's Web Application Proxy server has been chosen in this book along with the configuration steps in Windows PowerShell. Refer to the following subsections in the section "Configuring inbound hybrid search" in Chapter 2:

- Publishing the SharePoint On-Premises Web Application by using client certificate preauthentication
- Configuring Web Application Proxy

The main thing is to note here is that preauthentication occurs with the client certificate to ensure that the published endpoint is secure.

SharePoint farm configuration

You will need to check a few things on your SharePoint on-premises farm before you begin configuring for BCS hybrid. The following points will help with the your checks:

- A Managed Metadata Service Application configured and the service instance running

- A configured user profile service application that has been synchronized and the user profile store contains the same users that are synchronized to Azure Active Directory. The corresponding users that have been synchronized to Office 365 must have a valid Office 365 subscription license assigned to them.

This is used by the STS service that uses the metadata from the User Profile Service Application to construct security tokens for gaining access to hybrid resources.

- A BCS solution using OData to connect to the LoB.

For example, for a SQL database, an OData service endpoint hosted as a web service would look like

<https://odata.contoso.com/AdventureWorks.svc>.

OData source

You need to confirm that the OData service endpoint has been configured and is available; for example,

<https://odata.contoso.com/AdventureWorks.svc>.

More info To create your own OData source and endpoint, you could try using the AdventureWorks sample database. To download the AdventureWorks database 2012, go to <http://msftdbprodsamples.codeplex.com>.

To learn how to create an ASP.NET Windows Communication Foundation (WCF) Data Service to expose the AdventureWorks sample database, go to <https://msdn.microsoft.com/library/office/jj163810.aspx>.

Note You might encounter issues querying the AdventureWorks database 2012 on SQL Server 2014 for which you will have to change the compatibility level in SQL to SQL Server 2012 (110).

Validate the prerequisites

The following steps help to validate that the prerequisites are in place and you are ready to proceed further with configuration:

1. Verify that your public Internet domain name can be resolved in DNS; for example, intranet.contoso.com.

2. Verify that you can connect to the primary web application by using both the internal and external URLs; for example, `https://intranet.contoso.com`
3. To verify that your reverse proxy endpoint is successfully configured and ready for client preauthentication, validate by navigating to your externally published URL such as `https://intranet.contoso.com` from an external web browser with Fiddler2 loaded to inspect the web traffic. Figure 3-2 shows that Fiddler2 displays the Client Certificate Requested message box, which confirms that a certificate challenge was received. No further steps are necessary in this validation step.

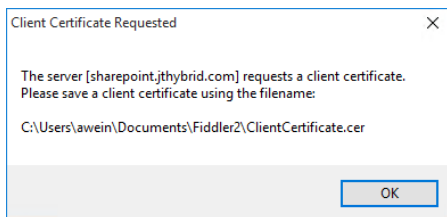


Figure 3-2: Fiddler being challenged to produce the client certificate for preauthentication with the reverse proxy.

Configuring SharePoint BCS hybrid

After the prerequisites have been completed, you must perform the following steps to configure SharePoint BCS hybrid. We will go through all the steps in sequence. It is advised to record your configuration information (such as names of services) as you progress with the configuration steps, especially if you deviate from the names suggested here.

SharePoint Online Secure Store Service configuration

You need to set up a secure store target application in SharePoint Online. This target application is used to store the certificate for client preauthentication.

Note This target application is also referred to as the Secure Channel Target Application in some TechNet documentation. For this reason, we will refer to it as “Secure Channel” in this chapter. You can use any name you prefer.

1. Sign in to the SharePoint Admin Center with administrator rights.
2. Click Secure Store, and then click New.

3. In the Target Application ID box, type **SecureChannelTargetApplication**.

The ID can be anything you want, but note that it should not contain any spaces. You will need to use this same ID at a later stage in the configuration.

4. In the Display Name box, type **Secure Channel Target App**.
5. In the Contact E-mail box, provide an address and leave the target application type as Group Restricted.
6. In the Credential Fields section, replace any text in the field name of the first row with **Certificate**.
7. In the upper Field Type box, select Certificate.
8. If you have a .pfx certificate as your preauthentication certificate, you would need to replace any text in the field name of the second row with **Certificate Password**.
9. In the lower Field Type box, select Certificate Password, as illustrated in Figure 3-3.

Note You can delete the second row if you have only a .cer certificate to work with as your secure channel certificate.

Credential Fields

Enter the credential fields. The maximum number of fields enabled is 10. The field names cannot be edited later. To add a new field, click the "Add Field" button

FIELD NAME	FIELD TYPE	MASKED	DELETE
Certificate	Certificate	☐	X
Certificate Password	Certificate Password	☒	X
Add Field			

Figure 3-3: Configuring the certificate and password for a .pfx preauthentication certificate in the Secure Store Service Online.

- 10. In the box in the Target Application Administrators section, type the list of users who need to manage the Target Application settings, as demonstrated in Figure 3-4.
- 11. In the Members section, add the users and groups that are mapped to the credentials defined for this target application; for example, Everyone Except External Users is available as a default group in SharePoint Online.

Target Application Administrators

The list of users who have access to manage the Target Application settings.

Jeremy Taylor; Jeremy P Taylor; Jeremy Taylor;

Members

The users and groups that are mapped to the credentials defined for this Target Application.

Everyone except external users;

Figure 3-4: Configuring target application administrators and using Everyone Except External Users as members.

12. Click ok.

After you create it, you will see the Target Application ID called SecureChannelTargetApplication in the SharePoint Online Secure Store Service.

13. Select the Target Application ID check box, and then click, on the ribbon, in the Credentials group, click Set, as depicted in Figure 3-5.

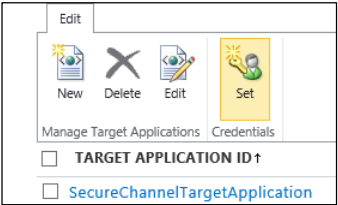


Figure 3-5: Set Credentials on the SecureChannelTargetApplication in the Secure Store Service Online.

14. After you upload your certificate and the password, click Ok to complete the Secure Store Service target application ID configuration.

Figure 3-6 presents the credentials in this screen, which are the certificate and certificate password that would be used for the client preauthentication process.

NAME	VALUE
Certificate	C:\SSL\contoso.com.pfx Browse...
Certificate Password	
Confirm Certificate Password	

Note: Once the credentials are set, they cannot be retrieved by the administrator. Any existing credentials for this credential owner will be overwritten.

Figure 3-6: Uploading the SSL certificate (contoso.com.pfx) with its password in Secure Store Service Online.

On-premises service account and security group creation

You would need to create a new service account and a security group in Active Directory on-premises by performing the following steps:

1. Create a new on-premises service account. This will access the OData service endpoint; for example, CONTOSO\ODataAccount.
2. Create a new on-premises global security group; for example, CONTOSO\ODataGroup.
3. Identify all users that will use the BCS hybrid solution. Ensure that they are federated accounts. Add them to the CONTOSO\ODataGroup.

4. Add the CONTOSO\ODataGroup as a Member of the SharePoint site to grant all the designated users access to the BCS hybrid solution.

On-premises Secure Store Target application configuration

Through the on-premises secure store service, users in the CONTOSO\ODataGroup access the OData service endpoint through only one account, the CONTOSO\ODataAccount

Here's how to create a target application:

1. On the Central Administration home page, in the Application Management section, click Manage Service Applications.
2. Click the Secure Store service application.
3. In the Manage Target Applications group, click New.
4. In the Target Application ID box, type a text string; for example, **ODataApp**.
5. In the Display Name box, type a name for the target application; for example, **ODataApp**.

6. In the Contact Email box, type a contact email address.
7. In the Target Application Type list box, select Group.

This indicates the mapping of many user credentials or a security group to one credential. In this case, the Target Application Page URL is not needed and automatically selects None.

8. Click Next.
9. On the Create New Secure Store Target Application page, for both Field Name and Field Type, accept the default values of Windows User Name and Windows Password, and then click Next.
10. In the Target Application Administrators box, add the Farm Administrators account and an account that has farm administrator rights.
11. In the Members box, add the domain security group you are using to control access to the BCS hybrid scenario solution; for example, ODataGroup.
12. Click OK.

Here's how to set credentials for a target application:

1. In the target application list, point at the target application that you just created (ODataApp), click the arrow that appears, and then, on the menu, click Set Credentials.
2. If the target application is of type Group, type the credentials for the external data source.

Depending on the information that is required by the external data source, the fields for setting credentials will vary.

3. If the target application is of type Individual, type the user name of the individual who will be mapped to this set of credentials on the external data source, and type the credentials for the external data source.

Depending on the information that is required by the external data source, the fields for setting credentials will vary.

4. In the Windows User Name box, type the account name for the account that will have access to the OData service endpoint in domain\username format; for example, CONTOSO\ODataAccount.

5. Type and confirm the password for that account, and then click OK.

On-premises Secure Store Service Application master key configuration

If you do not have a Master key configured in the Secure Store Service Application in your on-premises farm, you will need to perform the following steps:

1. Go to your on-premises Secure Store Service.
2. Ensure that there are no keys already configured. Confirm with a colleague or SharePoint farm administrator if you are unsure.
3. If no one has yet set up a key for the farm, click Generate New Key.
4. Type a passphrase, and then click OK

Ensure that you have recorded this passphrase in a safe place.

SharePoint Online site and App Catalog preparation

You can present the data either through a SharePoint Online external list or through an

add-in (app) for SharePoint. If you choose to use an add-in for SharePoint, you must also have a SharePoint Online App Catalog configured. In this book, we will present data through a SharePoint Online external list and not an add-in (app) for SharePoint.

More info To read more about turning on the App Catalog, go to <https://technet.microsoft.com/en-us/library/fp161236.aspx>.

SharePoint Online BDC Metadata Store permissions configuration

The BDC Metadata Store holds external content types, external systems, and BDC model definitions for the BCS Service Application. You will be required to configure permissions on the Metadata Store for users to be able to access the external content types.

To set permissions on the BDC Metadata Store in SharePoint Online, perform the following steps:

1. Open the SharePoint Online Admin Center by using an administrative account.
2. In the navigation pane on the left, click “bcs,” and then click Manage BDC Models And External Content Types.

3. Click Set Metadata Store Permissions, and then add All Authenticated Users with at least Execute permissions.

This will make it possible for all users who authenticate to your SharePoint Online tenancy to use the external content types stored in the Metadata Store.

4. Select the "Propagate permissions to all BCS Models, External Systems and External Content Types in the BDC Metadata Store" check box. Doing so will overwrite any existing permissions check boxes.
5. Click OK.

SharePoint Online BCS connection settings for apps configuration

Unlike BCS in SharePoint on-premises, BCS in SharePoint Online requires that you configure additional connection settings, which contains additional information to establish the connection to the external system and the OData source.

Before you begin this procedure, ensure that you have the following:

- The URL or published service endpoint of the on-premises OData service that you

configured
(<https://odata.contoso.com/AdventureWorks.svc/>).

- The ID of the on-premises Secure Store target application that you configured; for example, ODataApp.
- The Internet-facing URL that Office 365 uses to connect to the service address and that was published by the reverse proxy. This is the address that you used to browse to the external service in the last procedure, with the addition of `/_vti_bin/client.svc`; for example,
https://intranet.contoso.com/_vti_bin/client.svc

Important Ensure that you do not forget to add the path to the client side object model to the URL `/_vti_bin/client.svc`. So your URL would look similar to
https://intranet.contoso.com/_vti_bin/client.svc.

- The ID of the Secure Store target application for the client preauthentication certificate in Office 365; for example, SecureChannelTargetApplication.

To configure the connection settings object for the BCS hybrid scenario, perform the following steps:

1. Open the SharePoint Online Admin Center by using a Global Administrator account, and then, in the navigation pane, click "bcs."
2. Click Manage Connections To On-Premises Services, and then click Add
3. On the Connection Settings Properties page, give the connection settings object a name; for example, ODataOnPremises.

Important Keep track of this name; you will require it when you create the external content type in the next procedure.

4. In the Service Address box, type the URL of the OData service endpoint that you created; for example,
<https://odata.contoso.com/AdventureWorks.svc>.
5. For this scenario, select the Use Credentials Stored In Sharepoint On-Premises as the authentication option, and then type the name of target application ID that holds the group to account mapping. In this scenario, it is **ODataApp** that you created.

6. In the Authentication Mode list box, select Impersonate Window's Identity.
7. In the Internet-Facing URL box, type the external URL with the **/_vti_bin/client.svc** extension; for example,
https://intranet.contoso.com/_vti_bin/client.svc

Important Ensure that you do not forget to add the path to the client side object model to the URL **/_vti_bin/client.svc**. So your URL would look similar to https://intranet.contoso.com/_vti_bin/client.svc.

8. In the Secure Store Target Application ID box, type the ID of the target application that holds the Secure Channel certificate; for example, SecureChannelTargetApplication. Before clicking create, reconfirm your settings. It should be similar to what you see in Figure 3-7.
9. Click Create.

connection settings properties

Title
The name given to this connection.

Title:
ODataOnPremises

Service Address
The URL (or published service endpoint) of the on-premises OData service.

Service Address:
https://odata.contoso.com/AdventureWorks.svc

Authentication
The authentication type required by the OData data source.

☐ Don't use authentication

☐ Use user's identity

☒ Use credentials stored in SharePoint on-premises

☐ Use OData Extension Provider

Secure Store Target Application ID:
ODataApp

Authentication Mode
Impersonate Window's Identity

Internet-facing URL
The internet facing URL that Office 365 uses to connect to the Service Address, and that is usually published by a Reverse Proxy, a Service Bus, or other Network Appliance.

Internet-facing URL:
https://intranet.contoso.com/_vti_bin/client.svc

Client Certificate
The Target Application ID for the SSL client certificate in the Secure Store Service that Office 365 uses to connect to the Internet facing URL. This must be pre-configured in the Office 365 Secure Store Service.

Secure Store Target Application ID:
SecureChannelTargetApplication

Figure 3-7: The BCS Online Connection Settings Properties page to manage connections to on-premises services.

SharePoint 2013 compatibility setting for SharePoint Online

If you configured Use Credentials Stored In SharePoint On-Premises in step 9 of the previous

procedure, and if you are working with SharePoint Server 2013 on-premises, there is an additional change you need to make to the web.config file in your on-premises web application. Because SharePoint Online essentially contains version 16 bits and if you are running SharePoint Server 2013 on-premises with version 15 bits, there is a mismatch in versions that could cause an issue when uploading your BDC model file in Office 365.

```
<dependentAssembly xmlns="urn:schemas-microsoft-com:asm.v1">  
    <assemblyIdentity  
name="Microsoft.Office.SecureStoreService"  
publicKeyToken="71e9bce111e9429c" culture="neutral"  
/>  
    <bindingRedirect oldVersion="16.0.0.0"  
newVersion="15.0.0.0" />  
</dependentAssembly>
```

Without this in place you will get the following error when you import your BDC model: The Type Name For The Secure Store Provider Is Not Valid.

Create and configure the external content type

An external content type (ECT) holds important configuration information that BCS needs to understand and to get data from the LoB data

source. ECTs map external data fields to business entities; for example, Customer, Order, and Product. An ECT defines how the LoB data is structured and typically includes the service URL of the data source, or in a hybrid BCS scenario, it points to the BCS connection configured in the previous procedure; for example, ODataOnPremises in the Connection Settings For Apps.

An ECT also includes specific portions of the external data that you want to interact with, and the permitted operations such as create, read, update and delete.

More info To read more on External Content Types, go to [https://msdn.microsoft.com/library/office/ee556391\(v=office.14\).aspx](https://msdn.microsoft.com/library/office/ee556391(v=office.14).aspx).

In the BCS hybrid scenario, only OData sources are supported and the preferred way to make an external content type for an OData source is to use Visual Studio. With Visual Studio, you are able to easily create the external content type by directly connecting to the OData source, reading it, and building it. After it is created, you would need to extract the BDC model file (.bdcm) and make some changes to get it ready for upload to SharePoint Online BCS. These modifications are

described in the section “Make the BDC model file Office 365 tenant ready” later in this chapter.

Before you begin, ensure you have the following:

- Visual Studio 2012/2013 installed
- Microsoft Office Tools for Visual Studio
- The OData service endpoint URL, such as <https://odata.contoso.com/AdventureWorks.svc>

You need to create an ECT from the OData service endpoint by using Visual Studio.

The following steps show how to use Visual Studio 2012 to create an ECT based on an OData source.

To create a new SharePoint Add-in:

1. In Visual Studio, create a new App For SharePoint project, which is located under the Visual C#, Office/SharePoint template node, as depicted in Figure 3-8.

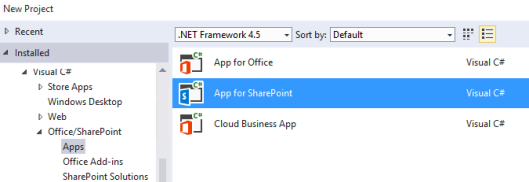


Figure 3-8: Creating a new Visual Studio project in C# - App for SharePoint.

2. Name your project, and then choose OK. In our example, we named it ContosoSalesApp.
3. To specify the SharePoint settings, type a name for your app, and the URL of the on-premises SharePoint dev farm you will be debugging against. In our example here, we have `https://dev-intranet.contoso.com` configured with a Developer Site web template (DEV#0), as illustrated in Figure 3-9.

New app for SharePoint



Specify the app for SharePoint settings

What SharePoint site do you want to use for debugging your app?

`https://dev-intranet.contoso.com`

Don't have a developer site?

[Sign up for an Office 365 Developer site to develop, test and deploy apps for Office and SharePoint](#)

How do you want to host your app for SharePoint?

☐ Provider-hosted

☒ SharePoint-hosted

[Learn more about this choice](#)

Figure 3-9: Settings for the new app for SharePoint project in Visual Studio.

4. Click Finish.

After the project is created, you use the new auto generation tooling for OData sources

and add a BDC model for the OData source to your app.

To add a new BDC model:

5. In Solution Explorer, right-click the App (ContosoSalesApp), and then, on the shortcut menu that opens, click Add.
6. On the submenu that appears, select Content Types For External Data Source, as depicted in Figure 3-10.

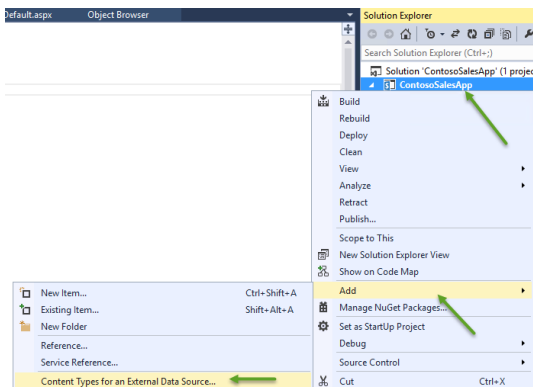


Figure 3-10: Adding content types for an external data source for the ContosoSalesApp in Visual Studio.

This starts a wizard that will help you discover the selected data source and create the BDC model.

7. The first page of the wizard is used to collect the URL of the data service. On the Specify OData Source page, type the URL of the OData service to which you want to connect. In our example, it is <https://odata.contoso.com/AdventureWorks.svc>.

If you don't have an on-premises OData service created yet, you can work with freely available read-only OData service endpoints on the Internet such as:

<http://services.odata.org/AdventureWorksV3/AdventureWorks.svc> or <http://services.odata.org/Northwind/Northwind.svc>.

8. Choose a name for your OData source, and then choose Next.
9. A list of data entities that are being exposed by the OData Service appears. Select one or more of the entities (see Figure 3-11), and then choose Finish.



Select the Data Entities

Select the data entities for which you want to generate external content types.

☒	CompanySales
☐	ManufacturingInstructions
☐	ProductCatalog
☐	TerritorySalesDrilldown
☐	WorkOrderRouting

☒ Create list instances for the selected data entities (except Service Operations).

Figure 3-11: Data entities enumerated and selecting CompanySales to build the new external content type.

10. Verify if the .ect file has been created by expanding the newly created folder named External Content Types in Solution Explorer. As depicted in Figure 3-12, you will see your newly created data source (ContosoSales) and if you further expand the ContosoSales folder, you will see the newly created .ect file.

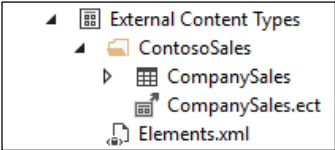
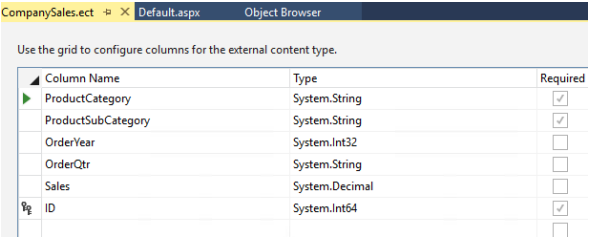


Figure 3-12: ECTs created based on selection of CompanySales data entity.

You can view the .ect file in a graphical list of the entities by double-clicking the .ect file in Visual Studio, as shown in Figure 3-13.



CompanySales.ect Default.aspx Object Browser

Use the grid to configure columns for the external content type.

Column Name	Type	Required
ProductCategory	System.String	☒
ProductSubCategory	System.String	☒
OrderYear	System.Int32	☐
OrderQtr	System.String	☐
Sales	System.Decimal	☐
ID	System.Int64	☒

Figure 3-13: Viewing the .ect file in graphical list in Visual Studio.

Alternatively, to view the contents in XML format, in an XML editor, right-click the .ect file in Visual Studio, select Open With, and then select XML (Text) Editor.

How to prepare the .ect file

To use multiple ECTs in the BCS service application, you need to ensure that unique names are configured in the .ect files.

Note You will be prevented from adding multiple ECTs in the form of BDC model files if you skip the steps in this procedure.

1. After you have opened the .ect file in an XML editor such as Visual Studio, you will need to replace the Name attribute in the Model element, as illustrated in Figure 3-14 and Figure 3-15. In our example, we used the AdventureWorks.svc OData source endpoint, so the name in your ECT will have something similar to AdventureWorksModel. You will need to replace this with a unique name such as **ContosoCompanySales**.



```
CompanySales.ect  X Default.aspx  Object Browser
<?xml version="1.0" encoding="utf-16"?>
<Model xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" Name="AdventureWorksModel">
  <LobSystems>
    <LobSystem Name="ContosoSalesDataSource" Type="OData">
      <Properties>
```

Figure 3-14: The AdventureWorksModel automatically generated in the ECT needs to be changed to unique name.

You can change this to anything you like that describes this particular ECT.



```
CompanySales.ect  X Default.aspx  Object Browser
<?xml version="1.0" encoding="utf-16"?>
<Model xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" Name="ContosoCompanySales">
  <LobSystems>
    <LobSystem Name="ContosoSalesDataSource" Type="OData">
      <Properties>
```

Figure 3-15: Model name changed to ContosoCompanySales to make it unique.

2. For consistency, you can change the Namespace attribute of the Entity element, which is about 28 lines down in the .ect file (see Figure 3-16). Replace AdventureWorksModel with **ContosoCompanySales**.

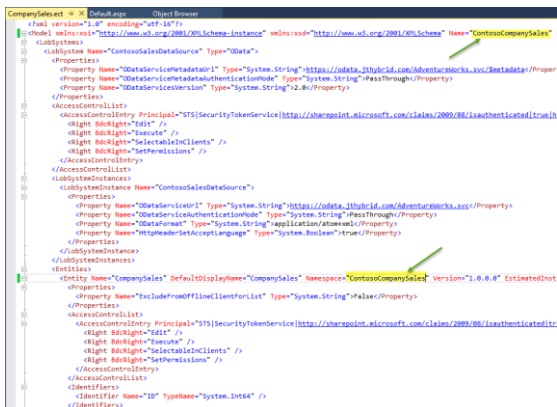


Figure 3-16: Update Entity NameSpace to ContosoCompanySales.

3. Modify the Elements.xml file (Figure 3-17) with the same name for consistency. Replace AdventureWorksModel1 with **ContosoCompanySales** and save all the files in that project.

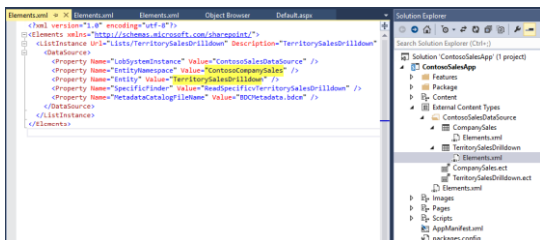


Figure 3-17: Update the Elements.xml file for consistency.

Note The preceding steps have been adapted from <https://msdn.microsoft.com/library/jj163967.aspx> and <https://sam1man.wordpress.com/2015/03/02/setting-up-bcs-hybrid-features-end-to-end-in-sharepoint-2013>.

Manually extract an external content type to a BDCM file

The external content type that you configured must be manually extracted and saved as a file with a .bcdm extension. You do this in Windows Explorer by locating the project files where the .app package is created. Follow the procedure in “How to: Convert an App-Scoped External Content Type to Tenant-Scoped” in the MSDN Library.

More info To learn more on how to extract your BDC model file from a Visual Studio package, go to <https://msdn.microsoft.com/library/office/dn130133.aspx>.

You'll need the .bcdm file for the next few procedures, such as importing it into BCS on-premises and BCS online.

Import the BDCM file into the SharePoint on-premises BDC Metadata Store

After you have the .bdcml file, you need to import it into your SharePoint on-premises BDC metadata store by performing the following steps:

1. Upload the .bdcml file into your on-premises BCS service application through the Central Administration site. Just use the default options while importing via Central Administration.

Alternatively, you can use the following Windows PowerShell script to import the BDC Model directly into your on-premises SharePoint BCS. Update the script with your SharePoint Central Administration URL and the path to your .bdcml file.

```
$BDCMetadataObject = Get-SPBusinessDataCatalogMetadataObject -BdcObjectType Catalog -ServiceContext "http://SPCentralAdmin:44000"
```

```
Import-SPBusinessDataCatalogModel -Identity $BDCMetadataObject -Path "D:\Temp\BDCmodel.bdcml"
```

2. After the file is imported into the on-premises BCS, you would need to grant permissions to the on-premises users to be

able to use the BCS. For convenience, you could use the CONTOSO\ODataGroup security group and give them execute permissions, as shown in Figure 3-18.

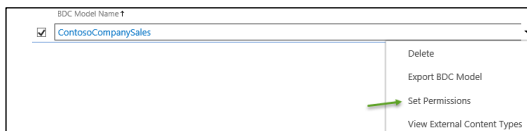


Figure 3-18: Set permissions on the ContosoCompanySales BDC Model in the on-premises BCS.

Make the BDC model file Office 365 tenant-ready

When you open the BDC Model (.bdcm) file in an XML reader, you would have noticed that the file has your OData service endpoint URL present in two places in the file. Because the SharePoint Online BCS uses its own connection details that you already configured in previous steps, you would have to remove these references in the .bdcm file and add a reference to the Connection name that was configured; for example, ODataOnPremises. BCS hybrid connections from Office 365 to the on-premises data source will not work if these steps are missed or improperly configured.

1. Make a copy of the .bdcm file that you'll be importing into Office 365.
2. In the .bdcm file, delete the `ODataServiceMetadataUrl` and `ODataServiceMetadataAuthenticationMode` properties from the `LobSystem` property list.
3. Again, in the .bdcm file, delete the `ODataServiceUrl` and `ODataServiceAuthenticationMode` properties from the `LobSystemInstance` property list.
4. Add this property to the list of properties for both the `LobSystem` and `LobSystemInstance`:

```
<Property Name="ODataConnectionSettingsId"
Type="System.String">ODataOnPremises</Property>
```

5. Save the .bdcm file and you are now ready to import it into the SharePoint Online BDC Metadata Store. Your .bdcm file should look similar to that shown in Figure 3-19.

```
<LobSystems>
  <LobSystem Name="ContosoSalesDataSource" Type="OData">
    <Properties>
      <Property Name="ODataConnectionSettingsId" Type="System.String">ODataOnPremises</Property>
      <Property Name="ODataServicesVersion" Type="System.String">2.0</Property>
    </Properties>
    <AccessControlList>
      <AccessControlEntry Principal="STS|SecurityTokenService|http://sharepoint.microsoft.com/claims/2"
        <Right BdcRight="Edit" />
        <Right BdcRight="Execute" />
        <Right BdcRight="SelectableInClients" />
        <Right BdcRight="SetPermissions" />
      </AccessControlEntry>
    </AccessControlList>
  </LobSystem>
  <LobSystemInstances>
    <LobSystemInstance Name="ContosoSalesDataSource">
      <Properties>
        <Property Name="ODataConnectionSettingsId" Type="System.String">ODataOnPremises</Property>
        <Property Name="ODataFormat" Type="System.String">application/atom+xml</Property>
        <Property Name="HttpHeaderSetAcceptLanguage" Type="System.Boolean">true</Property>
      </Properties>
    </LobSystemInstance>
  </LobSystemInstances>
</LobSystems>
```

Figure 3-19: The .bdcm file updated and ready to upload to Office 365.

Import the BDCM file into the SharePoint Online BDC Metadata Store

When you import the BDC Model file into SharePoint Online, you must be logged in to the SharePoint Online administrator site as a federated or synchronized account (an account imported to Office 365 and synchronized with the on-premises Active Directory). This federated account must be a Global Administrator in Office 365. When importing the BDC Model to configure a hybrid BCS, certain calls are made to on-premises SharePoint farm that will require you use a federated user account. This account must also have a populated user profile in your on-premises SharePoint farm.

To import a .bdcm file into the SharePoint Online BDC Metadata Store, perform the following procedure:

1. Sign in to your SharePoint Online tenancy by using an account as described in the preceding paragraph, and then, in the SharePoint Online Admin Center, click “bcs.”
2. In the Business Connectivity Services section, click Manage BDC Models And External Content Types.

3. On the Edit tab, click Import.
4. Click Browse, and then browse to the .bdcm file that you exported.
5. Leave the default selections for File Type and Advanced Settings, and then click Import. During the import, BCS validates the XML in the model, queries the connection settings object, and connects to the on-premises OData source.

When you import a BDCM model into the BDC metadata service, you are creating an ECT. This ECT is available across your SharePoint Online in your Office 365 tenant.

Create an external list in your SharePoint Online site

The next step is to create an external list in your desired SharePoint Online site.

1. Open the SharePoint Online site where you want to create an external list. Ensure that the site has appropriate permissions configured to allow your ODataGroup users access to work with the LoB data within it.
2. In SharePoint Online, click Site Contents, and then click add an app.

3. Click External List, and then provide a name for the list; for example, Contoso Sales.
4. Click the Select External Content Type link next to the External Content Type box.
5. Select the external content type that you created, click OK, and then click Create.
6. Open the external list and confirm that your external data is displayed.
7. After the list is created, validate the scenario.

Validation steps for BCS hybrid

To validate the external list, ensure that you and the selected users are able to access it, as illustrated in Figure 3-20.

If your OData Source allows you to write back, you should be able to test creating, updating, and deleting content as another nonprivileged user who is part of the CONTOSO\ODataGroup.

ProductCategory	ProductSubCategory	OrderYear	OrderQtr	Sales
Clothing	Jerseys	2008	Q3	7884.4700
Clothing	Socks	2007	Q4	6183.1422
Clothing	Gloves	2006	Q3	52536.8767
Clothing	Gloves	2007	Q2	41875.9919
Clothing	Vests	2007	Q4	66882.6450
Clothing	Tights	2007	Q2	51600.6190
Clothing	Jerseys	2007	Q3	173041.0492
Clothing	Gloves	2007	Q4	23619.1700
Clothing	Jerseys	2006	Q3	48901.7598

Figure 3-20: Contoso Sales data displayed in SharePoint Online in a BCS hybrid environment.

To summarize, every user who will be reading, creating, and updating the external data must have three properties:

- He must have user or greater permissions to the SharePoint Online site and the external list or app for SharePoint.
- He must be a federated or synchronized account.
- He must be a member of the on-premises global security group that you are using to control access to the OData service endpoint; for example, he must be a member of ODataGroup.

More info To follow four account validation scenarios, go to <https://technet.microsoft.com/library/dn197246.aspx>.

Additional hybrid solutions

This chapter covers additional hybrid capabilities that are possible with Microsoft SharePoint. We discuss Microsoft OneDrive for business, its uses, and how to implement it in a SharePoint hybrid context. We walk through the Hybrid Sites' features, which includes hybrid profiles, site following, hybrid Delve, and the extensible hybrid app launcher. We cover how each of them works, and, finally, how to turn them on along with some verification steps.

Overview of additional hybrid capabilities

There are various other features that are available to provide new ways of collaborating in a hybrid environment. These are grouped together to help you to easily deploy them to make these features available. Here are the two feature bundles:

- Hybrid OneDrive for Business
- Hybrid Sites Features which includes the following:
 - Site following
 - Hybrid profiles
 - Extensible hybrid app launcher

Let's look at the capabilities of these feature bundles and how to set them up.

OneDrive for Business

OneDrive for Business provides storage for user's documents and other files in the cloud or on SharePoint Server. Users can also easily share files stored on OneDrive for Business and synchronize files to any device with the OneDrive for Business client. You can view, edit, or share files stored in OneDrive for Business from all devices. OneDrive for Business provides for coauthoring, by which multiple users can edit a document at the same time.

OneDrive for Business is different from OneDrive, which is a separate service offering by Microsoft specifically for personal storage in the cloud; it is separate from your workplace. OneDrive for Business is also different from your Microsoft Office 365 team site, which is intended for storing team or project-related documents.

OneDrive for Business files are generally used for business files for individuals to work with and are not shared with others in the organization unless you explicitly decide to share them.

OneDrive for Business with Office 365 offers 1 TB of storage and is purchased via an Office 365 subscription or bundled with a SharePoint online subscription. OneDrive for Business that ships with SharePoint on-premises is the My Site

document library for each user if personal sites are provisioned in your organization. These files are stored in the My Site content database and storage settings are managed at the web-application level of the SharePoint on-premises farm.

With OneDrive for Business in Office 365, you can share with others outside of the organization.

OneDrive for Business hybrid

In a hybrid scenario, users' work files are stored in OneDrive for Business in Office 365 while collaborating in a SharePoint hybrid environment. The advantage to this is the versatility OneDrive for Business in Office 365 offers without the need to move all SharePoint workloads to Office 365. When users click the OneDrive link in SharePoint on-premises, they are redirected automatically to their OneDrive for Business storage in Office 365.

It is important to note that when you turn on OneDrive for Business hybrid, the documents in the old location "OneDrive for Business," which is essentially the Documents library in a user's My Site in SharePoint on-premises, are not moved to Office 365. Instead, the documents are left in the

same location and users are able to visit their old OneDrive for Business in their My Site by either manually typing the URL or by visiting a published link on your SharePoint intranet to the old My Sites URL where they can retrieve their documents.

The old My Site URL would look something similar to this: <https://mysites.contoso.local/personal/jtaylor> or https://mysites.contoso.local/personal/contoso_jtaylor.

The redirected URL for OneDrive for Business will look something similar to this: https://contoso-my.sharepoint.com/personal/jtaylor_contoso_com

To move their documents across, they could manually copy them from the old on-premises OneDrive for Business to the new OneDrive for Business in the cloud, but they would lose their metadata such as the modified date. If you manually copy files on behalf of users, you become the owner of the document. Furthermore, manually moving personal work files in OneDrive for Business can be an onerous on the user, you, and/or your team, so it is advisable to look at bulk migration if you have a lot of user's data that needs to be moved to Office 365.

To preserve the metadata of these files and move users in bulk, it is recommended to evaluate the options you have with third-party migration tools.

More info To read about moving file shares to OneDrive for Business as well as about a number of third-party tools that you can use to do that, go to

<https://blogs.technet.microsoft.com/akieft/2013/09/06/migrating-file-shares-to-onedrive-for-business/>.

Microsoft offers an import service with which you can move files to Office 365, but it does not preserve metadata. With the Microsoft migration service, you can move via a network upload or by sending encrypted physical hard drives via courier service for upload into Office 365.

More info To read more about Microsoft's migration service, go to

<https://blogs.office.com/2015/09/16/office-365-import-service-migration-to-sharepoint-online-and-onedrive-for-business-just-became-easier/>.

Users can keep working in their old OneDrive for Business on-premises, but to avoid data duplication and end-user confusion, it makes

sense for the business to dictate a strategy of working only in OneDrive for Business in Office 365.

More info To read more about OneDrive for Business planning, go to <https://support.office.com/article/Plan-hybrid-OneDrive-for-Business-b140bc4c-f54d-4b5a-9409-a3bece4a9cf9?ui=en-US&rs=en-US&ad=US>.

There is no direct link between OneDrive for Business in SharePoint on-premises and OneDrive for Business in Office 365, so user's Shared With Me list in SharePoint Online will not contain documents that have been shared with them from SharePoint on-premises.

OneDrive for Business synchronization client

The OneDrive for Business synchronization client is available to synchronize any of these files to your laptop, desktop, or mobile device. This makes it possible for you to work offline, such as when you're traveling or working remotely without access to an Internet connection.

If you are using OneDrive for Business in SharePoint on-premises, your files are

synchronized back to SharePoint on-premises from your laptop or mobile device as soon as you reconnect to your corporate network. If you are using OneDrive for Business in Office 365, your files are synchronized back to Office 365 when you regain access to an Internet connection, not just your corporate network. This makes it more versatile for a remote workforce and consumable from a multitude of devices.

The OneDrive for Business synchronization client is available via any of the following:

- Office Professional Plus 2016
- Office Professional Plus 2013
- Office 365 Enterprise E3
- Office 365 Midsize Business
- Office 365 Small Business Premium
- Windows 10
- Windows 8.1
- Standalone client is also available as a separate download

More info To learn more about OneDrive for Business and to download the client, go to <https://onedrive.live.com/about/business>.

Hybrid Sites features

Hybrid Sites features—also referred to hybrid team site features in some documentation—is a set of hybrid features specific to the consolidation of users' profile My Sites, online Delve-powered profile sites, and sites following functionality in a hybrid environment.

Hybrid site following

Hybrid site following is part of Hybrid Sites features, and is available on both SharePoint Server 2013 and SharePoint Server 2016.

When a user follows a SharePoint site, a link to that site is added to a list that is the Social list in the user's personal profile site. This list contains three views, Followed Sites Documents, Followed Content, and Followed Sites.

Without the hybrid site-following feature turned on, your users will have two different social lists and different followed sites items where the on-premises SharePoint sites followed will not contain the SharePoint Online sites followed. The

SharePoint hybrid site following consolidates the site following information from both locations into the SharePoint Online list in Office 365 for all new sites that are followed. When users click a followed-sites list on the on-premises farm, they are redirected to their SharePoint Online followed-sites list.

Behind the scenes, the Followed Sites Documents, Followed Content, and the Followed Sites are nothing but SharePoint views with their own URLs, as demonstrated in the example that follows, and will help you when providing support or troubleshooting issues:

View Name: Followed Sites Documents

Example URL: https://contoso-my.sharepoint.com/personal/user_contoso_com/Social/SitesDocuments.aspx

View Name: Followed

Example URL: https://contoso-my.sharepoint.com/personal/user_contoso_com/Social/FollowedContent.aspx

View Name: Followed Sites

Example URL: https://contoso-my.sharepoint.com/personal/user_contoso_com/Social/Sites.aspx

It is important to note that turning on hybrid site following does not move any existing followed-sites lists in SharePoint on-premises to SharePoint Online, because they are two separate lists without any synchronization or replication between them. When you turn on Hybrid Sites features, any followed sites in the SharePoint Online list will remain there and not be erased; however, users must refollow their SharePoint on-premises sites again after you turn on Hybrid Sites features.

To selectively roll out Hybrid Sites features and site following, consider creating an audience in the SharePoint on-premises user profile service application, giving you control on the Hybrid Sites features roll out.

Turning on the Hybrid Sites features also does not affect the SharePoint on-premises newsfeed functionality. Users will continue to have separate newsfeeds in SharePoint on-premises and SharePoint Online. Because there is no integration with newsfeeds, each newsfeed shows activities for sites and documents in their respective environments.

Note Hybrid document following is not available with site following. If you use hybrid OneDrive for Business, the on-premises documents that have been followed prior to configuring OneDrive for Business, will be hidden from users. It is important to note that the Office 365 followed-documents list contains only followed documents from Office 365. If you configure hybrid search and you have Delve as part of your Office 365 license, you can “favorite” documents that reside in your SharePoint on-premises farm.

After you turn on hybrid site following, depending on your version of SharePoint on-premises, users will need to click either the Sites link in SharePoint Server 2013 or the Sites tile in the SharePoint Server 2016 app launcher to be redirected to Office 365.

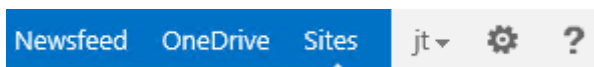


Figure 4-1: The Sites link in SharePoint Server 2013.

The steps to configure hybrid site features are described later in this chapter.

Hybrid profiles

One of the requirements of a SharePoint hybrid deployment is that you configure the on-

premises SharePoint User Profile service application with My Sites and run a user profile synchronization. This process creates user profiles on-premises. Users in Office 365 also have their own profile for storing user-related profile information.

Users who have profiles in both SharePoint on-premises and Office 365 can end up having a confusing profile experience. When you turn on Hybrid Sites features, hybrid profiles are in effect, meaning users will have a single Delve-powered profile for their profile information for organizational collaboration purposes. Turning on hybrid profiles does not mean that you can delete user profiles on-premises. The User Profile service application and correct profile information on-premises is a requirement for the hybrid user lookup experience for most hybrid scenarios like search and business connectivity services.

Hybrid profiles essentially redirects hybrid users to their own profile in Office 365 instead of the on-premises My Sites user profile. Hybrid profiles is available with both SharePoint Server 2013 and SharePoint Server 2016. When users click About Me in the top navigation of a SharePoint site, they are redirected to their profiles in Office 365. This ensures that hybrid

users have a single place for their profile information and avoids confusion with duplicate profile locations.

Planning a hybrid profile roll out

Because hybrid profiles are part of the Hybrid Site features bundle, you can choose to selectively offer Hybrid Site features such as hybrid profiles to users via an audience in the on-premises SharePoint User Profile service application. Users who aren't part of the audience will not have a hybrid profile, but when these nonhybrid users in your on-premises environment click a hybrid user's profile, they are redirected to the hybrid user's profile in Office 365. Nonhybrid users who are not in the audience will have their user's profiles on-premises by default and optionally an Office 365 profile if they are licensed Office 365 users; however, no redirection to their Office 365 profile will occur when anyone clicks their name to view their profile, until they are added to the audience.

Managing user profiles in SharePoint Online

You can view user attributes, manage user profiles, and other settings such as audiences and My Site settings through the SharePoint

admin center. The User Profiles administration page (see Figure 4-2) is useful for viewing user profile properties for troubleshooting purposes, creating audiences for SharePoint Online, managing social tags, and to setting up contacts who should be notified during the My Site cleanup process.

When a user leaves the organization, the user's profile (My Site) will be flagged for deletion after 30 days. To prevent data loss, access to the former user's profile can be granted to the user's manager or, in the absence of a manager, a secondary My Site owner. This gives the manager or the secondary owner an opportunity to retrieve content from the profile before it is deleted.



Figure 4-2: The User Profiles administration page in the SharePoint Admin Center in Office 365.

Migrating profile data

Many organizations have requirements to replicate custom attributes for their user profiles. With the on-premises versions of SharePoint, this was possible, but with Microsoft Azure Active Directory, a standard set of attributes that are compatible with SharePoint Online are synchronized by default. To augment these attributes with your custom attributes (from various on-premises systems), Microsoft has developed a bulk Application Programming Interface (API) to import custom user profile attributes into Azure Active Directory for SharePoint Online and the Delve-powered user profile store. Microsoft has developed a SharePoint Online timer job that checks and processes queued import requests and imports based on the API calls and information provided by you via a JSON-formatted file containing the attributes and values.

More info To read more about the user profile bulk API, go to <http://go.microsoft.com/fwlink/p/?LinkId=786318>.

Delve in a hybrid deployment

Delve is an Office 365–hosted product that offers a powerful functionality to a personalized view of

content from SharePoint Online sites and OneDrive for Business that is relevant to users. It fosters more collaboration because it can show users what their colleagues are collaborating on that is relevant to them. Delve is based on the Office Graph which intelligently gathers your workforce interactions. So, the more your users collaborate on documents, email, and chat and call using Skype for Business, the more useful Delve will be to improve productivity in your organization. All Delve results are security trimmed and doesn't modify permissions itself. Private documents remain private.

Delve, in a hybrid context becomes more powerful when a Cloud Hybrid Search service application is configured. Delve, via the Office Graph has visibility into your on-premises content and presents it to Delve users based on the security permissions of the documents. When a Delve user performs a search, results from on-premises sources can also be presented in Delve via the Cloud Hybrid Search. Adding items to a board in Delve will work the same way regardless of whether the content was in Office 365 or on-premises. Delve will display activity for users working or collaborating on SharePoint on-premises content.

Currently, Delve is available for users licensed with any of the following plans:

- Office 365 Enterprise E1–E5 subscription plans (including the corresponding A2–A4 and G1–G4 plans for Academic and Government customers, respectively)
- Office 365 Business Essentials
- Office 365 Business Premium

Delve is available to users who have a valid license in any of the preceding plans and are activated with a SharePoint Online license (see Figure 4-3). If Delve is not part of your subscription license in Office 365, or you have disabled the Office Graph functionality in the SharePoint Admin Center settings, your users will not have the Delve-powered features such as colleague's recent documents and relationships.

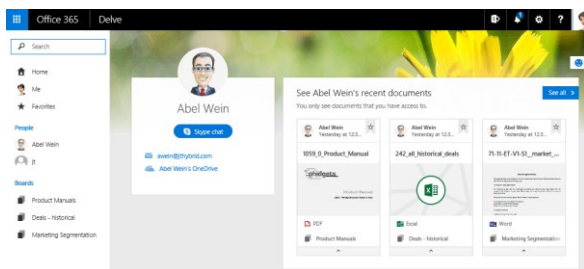


Figure 4-3: A Delve-powered profile displaying the user's recent documents to which others have access.

There might be reasons why users do not want their profile crawled and exposed by Delve, regardless of whether others have access. You can do this via the Site Settings, Search, and Offline Availability on the user's profile site. Users are site collection administrators of their personal sites by default. You can add yourself as a site collection administrator, but you would need to explicitly add your user name as a Site Collection Administrator. To do that, In the SharePoint Admin Center, in the navigation pane on the left, click User Profiles. Next, in the center pane, in the People section, click Manage User Profiles, and then click Manage Site Collection Owners.

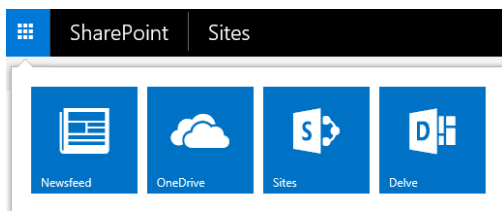


Figure 4-4: The Newsfeed, OneDrive, Sites, and Delve tiles in SharePoint Server 2016.

Clicking the Delve tile takes you to your user profile home page or equivalent My Site home page in Office 365. The URL would look

something similar to https://contoso-my.sharepoint.com/_layouts/15/me.aspx.

Click the Me page in Delve, and then, on the menu that opens, click About Me. This takes you to your specific Delve-powered profile. The URL will look something similar to https://contoso-my.sharepoint.com/_layouts/15/me.aspx?u={GUID}&v=work.

To try new Delve features more quickly, you would need to opt in to the First Release program. To learn more about the First Release program, go to <https://support.office.com/article/HA104204958>.

More info To plan how to plan and administer Delve, go to <https://support.office.com/article/Office-Delve-for-Office-365-admins-54f87a42-15a4-44b4-9df0-d36287d9531b>.

Extensible hybrid app launcher

The app launcher is present in both SharePoint Server 2016 and Office 365. The SharePoint Server 2016 app launcher includes tiles that link to some on-premises capabilities, but some are changed when you turn on Hybrid Sites features; for example, OneDrive and Sites. Users who are

licensed for Delve will see another tile labeled Delve.



Figure 4-5: The app launcher in SharePoint Server 2016.

To make SharePoint hybrid a more seamless experience, you can use the extensible hybrid app launcher to offer new apps that hyperlink to sites or web applications with their own custom icon. Then, users have a choice to pin any of these apps as tiles to their app launcher for quick access. When users pin these to their app launcher, the tiles automatically appear on the on-premises SharePoint Server 2016 app launcher within a day.

Here's how to add a custom tile:

1. Sign in to the Office 365 Admin Center (preview).
2. Click the Settings button, and then, on the menu that opens, click Organization Profile, as shown in Figure 4-6.

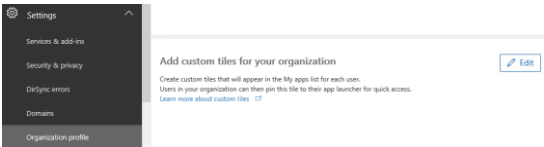


Figure 4-6: Add custom tiles for your organization.

3. In the Add Custom Tiles For Your Organization Pane, click Edit.
4. Go to the MyApps page at <https://portal.office.com/myapps>.
5. Locate any app of your choice; for example, the Intranet, as seen in Figure 4-7.

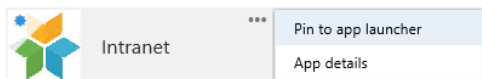


Figure 4-7: Pin to app launcher on the MyApps page.

6. Select the More Options button (the ellipsis), and then, on the menu that opens, select Pin To App Launcher.
7. Verify that the Intranet app is displaying in the app launcher in Office 365 (Figure 4-8).

It can take up a few hours to a day to display in the SharePoint Server 2016 app launcher because your browser might be cached with the old tiles.

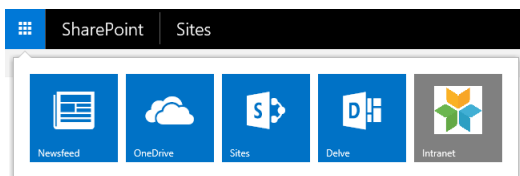


Figure 4-8: The custom tile has synchronized back to SharePoint Server 2016.

Note Testing results on my test user's desktop indicate that the app launcher updates within 5 to 10 minutes by refreshing the browser with Ctrl+F5.

You can make changes easily by editing the custom tiles you created. After you make changes, they will be updated for your users when they visit a SharePoint Server 2016 site and click the app launcher there. Again, keep in mind that this process can take a day or so to reflect the new changes.

The extensible hybrid app launcher feature is automatically turned on as part of the Hybrid Sites features bundle.

More info To learn more about the extensible hybrid app launcher, go to <https://support.office.com/article/The-extensible-hybrid-app-launcher-617a7cb5-53da-4128-961a-64a840c0ab91>.

Overview of configuring additional hybrid solutions

To turn on hybrid solutions in your environment, perform the following steps:

1. Plan and prepare for SharePoint hybrid for the synchronization of your users from Active Directory to Azure Active Directory (see the ebook *Planning and Preparing for Microsoft SharePoint Hybrid*, which you can get at <https://blogs.msdn.microsoft.com/microsoftpress/2016/04/26/free-ebook-planning-and-preparing-for-microsoft-sharepoint-hybrid>).
2. Set up SharePoint on-premises for a hybrid environment.

Configure the Managed Metadata Service application, User Profile Service application, My Sites, and the App Management Service application. To configure and start these services, go to

<https://msdn.microsoft.com/library/dn957480%28v=office.16%29.aspx>.

3. Configure hybrid search to set up a search-driven experience to look up documents, or people using Delve, and sites across Office 365 and SharePoint on-premises. To configure hybrid search, go to Chapter 1 and Chapter 2 in this ebook.
4. Configure additional hybrid capabilities with the following methods:
 - Cloud-driven Hybrid Picker
 - Cloud configuration page in the on-premises SharePoint Central Administration site

Note Configuring a server-to-server (S2S) trust with Azure Access Control Services (ACS) is a prerequisite if you are planning to configure using the cloud configuration page in the SharePoint central administration site. To configure the ACS trust, go to Chapter 1 in this book.

5. Verify that additional hybrid capabilities are available.

Configuring by using the Hybrid Picker tool

The Hybrid Picker tool helps you to configure OneDrive for Business and Hybrid Site features. The Hybrid Picker tool is available in Office 365 by going to the SharePoint Admin Center.

Hybrid Picker prerequisites

To run the Hybrid Picker, the account you sign in with must be the following:

- A member of the on-premises SharePoint farm Administrators group.
- Must have full control on the User Profile Service application.
- A global administrator in Office 365 or a SharePoint Online administrator.
- Signed in to Office 365. You can then start the Hybrid Picker from a server in your on-premises SharePoint server farm. This server must have access to the Internet.

Note Before running the Hybrid Picker tool, you will need to turn off any pop-up blockers in your browser.

When you visit the Hybrid Picker page in the SharePoint Admin Center, you are presented with two options (Figure 4-9):

- **Hybrid OneDrive** Choosing this option will redirect on-premises My Sites/OneDrive for Business sites to SharePoint Online OneDrive for Business in Office 365. Any click of the OneDrive link from anywhere in the on-premises SharePoint farm will redirect the user to his OneDrive for Business in Office 365.
- **Hybrid OneDrive and Sites Features** Choosing this option sets up Hybrid Sites features, a set of bundled site integration features, as well as OneDrive for Business redirection. Turn on hybrid OneDrive with Hybrid Site features to provide a more seamless UX.

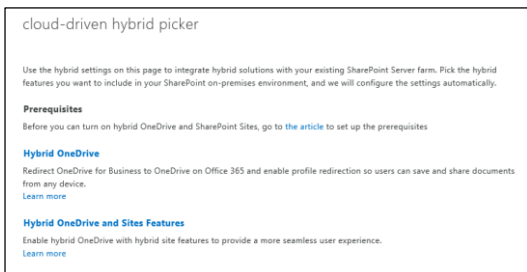


Figure 4-9: The Cloud-Driven Hybrid Picker page in the SharePoint Admin Center.

Running the Hybrid Picker

Running the Hybrid Picker on the SharePoint server requires Internet access because it is an Office 365–hosted tool that performs several operations such as S2S authentication trust and other configurations. Running the Hybrid Picker tool also downloads additional software it requires, like the Microsoft Office 365 Support Assistant.

Here are the steps to run the Hybrid Picker to configure either hybrid OneDrive for Business or hybrid OneDrive for Business and sites features:

1. Sign in to a SharePoint Server 2016 server as a farm administrator.
2. Go to the Office 365 Admin Center as an Office 365 global administrator.
3. In the Admin Center's pane, click SharePoint, as shown in Figure 4-10.

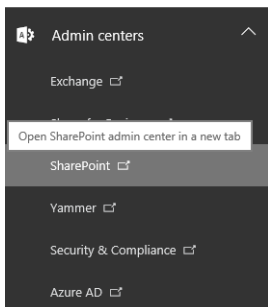


Figure 4-10: SharePoint option in the Admin Centers' pane in the new Office 365 Admin Center (preview).

4. In the SharePoint Admin Center, in the pane on the left, click **Configure Hybrid**.

The Cloud-Driven Hybrid Picker page opens, offering the following two options:

- Hybrid OneDrive
 - Hybrid OneDrive and Sites Features
5. Select either of the options to begin running the Hybrid Picker tool.
 6. You might see a couple of prompts asking you to allow the running of the prerequisite software to run the tool. Go ahead and accept this.

7. When you are done, as illustrated in Figure 4-11, proceed to the Office 365 cloud configuration in the SharePoint Central Administration site to validate the configuration and also configure an audience if you choose so.

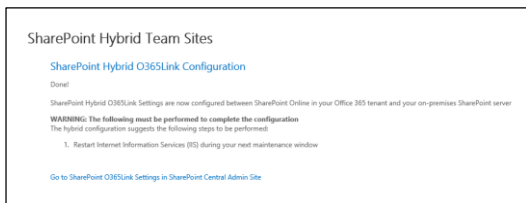


Figure 4-11: Hybrid Sites features and OneDrive for Business configuration complete.

8. Restart Internet Information Services (IIS) on all servers in your SharePoint Server farm at an approved maintenance window.

Configuring by using Central Administration

Since SharePoint Server 2013 Service Pack 1 onward, the SharePoint Central Administration site had an Office 365 configuration page. SharePoint Server 2016 has the same page and links except for a link to a feature planned for the future hybrid capability called SharePoint

Insights, which gives you the ability to view on-premises diagnostic and usage log reports in Office 365.

Configuration prerequisites via central administration

The following will help you to set up hybrid OneDrive and Sites features through the SharePoint Central Administration site:

- An S2S authentication trust with Azure ACS completed
- Be a member of the on-premises SharePoint farm Administrators group
- The My Site URL in Office 365
- An audience created in the on-premises User Profile service application if you want to selectively roll out OneDrive for Business and Sites Features.

Note To find the My Sites URL in Office 365, on the Admin menu, click SharePoint. In the Site Collections list, look for the site collection

that contains *<domain>-my.sharepoint.com*, as illustrated in Figure 4-12.

☐ URL
https://contoso.sharepoint.com
https://contoso.sharepoint.com/portals/hub
https://contoso.sharepoint.com/search
https://contoso.sharepoint.com/sites/CompliancePolicyCenter
https://contoso.sharepoint.com/teams/executives  NEW
https://contoso.sharepoint.com/teams/marketing  NEW
https://contoso-my.sharepoint.com

Figure 4-12: List of SharePoint Online site collections to determine the My Site URL in Office 365.

Configuration in Central Administration

To set up hybrid OneDrive and Sites features through the SharePoint Central Administration site, Perform the following steps:

1. In Central Administration, in the navigation pane, click Office 365, and then click Configure Hybrid OneDrive And Sites Features.

The Configure Hybrid OneDrive And Sites Features page opens, as depicted in Figure 4-13.

Configure hybrid OneDrive and Sites features

Use the hybrid settings on this page to integrate SharePoint Server 2016 with Office 365 OneDrive and Sites.

Configure hybrid OneDrive and Sites features
To manually configure hybrid OneDrive and Sites features, [check the prerequisites](#) and use the settings below

Use the Hybrid Picker to automatically configure hybrid OneDrive and Sites features.

[Learn more](#)

My Site URL
To find your My Site URL, sign in to Office 365 as the Office 365 global admin.

My Site URL: [\(Try link\)](#)

Select audience for hybrid features
If you want only a specific set of users to use hybrid features, you can select an existing audience or [create a new audience](#).

☐ Everyone

☒ Use a specific audience:
 

Select hybrid features

☒ OneDrive and Sites
Redirect OneDrive for Business to OneDrive on Office 365 and turn on hybrid Sites features. [Learn more](#)

☐ OneDrive only
Redirect OneDrive for Business to OneDrive on Office 365 so users can save and share documents from any device. No other SharePoint on-premises features are affected. [Learn more](#)

☐ None
Turn off hybrid OneDrive and Sites features.

Figure 4-13: Configuring hybrid OneDrive and Sites features in SharePoint Central Administration site.

2. In the My Site URL box, type the My Sites URL in Office 365; for example, `https://contoso-my.sharepoint.com`.
3. Optionally, select Use A Specific Audience to choose a specific audience that you already created. The default Everyone will roll out the chosen capabilities to all users in your organization.
4. Select the OneDrive And Sites option to turn on both OneDrive for Business and the

hybrid Sites features bundle. Optionally, select OneDrive Only to redirect hybrid OneDrive for Business and not the other features such as site following and hybrid profiles.

5. Choose OK to proceed.

Users will need to refresh their SharePoint pages to get the new links and begin using the new hybrid capabilities.

Verification

There are a few steps that you need to perform to verify that hybrid OneDrive for Business and Hybrid Sites features have been set up properly.

OneDrive for Business verification

After you set up the OneDrive hybrid redirect feature, the redirection is usually instant but it could take up to a minute to fully update the farm. You would need to ensure that your browser isn't caching the old links either.

- To verify that the redirect links are working as expected, test with a user account that is part of the audience you created. Clicking OneDrive in the top menu bar in SharePoint Server 2013 or the app launcher in

SharePoint Server 2016 will take you to OneDrive for Business in SharePoint Online. The URL should look similar to the following: https://contoso-my.sharepoint.com/personal/jtaylor_contoso_com.

- Verify with users who are not a part of the SharePoint audience that you configured. Users who are not a part of the SharePoint audience will experience no changes and will continue to go to their on-premises OneDrive for Business location, which is their document library in the personal site evidenced by the URL containing the My Site hostname.
- If audiences were not used, all users in your organization will be redirected to OneDrive for Business in SharePoint Online when they click OneDrive in the top menu bar in SharePoint Server 2013 or the app launcher in SharePoint Server 2016.

Users can directly browse to their OneDrive for Business by visiting <https://office365tenantname.onedrive.com>; for example, <https://contoso.onedrive.com>. This will redirect them to their OneDrive for Business document library after authenticating and authorizing them to successfully view the content specific to their account at that tenant,

as depicted in Figure 4-14. This is a great way to easily access OneDrive for Business storage when on the road for mobile or remote workers. This shortcut redirect might not be recognizable from within some client applications installed on desktops or mobile devices but will be recognized by most compatible browsers.

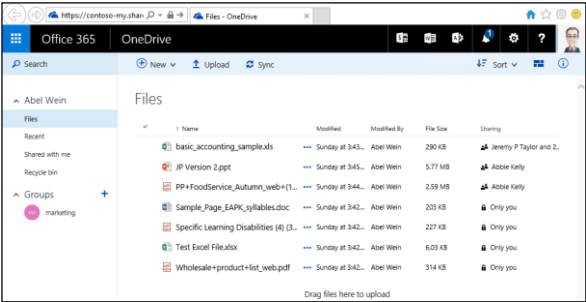


Figure 4-14: Verify that OneDrive for Business is redirecting to the Office 365 hosted service.

Hybrid Sites features verification

Because there are a few features bundled with the Hybrid Sites features, we will go through them here.

Site following verification

To verify if site following is working, perform the following steps:

1. Sign in to SharePoint Server 2016/2013 as a regular user. (Be sure you're a member of the correct audience if you used audiences.)
2. At the top of the page, click the Follow link.
3. You should see a small message appear under Follow, letting you know that you're following the site. Click this message and notice that it brings you to your personal site and the list of sites you're following in SharePoint Online.

Hybrid profiles verification

To verify if hybrid profiles is working, perform the following steps:

1. Sign in to SharePoint Server 2016/2013 as a regular user. (Be sure you're a member of the correct audience if you used audiences.)
2. Toward the upper-right corner on the SharePoint page, click your name, and then, on the menu that appears, click About Me.

If you have been allocated a Delve license in Office 365, you should be redirected to your Delve-powered profile (Figure 4-14).

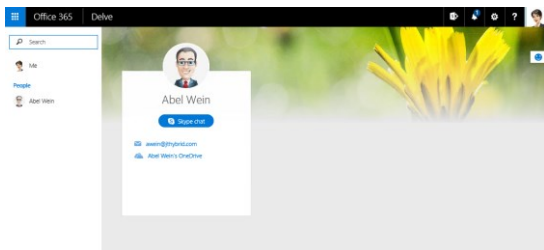


Figure 4-15: A user profile with Delve not turned on for the user.



Tell us what you think!

Is this book useful?
Does it meet your expectations?
Is there room for improvement?

Let us know at
<http://aka.ms/tellpress>

Your feedback goes directly to
the staff at Microsoft Press, and
we read every one of your
responses. Thanks in advance!

Microsoft Office 365 hybrid extranet and advanced sharing

This chapter focuses on the external sharing feature of Office 365 SharePoint Online and how it has developed to assist businesses in establishing collaboration partnerships with other businesses, without the usual requirements for expensive and complex technology. Extranets are traditionally difficult to implement, requiring both segregation and collaboration. This

often results in complex infrastructure and identity management implementations.

Introduction

Office 365 SharePoint Online external sharing provides the ability for subscribers to grant access to content in SharePoint Online to users outside their business. These users could be from other businesses or individuals, the only requirement being that those users have a Microsoft account to identify them. These users are referred to in Office 365 as *external users*.

An external user is someone outside of your organization who has been granted access to your SharePoint Online sites and documents but does not have a license for your SharePoint Online or Microsoft Office 365 subscription. The definition of an external user is based on their association to your primary business. External users cannot be employees, contractors, or onsite agents for you or any associated businesses.

External users inherit the use rights of the SharePoint Online customer who is inviting them to collaborate. That is, if an organization purchases an E3 Enterprise plan and builds a site that uses enterprise features, the external user is granted rights to use and/or view the enterprise features within the site collection to which they are invited. Although external users can be invited as extended project members to perform a full range of actions on a site, this does not grant them any extended rights beyond that site, such as those that a fully licensed user would have. The following table lists the key differences between external users and licensed users.

External users can...	External users can't...
Use Office Online for viewing and editing documents. If your plan includes Office Pro Plus, they will not have the licenses to install the desktop version of Office on their own computers.	Create their own personal sites (formerly referred to as My Sites), edit their profile, change their photo, or see aggregated tasks. External users don't get their own OneDrive for Business document library.

Perform tasks on a site consistent with the permission level that they are assigned For example, if you add an external user to the Members group, she will have Edit permissions and she will be able to add, edit, and delete lists. She will also be able to view, add, update, and delete list items and documents.	Be an administrator for a site collection (except in scenarios for which you've hired a partner to help manage Office 365. You can designate an external user as a designer for your Public Website. Note: The SharePoint Online Public Website information applies only if your organization purchased Office 365 prior to March 9, 2015. If you purchased Office 365 after March 9, 2015, use an Office 365 website hosting partner.
See other types of content on sites. For example, they can navigate to	See the company-wide newsfeed

different subsites within the site collection to which they were invited. They will also be able to do things like view site feeds.	
	Add storage to the overall tenant storage pool
	Access the Search Center or carry out searches against "everything." Other search features that might not be available include Advanced Content Processing, continuous crawls, and refiners.
	Access site mailboxes
	Access Microsoft Power BI features such as Power View, Power Pivot, Quick Explore, or Timeline Slicer. These features require

	an additional license, which is not inherited by external users.
	Use eDiscovery. This requires an Exchange Online license
	Open downloaded documents that are protected with Information Rights Management (IRM).

External sharing features of SharePoint Online

SharePoint Online external sharing features include the following:

- You can turn on or turn off external sharing globally for an entire Office 365 SharePoint Online Tenant. Turning external sharing off at the tenant level completely prevents the sharing of documents, sites, or site collections.
- You can turn on or turn off external sharing for individual site collections. This provides you with the ability to secure content on

specific site collections, making it possible for you to selectively manage private and shared content.

- You have the ability to share sites and documents with authenticated users. Authenticated users are those who are invited to sign in by using a [Microsoft account](#) or [work or school account](#).
- The ability to share documents with *guest users*. Guest users, also called *anonymous users*, don't need a [Microsoft account](#) or [work or school account](#) to access documents. These users access the document via a guest link which is essentially an anonymous link to access the specifically shared item.

For a business to make the best use of external sharing, it needs to carefully plan the approach to sharing options so as not to grant unnecessary access to content that otherwise should not be shared. It is also worth noting that the external sharing feature is turned on by default for your entire SharePoint Online tenant and the site collections within it. Many companies will opt to turn off this feature across the entire tenant to prevent accidental sharing until they have determined how they will make the best use of it.

You have a lot of flexibility when setting up external sharing, so you'll want to spend some time considering your options. You can configure sharing across the tenant, giving all users the capability to share. Or, you can limit sharing to certain site collections to reduce the number of people who can share to just the administrators of those sites. Finally, you can also limit the ability to share sites and documents to a select group of users.

When considering if and how you want to share content externally, think about the following:

- When granting access to content, to whom should the access be granted and what level of access should they have?
- To whom in your organization do you want to grant permission to share content externally?
- Is there content that should never be shareable with anyone outside the business? Perhaps the site contains confidential data or must not be shared for compliance reasons.

Planning for external sharing should be a part of your permissions planning for Office 365 SharePoint Online, and, where possible, you should ensure that you have solid control over

what content can be shared and by whom. A good security practice is to follow the *principal of least privilege*, which ensures that not only are you limiting the scope of the content that can be shared, but you are also limiting the audience of users who can share it. Some good concepts to follow as a part of this approach would be to consider segmenting the content into silos of shareable and nonshareable information, perhaps also separating the shareable information into bands of different security levels.

Configuring external sharing

You can configure the external sharing feature in a number of different ways, as just discussed. We should begin by assuming the global administrator has left the tenant-level sharing configuration as per the default settings (see Figure 5-1). This leads us to the scenario in which we can set different sharing policies at the site collection level.

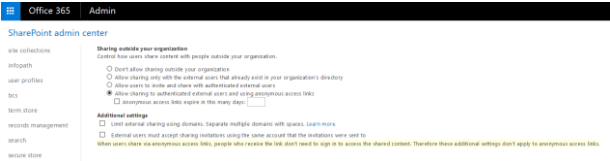


Figure 5-1: The default tenant-level sharing settings.

With the default configuration for external sharing, the SharePoint Online administrator can now choose to set individual sharing policies per site collection. To set these policies, in the SharePoint Admin Center, on the ribbon, click the Site Collections tab, and then click Sharing, as illustrated in Figure 5-2.

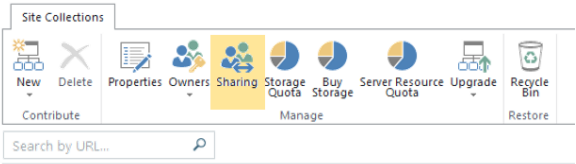


Figure 5-2: The available option on the Site Collections tab of the SharePoint Online site collection administration ribbon.

This opens the Sharing dialog box in which you can select the appropriate policy options. Figure 5-3 shows the available options when the tenant has the default properties selected.

sharing

Sharing outside your company

Control how users invite people outside your organization to access content

☐ Don't allow sharing outside your organization

☐ Allow sharing only with the external users that already exist in your organization's directory

☐ Allow external users who accept sharing invitations and sign in as authenticated users

☒ Allow sharing with all external users, and by using anonymous access links

Allowing non-owners to invite new users

Status: Allowed. This is the default setting for new sites.

Some sites in this site collection allow non-owners to grant permission to files, folders, or sites and sub-sites without requiring owner approval. [Learn more](#)

[Turn off sharing for non-owners on all sites in this site collection.](#)

Changes will be applied to the following 1 site collections:

URL	SHARING
https://contoso.sharepoint.com	Share links and invitations

Save

Cancel

Figure 5-3: Using the Sharing dialog box, you can configure policy options for the individuals or groups with whom you want to share.

Also in the Sharing dialog box, there is an additional option to restrict sharing to site owners only. By default, anyone can share any item they have access to with any external users. By turning off sharing for non-owners on all sites

in this site collection, you can begin implementing a more restrictive sharing regimen which leads us onto the concept of partner-facing extranet-type scenarios for which content access is more likely to require restrictive policies. Figure 5-4 shows the change after selecting this option. We will look specifically at the partner-facing extranet scenario later in the chapter.



Figure 5-4: Change to the site collection sharing status when non-owners are blocked from sharing.

In addition to the features used to restrict the sharing to sites and users, there is a relatively new change implemented in Office 365 SharePoint Online by which SharePoint administrators can restrict which email domains can access the shared sites.

Using the Restricted Domains sharing feature for SharePoint Online business-to-business

extranet sites and OneDrive for Business

The Office 365 tenant administrator now has an additional feature with which to manage the secure sharing experience when collaborating with external partners. At a tenant level, administrators can limit sharing invitations to a limited number of email domains by listing them in the Allow List or opt to use the Deny List, listing email domains to which users are prohibited to extend invitations. Figure 5-5 shows how the global administrator has configured a tenant to allow sharing only with fabrikam and tailspintoys.

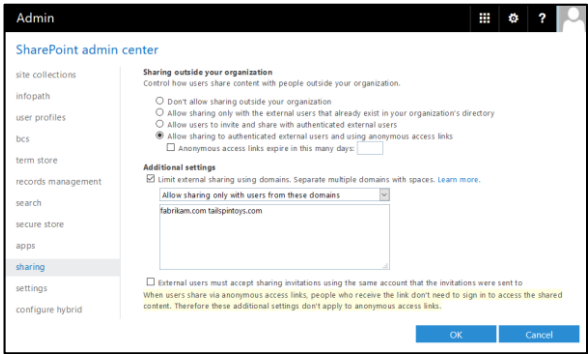


Figure 5-5: The Sharing page in the SharePoint Admin Center, showing external sharing turned on for users only in the fabrikam and tailspintoys domains.

You cannot configure the external domains list with wildcard domain entries, nor can you alter it at site-collection level. This list applies to all sites across the tenant.

The Windows PowerShell Set-SPOTenant cmdlet has been modified to allow configuration of restricted domains by using Windows PowerShell. Three new parameters have been added:

- SharingDomainRestrictionMode
- SharingAllowedDomainList
- SharingBlockedDomainList

The following example adds fabrikam.com and tailspintoys.com to the allowed domain list and sets up the Allow List feature:

```
Set-SPOTenant -SharingAllowedDomainList "adatum.com  
fabrikam.com" -SharingDomainRestrictionMode  
AllowList
```

You need to have the SharePoint Online Management Shell version 16.0.4915.1200 to use these new parameters. If you don't have it already, you can download it from <http://go.microsoft.com/fwlink/?LinkID=761521&clcid=0x409>.

Planning for external sharing

The external sharing feature is a powerful tool, and in some cases it can be overlooked as a means to bring business partners into a collaborative relationship. In other cases, it is looked upon with suspicion by security teams because company information could be accidentally shared by the untrained user, resulting in data breach or loss of company intellectual property. What is critical to remember, however, is that Microsoft provides all the capability to allow or restrict access to the content of sites.

So far in this chapter, we have looked only at the basic settings to allow or deny sharing. Next, we will look at the additional settings a business can use to create a true partner-facing extranet where business partners can be invited to collaborate and share content, secure in the knowledge that the policies in place will protect the information on the site. Before we look at this, though, there are some planning concepts for external sharing that the administrator must be aware of and take into consideration when setting up external sharing. These concepts can be divided into global and site-level concepts.

Global sharing planning considerations

You can plan for sharing at the Global level by considering actions that will have tenant-wide effect. These actions usually cannot be overridden by the site collection administrators.

- If external sharing is turned off for the entire SharePoint Online environment, you will not be able to turn it on for specific site collections.
- If external sharing is turned off for the entire SharePoint Online environment, any shared links will stop working and external users will lose access to the shared content. If the feature is later reactivated, links will resume working and external users will regain the previous access. It is also possible to turn off individual sharing links if, for example, you want to permanently revoke access to a specific document.
- If you know that external sharing was previously turned on and in use for specific site collections and you do not want external users to be able to regain access if external sharing is ever turned on again globally, we recommend that you first turn off external sharing for those specific site collections.

- If you turn off external access, or limit external access to a more restrictive form, external users will typically lose access within one hour of the change.

Site collection–level considerations

With site collection–level planning, you can begin to scope the sharing configuration down to the purpose of the site. The settings will be a superset of the tenant-level settings, however; thus, you cannot bypass tenant-level controls.

- The external sharing settings for individual site collections cannot be less restrictive than whatever is allowed for the entire SharePoint Online environment, but these settings can be more restrictive. In essence, the sharing configuration of a site collection can match or be a subset of the settings defined at the SharePoint Online tenant level.
- Sharing settings on the My Site collection (e.g., <https://contoso-my.sharepoint.com>) will apply to the OneDrive for Business sites for all users of the organization. You cannot selectively manage sharing for a particular user's OneDrive for Business site. Individual users will be able to control what is shared on their own OneDrive sites, assuming that

the global administrator has turned on sharing at the root level.

- When you turn off external sharing at the site-collection level, all external user permissions for that site collection will be permanently deleted. This is distinctly different from turning off sharing at the tenant level.
- When you turn off external sharing at the site-collection level, guest links will be turned off, but they could begin working again if external sharing is ever turned on again. If you want to permanently revoke access to specific documents, you will need to turn off the anonymous guest links in the Sharing dialog box.

Managing external users and invitations

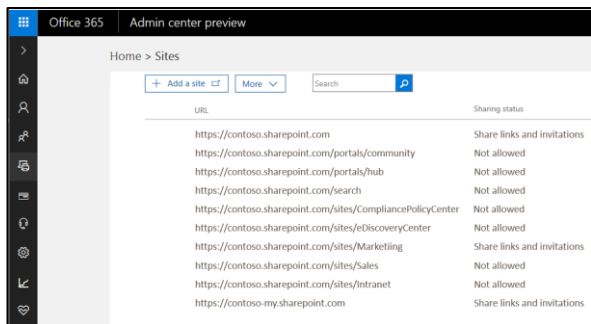
After you have turned on external sharing for the tenant and/or site collection and established sharing permissions, authorized users can send invitations, create guest links, and revoke access, and so on.

More info Walking through all the different ways to share content is beyond the scope

of this chapter, but for complete instructions on sharing sites and documents, go to <https://support.office.com/article/Share-sites-or-documents-with-people-outside-your-organization-80e49744-e30f-44db-8d51-16661b1d4232>.

Although we have some excellent controls to manage the sharing features, the retrospective viewing of what has been shared with whom is more difficult to view and manage.

You can use the Office 365 Admin Center Preview site to view the new admin experience. In this preview, you can view the sites and see the sharing configuration, as shown in Figure 5-6



Office 365 Admin center preview	
Home > Sites	
+ Add a site More Search	
URL	Sharing status
https://contoso.sharepoint.com	Share links and invitations
https://contoso.sharepoint.com/portals/community	Not allowed
https://contoso.sharepoint.com/portals/hub	Not allowed
https://contoso.sharepoint.com/search	Not allowed
https://contoso.sharepoint.com/sites/CompliancePolicyCenter	Not allowed
https://contoso.sharepoint.com/sites/eDiscoveryCenter	Not allowed
https://contoso.sharepoint.com/sites/Marketing	Share links and invitations
https://contoso.sharepoint.com/sites/Sales	Not allowed
https://contoso.sharepoint.com/sites/Intranet	Not allowed
https://contoso-my.sharepoint.com	Share links and invitations

Figure 5-6: The Sites list page in the Office 365 Admin Center showing the Sharing Status.

Selecting any one of the sites in this list presents additional information about the site. The global administrator is also presented with options to further control the settings, as depicted in Figure 5-7.

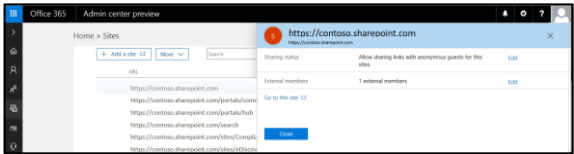


Figure 5-7: Global administrators can view and control additional settings for a site, including the Sharing Status and External Members count of a selected site.

Although external users have no way to view all the items shared with them, internally licensed users can navigate to their profile site and view the Shared With Me page to see a list of all the items shared with them by other internal users. Equally, there is no global way to see a list of all the sites to which an external user has access. You need to go to the individual sites to determine whether a specific user has access to it. There is also no global way to see a list of all documents that have been shared externally. One way to get visibility of all the shared content in your tenancy is to use the Compliance Search feature in the Compliance Center by using the ViewableByExternalUsers property in a search query. For more information, go to

<https://support.office.com/article/Keyword-queries-and-search-conditions-for-Content-Search-c4639c2e-7223-4302-8e0d-b6e10f1c3be3>.

Partner-facing extranet scenario

The natural evolution of external sharing is to develop scenarios that make business-to-business (B2B) collaboration possible in a secure manner. Extranet sites provide a way for partners to securely conduct business with your organization. The content for your partner is kept in one place and that partner has only the content and access it needs. Your partner doesn't need to email the documents back and forth or use some tools that are not sanctioned by IT. Traditionally, this has been done by using extranets

More info Microsoft has published some guidance for SharePoint extranet scenarios at [https://technet.microsoft.com/library/cc263513\(v=office.14\).aspx](https://technet.microsoft.com/library/cc263513(v=office.14).aspx).

There are a number of common factors that all of these extranet configurations share. All of them require one or more firewalls with complex

rule sets to pass user traffic and sometimes SharePoint, SQL, or Active Directory traffic. Complex security settings are often needed on the servers themselves including compliance-level security hardening, especially in public government, military, health, or financial sectors. Add to this the additional complexity of Secure Sockets Layer (SSL)/Transport Layer Security (TLS) certificate management and how to handle the external partner user identities, and you can see how this becomes an expensive, time-consuming scenario both to deploy and operate. To quote Seshadri Mani, principal program manager with the SharePoint OneDrive team, "...you need a Ph.D. in 'SharePointology' to deploy an effective SharePoint extranet."

With Office 365 SharePoint Online, you can change the paradigm of extranet sites. Partners connect directly to a members-only site in Office 365, without access to the corporate on-premises environment or any other Office 365 site. Office 365 extranet sites can be accessed anywhere, bringing flexibility to the relationship, too. If you consider the industry verticals where B2B collaboration is key to success, the list is almost endless. Just considering example industries such as automotive, manufacturing, retail, and energy, you can readily reel off a list of household-name businesses within each of

those verticals. All of them highly dependent on a partner ecosystem to develop and grow their businesses.

Office 365 SharePoint Online uses the B2B collaboration feature set to provide the partner-facing extranet capability.

SharePoint Online B2B collaboration features

SharePoint Online B2B collaboration features are made up of the capabilities discussed already in this chapter. In summary, it includes the following key capabilities of SharePoint Online:

- **SPO cloud B2B** In an SPO cloud B2B, you can have both intranet and extranet (B2B) sites in the same SharePoint Online tenant. You can allow users to initiate sharing but implement control from a central IT function.
- **Site owners-only sharing** This adds the ability to have site collections where only owners can invite or share with new users. Site members—who are typically external partner users—can see only the existing site members in the site. This goes a long way toward limiting the ability of external users to see into the corporate directory via the

people picker function, something that was previously impossible to control in SharePoint Online. It also prevents external users from sharing the content they have been invited to see; again, this provides additional protection of the content in the partner access sites so that the company can be sure no accidental or intentional oversharing is possible. For more details, go to <https://support.office.com/article/Create-a-partner-facing-Extranet-Site-in-Office-365-c40d4670-7f6c-4719-9c6f-8dee36220a48>.

- **Allow users to invite new partner users**

In certain site collections, administrators can optionally allow users to invite new partner users. In this model, an email invitation is sent to the partner user and the user must redeem that invitation by following the embedded link in the email to access the resource. For more details, go to <https://support.office.com/article/Manage-external-sharing-for-your-SharePoint-Online-environment-C8A462EB-0723-4B0B-8D0A-70FEAFE4BE85>.

- **Restricted domains sharing**

Administrators can control the list of partner domains outside the organization with which their employees can share. Administrators

can configure either an allow-list of email domains or a deny-list of email domains. With this newer capability, the business has another level of security over the sharing functions. By using the restricted list in an allow mode, the administrators can define the exact domains with which their users can share. In the deny-list mode, you only specify particular blocked domains and all others are available. For more details, go to <https://support.office.com/article/Restricted-Domains-Sharing-in-Office-365-SharePoint-Online-and-OneDrive-for-Business-5d7589cd-0997-4a00-a2ba-2320ec49c4e9>.

- **Auditing and reporting** Activities of the business partner users are audited and reports can be viewed in Office 365 Activity Reports. As with many corporate functions, it is critical to have a clear and accurate audit trail of the administrator and user activity. For more details, go to <https://support.office.com/article/Use-sharing-auditing-in-the-Office-365-audit-log-50bbf89f-7870-4c2a-ae14-42635e0cfc01>.

Example B2B scenario using hybrid extranet features

Figure 5-8 depicts Contoso, Ltd, a company whose core business is based on collaboration with partners such as suppliers, financial establishments, and distributors.

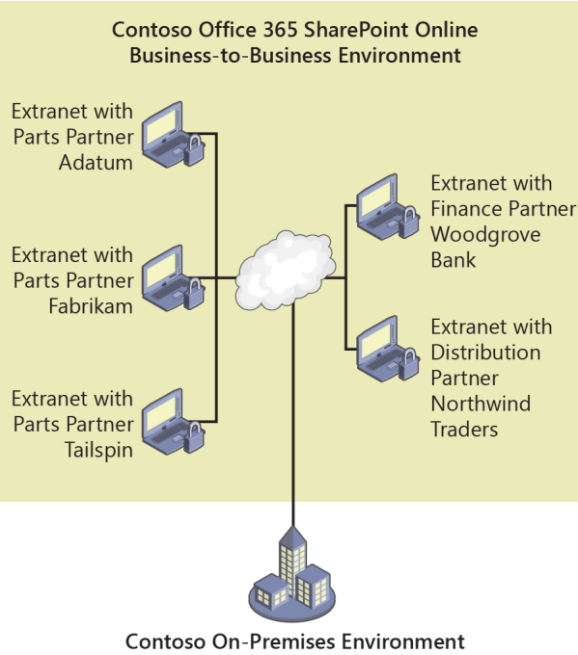


Figure 5-8: A representation of a hybrid extranet configuration in which Contoso on-premises users are able to collaborate with a variety of partner companies through the use of extranet B2B features.

Let’s take a look at what it takes to deploy this kind of extranet capability. The following table demonstrates the ease with which you can implement it in Office 365 SharePoint Online versus a traditional deployment approach.

Function	Office 365 hybrid extranet	SharePoint on-premises extranet
Firewall access required to external users	No	Yes
Complex network and infrastructure configuration required	No	Yes
Security hardening	Managed through Office 365 configurations	Manually configured by IT staff
IT Labor intensive	No	Yes

Ongoing maintenance needed	Minimal	Considerable
Additional hardware needed	No	Often
Managing external partner users; locally managed or cloud managed	Yes	Locally managed only
Controlling sharing experience for extranet sites	Part of Office 365 sites functionality	Often requires custom solutions/apps

We have already discussed the planning guidance for partner-facing extranet sites and provided home details and reading on how to configure them. The preceding table provides a clear view of the implementation differences, too.

Summary

Office 365 SharePoint Online extranet features can be a crucial element for fostering business growth. It provides the flexibility to expand the number of extranet sites without complex infrastructure or management changes. Because costly on-premises extranets are eliminated, there is no additional capital expenditure needed; thus, the IT department can focus on new projects and more important tasks than repetitive management activities.

Sharing is safeguarded by design in that it can provide a secure experience on your terms and using the IT governance, control, and policies dictated by your company. Granular controls are available to prevent accidental sharing and limiting the partner domains with which your users can collaborate. Partner users are constrained within the site they are invited to and cannot search for or see content beyond that boundary, including access to the list of Azure Active Directory users. You can also restrict partners to have enforced sign-ins using only the email account that was used for the sharing invitation.

You can configure additional collaboration, including giving your partners access to Skype

for business features such as instant messaging and conference calls.

Finally, Office 365 SharePoint Online offers visibility into the access of your content by external partner users. One of the key IT benefits is to be able to audit usage, including being able to see who is inviting whom and when an external user signs in to access the content.

Troubleshooting Microsoft SharePoint hybrid issues

This chapter is designed to give you a good hands-on overview of how to detect and troubleshoot many of the problems commonly seen in SharePoint hybrid setups. It is not a substitute for Microsoft Customer Support Services, but it will hopefully help you to fix most issues. If you need to open a Microsoft Customer Support Services case, the tips and

techniques you will learn throughout this chapter will assist in obtaining the required forensic information to provide to the support engineer.

Introduction

When Microsoft trains its support engineers in the customer support organization, the first thing the engineers are taught to do is properly scope-out the problem they are being asked to resolve. This scoping consists of defining the nature of the error condition, and, just as important, defining the success criteria so that the issues can be resolved to the satisfaction of all parties. When you are troubleshooting, we absolutely recommend that you take the same approach and consider the scope of the problem at hand. This will help you to home in on the possible causes of whatever problem you are presented with. Thus far, this ebook has focused on the key hybrid architectures with SharePoint and Microsoft Office 365; if you need to, refer

back to each relevant section as you scope and isolate the source of the issue at hand.

As you progress through this chapter, we will follow a similar set of guidelines, starting with the basics and progressing through the diagnostics process, providing real-world examples and scenarios along the way. This approach will help you to diagnose and remediate problems you might face when deploying SharePoint on-premises and SharePoint Online as a hybrid solution.

Troubleshooting approach

Many of the hybrid issues raised by customers to Microsoft support can be traced back to a set of common problems or deployment errors. When faced with a broken hybrid deployment, there is a preferred process for diagnosis. This diagnosis is based on a process of elimination whereby the most common possible causes are eliminated first, followed by the second most common, and so on and so forth, until the actual root cause of the problem is determined. In some cases, fixing one problem will reveal another, therefore it is important to isolate and resolve problems area by area, as opposed to trying to provide a one-stop solution for all hybrid problems.

Getting the basics right

When we look back to the early days of hybrid deployment with Office 365 and SharePoint, there are a number of common issues that crop up more frequently than others. In the main, these issues boil down to one key element of the hybrid deployment process: getting the basic prerequisites implemented correctly, especially the core identity requirements. We will therefore begin this hybrid troubleshooting chapter with some good practices for validating that the identity management setup is working as required before we move on to troubleshooting the actual hybrid workloads.

Validating directory synchronization

Before you can embark on any hybrid deployment scenario, it is critical that the identities of the users and groups who will participate in the workload have been successfully synchronized to Azure Active Directory by using one of the supported tools. At this stage, we are assuming that the directory synchronization process was working successfully earlier, so here we are looking for evidence of a post deployment problem.

Note: All Office 365 tenant experiences will be described for the new modern tenant admin pages only. As of this writing, the modern portal is in preview but is available via a link in the current admin portal, which you can access at <https://portal.office.com/adminportal/home?switchtomodern=true#/homepage>.

The first place to check for directory synchronization issues is by signing in to the Office 365 Admin Center and checking the Dashboard page. The dashboard shows a directory synchronization status tile (see Figure 6-1), which presents statistics about the synchronization health. You should ensure that the directory synchronization process is healthy before proceeding. If the tile does not show on the Dashboard, directory synchronization has not been turned on in the tenant, and you should follow the guidance in [*Planning and Preparing for Microsoft SharePoint Hybrid*](#) to set it up—without it, all hybrid scenarios will fail.

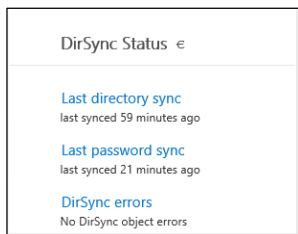


Figure 6-1: The DirSync status tile in the Office 365 Admin Portal. This tile shows a healthy status.

If the directory synchronization tile shows an error or warning state such as that shown in Figure 6-2, directory synchronization has been turned on but for some reason is broken.

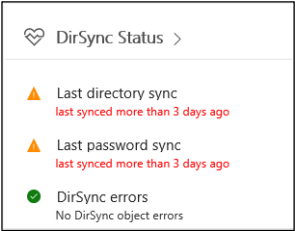


Figure 6-2: The Office 365 DirSync status tile showing an unhealthy status.

At this point, you can click the Last Directory Sync message on the tile to go to the Directory Sync Status page. The page contains several pieces of useful management information. Figure 6-3 shows a warning that an earlier version of the DirSync client was used. For the moment this isn't a concern, but in 2017 Microsoft intends to stop older versions of the sync client from working, and so upgrade is recommended. Also on the status page, you can see a couple of synchronization warnings along with links to the DirSync troubleshooting tool. The DirSync troubleshooting tool is a click-once app and

must be run on the DirSync server. It has two troubleshooting options: Quick Scan and Full Scan. Quick Scan reviews the DirSync server event logs and the Office 365 settings. Full Scan is more detailed and includes a scan of the active directory objects for potential errors.

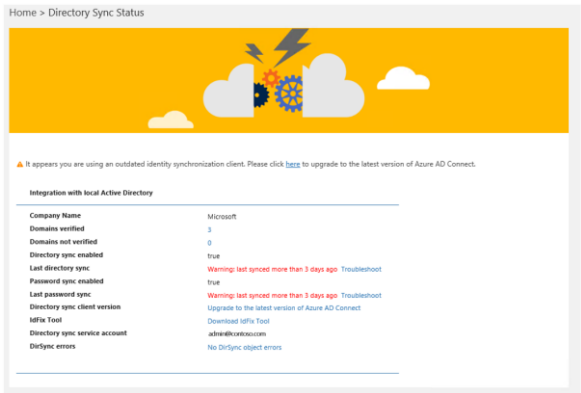


Figure 6-3: DirSync status dialog box.

There is another link to a useful troubleshooting tool on the Directory Sync Status page: IdFix is an Active Directory Object analyzer tool that can highlight problems with objects in Active Directory that will cause synchronization errors. IdFix is reviewed in [Planning and Preparing for Microsoft SharePoint Hybrid](#) as part of the Active Directory preparation steps.

More info You can find additional reading to help fix directory synchronization errors at <https://support.office.com/article/Fixing-problems-with-directory-synchronization-for-Office-365-79c43023-5a47-45ae-8068-d8a26eee6bc2?ui=en-US&rs=en-US&ad=US>.

Another approach to troubleshooting directory synchronization issues is to open the Microsoft Identity Integration Server (MIIS) client tool (Synchronization Service Manager tool), which is located on the Synchronization Server at C:\Program Files\Microsoft Azure AD Sync\UIShell\MIISClient.exe.

Figure 6-4 demonstrates that The MIISClient gives administrators a quick view of the state of synchronization and whether there are any connectivity or access issues between on-premises and Azure Active Directory.

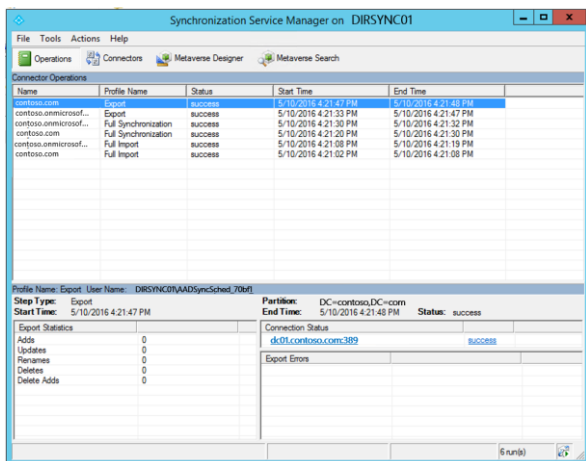


Figure 6-4: The Synchronization Service Manager client (MIISClient.exe) tool.

You will see errors in this client tool if there are connectivity issues between the on-premises Azure Active Directory Connect (Azure AD Connect) Server and the Office 365 Tenant. Some common errors are listed in this Microsoft TechNet guide to the MIISClient at [https://technet.microsoft.com/library/ee323428\(v=office.13\).aspx](https://technet.microsoft.com/library/ee323428(v=office.13).aspx). The guide is quite old now, but it is still a valuable resource for reviewing the error messages.

The range of problems is too broad for us to do a deep dive into troubleshooting all of them;

however, the most commonly seen synchronization error in the MIISClient is a status being reported for the Azure Active Directory agent (contoso.onmicrosoft.com, in Figure 5-4) of Stopped-Server-Down. This message tends to make the administrator believe that there is a network connectivity issue somewhere or the Azure Active Directory instance cannot be contacted for some reason. The most common cause of this error is in fact when the password for the account specified as the synchronization account during Azure AD Connect installation has expired or been changed. There are two ways to fix this issue:

- Rerun the Azure AD Connect Configuration tool from the beginning
- Modify the Account Password in the MIISClient tool

We do not recommend modifying the password in the MIISClient tool unless you have a thorough understanding of the Microsoft Identity Management product. Instead, we recommend running the Azure AD Connect Configuration tool to provide the updated credentials.

After you are satisfied that the directory synchronization process is working correctly and

there are no errors in the DirSync tile on the Office 365 Admin Portal, you can move the troubleshooting process to the next stage.

Validating the Azure Access Control Services server-to-server trust

At the heart of the hybrid workloads with SharePoint Server and Office 365 is a configuration element that forms the bridge between the on-premises and Online environments. Windows Azure Active Directory Access Control Service (ACS) is a cloud-based federation service that provides an easy way to authenticate users against identity providers and, most important of all, Azure Active Directory. With ACS being core to everything hybrid, it can affect all workloads when it is broken. Configuring ACS is described in Chapter 1, where you can follow the process step by step. This same step-by-step approach to configuring ACS means that we also have a step-by-step approach to validate the configuration to ensure everything is working as expected. The best way to carry out the validation is by using Windows PowerShell.

You can use the script blocks that follow to validate that the server-to-server (S2S) trust with ACS has been correctly configured.

First, let's ensure that we have the information we need to commence troubleshooting. This will consist of the certificate created or obtained to set up the ACS trust originally. We also need the Office 365 SharePoint Online App ID.

```
$stscertpfx="c:\certs\stscert.pfx"  
$stscertpassword="*****"  
$spoappid="00000003-0000-0ff1-ce00-000000000000"
```

Note If you used the Hybrid Picker or the Cloud Search Service Application onboarding script, you will not have this certificate in hand. In this case, however, it is safe to assume the scripts will match because it's the same certificate that's used to configure the trust.

When you create or obtain a certificate, you need to confirm this certificate is being used for token signing in SharePoint on-premises. You do this by checking the thumbprints of the certificates match.

```
#Validated STS Token Signing certificate thumbprint  
$pfxCertificate=New-Object  
System.Security.Cryptography.X509Certificates.X509Certificate2 $stscertpfx, $stscertpassword, 20  
$pfxCertificate  
(Get-
```

SPSecurityTokenServiceConfig).LocalLoginProvider.SigningCertificate

The output from this script should show matching certificate thumbprints.

Thumbprint	Subject
-----	-----
CC1727BDFADD43A1445C55331B4FE829E9B821F1	
CN=sharepoint01.contoso.com	
CC1727BDFADD43A1445C55331B4FE829E9B821F1	
CN=sharepoint01.contoso.com	

You next need to validate that the certificate used for the token signing has not expired. If it has, this will result in token signing issues typically seen as JWT token errors in the user interface or Unified Logging Service (ULS) logs.

```
#Validate Certificate is not expired
Connect-MsolService
Get-MsolServicePrincipalCredential -AppPrincipalId
"00000003-0000-0ff1-ce00-000000000000"|ft
startdate,enddate ,keyid -autosize
```

Output at this stage will show the current certificate and any previously deployed certificates that might have been replaced. The example that follows shows two certificates registered against the Office 365 Application Principal. One has expired, and the other is a newer one with a much longer expiry date. For your information, an expiry date of 1/1/9999 for a hybrid certificate usually indicates the built-in SharePoint Security Token Signing Certificate was used to form the trust. If you do not have

any valid certificates configured for the ACS trust, you must deploy a new one. You can deploy a new certificate by using the steps highlighted in Chapter 1 or else rerun a Hybrid Picker or Cloud Search Service Application onboarding script to re-create the trust.

StartDate	EndDate	KeyId
-----	-----	-----
11/22/2015 1:15:24 PM	1/1/9999 12:00:00 AM	fe45ae88-30cf-4254-9b4a-c507825dccfe
5/5/2015 6:47:23 PM	5/5/2016 12:00:00 AM	fa4c9828-adaa-43ef-9af7-8875fbb7140d

The next thing you should check for the ACS configuration to work is to validate that the Service Principal Names (SPNs) registered against the Office 365 application principal match the expected sources of the on-premises user requests.

```
#Validate SPNs setup properly in AAD
$app = Get-MsolServicePrincipal -AppPrincipalId
"00000003-0000-0ff1-ce00-000000000000"
$app.ServicePrincipalNames
```

The output from the script should show one or more SPNs that cover the SharePoint web application URLs from which outbound requests will be received or inbound requests will be sent. In the example that follows, you can see the SPN value for a wildcard matching *.contoso.com. This wildcard means that any web application with the fully qualified domain name (FQDN)

ending in contoso.com will be covered by this SPN.

```
00000003-0000-0ff1-ce00-000000000000/*.contoso.com
00000003-0000-0ff1-ce00-
0000000000000000/*.sharepoint.com
00000003-0000-0ff1-ce00-000000000000
Microsoft.SharePoint
```

One thing to be wary of with SPNs is preventing the addition of multiple SPNs that cover the same URLs. For example, if the output from the script were as shown in the example that follows, we would have a duplicate SPN clash because the wildcard covers all possibilities, and the explicit SPN for intranet.contoso.com isn't required. This is something that you should avoid.

```
00000003-0000-0ff1-ce00-000000000000/*.contoso.com
00000003-0000-0ff1-ce00-000000000000/intranet.
contoso.com
00000003-0000-0ff1-ce00-
0000000000000000/*.sharepoint.com
00000003-0000-0ff1-ce00-000000000000
Microsoft.SharePoint
```

To remove a duplicate SPN, you can use the following script:

```
$app = Get-MsolServicePrincipal -AppPrincipalId
"00000003-0000-0ff1-ce00-000000000000"
$app.ServicePrincipalNames.RemoveAt(1)
Set-MsolServicePrincipal -AppPrincipalId
$app.AppPrincipalId -ServicePrincipalNames
$app.ServicePrincipalNames
```

The indexer value, in this case (1), should be replaced with the ID of the SPN to remove. For the preceding example, this would remove the intranet.contoso.com SPN but leave the wildcard. This is because the wildcard could be in use for other purposes; however, because the wildcard also covers the SPN we are removing, there is no functional loss.

The final step in validating that the ACS trust is set up correctly is to ensure that the ACS ServiceApplicationProxy has been deployed successfully. SharePoint communicates to the ACS service endpoints via the ServiceApplicationProxy, and thus ensuring that it's deployed and online is critical to the ACS trust implementation.

```
#Validate on premises ACS Proxy
$proxy =Get-SPServiceApplicationProxy | ?
{$_ .typeName -eq "Azure Access Control Service
Application Proxy"}
$proxy | ft Name, Status, MetadataEndpointUri -
autosize
```

The output from the script should show the proxy as online and is the endpoint for ACS.

Name	Status	MetadataEndpointUri
----	-----	-----
ACS Proxy	Online	https://accounts.accesscontrol.windows.net/7d22a111-2888-458c-85d5-e26862e29fc6/metadata/json/1

One additional troubleshooting validation step at this point would be to check that the on-premises SharePoint servers are able to communicate to the MetadataEndpointUri. If you copy the URL and navigate to it by using a web browser, you should be prompted to download a file, 1.json, which contains the certificate and key details that could be useful for troubleshooting with Microsoft support. If you cannot access the file, you should verify that the servers have outbound Internet access.

Certificate validation in isolation

While we are on the topic of certificates, it is worth looking at the means of validating certificates generally. If you have suspicions or evidence that a certificate might be invalid for some reason, you can use the Active Directory Certificate Services tool, CertUtil.exe, to perform certificate verification. CertUtil.exe has many additional features, which you can read about at <https://technet.microsoft.com/library/cc732443.aspx>, but for this chapter, we will focus on just one: verification.

Using the command line as an administrator, run the following:

```
certutil -verify contoso.cer > certverify.txt
```

The output here is captured in the `certverify.txt` file, and you can examine it for evidence about problems with the certificate. In this example, we have tested a deliberately expired certificate, which is the most commonly seen error. The entries in the `certverify.txt` file to look for are similar to the following:

```
----- CERT_CHAIN_CONTEXT -----
ChainContext.dwInfoStatus =
CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
ChainContext.dwErrorStatus =
CERT_TRUST_IS_NOT_TIME_VALID (0x1)
ChainContext.dwRevocationFreshnessTime: 5 Days, 13
Minutes, 33 Seconds

SimpleChain.dwInfoStatus =
CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
SimpleChain.dwErrorStatus =
CERT_TRUST_IS_NOT_TIME_VALID (0x1)
SimpleChain.dwRevocationFreshnessTime: 5 Days, 13
Minutes, 33 Seconds
```

If the certificate is part of a chain, you will see the validation of the chain listed here, and of note is the line `ChainContext.dwErrorStatus = CERT_TRUST_IS_NOT_TIME_VALID (0x1)`, indicating the certificate trust is not time valid; in other words something in the certificate chain has expired.

Also in the output file, you can locate the specific certificate and the specific error message. Further details of the certificate are revealed, such as its purpose and the subject details.

```

CertContext[0][0]: dwInfoStatus=102 dwErrorStatus=1
  Issuer: CN=DigiCert SHA2 Secure Server CA,
O=DigiCert Inc, C=US
  NotBefore: 01/05/2015 01:00
  NotAfter: 11/05/2016 13:00
  Subject: CN=*.contoso.com, OU=o365, O=Department
X, L=Phoenix, S=Arizona, C=US
  Serial: 0f845869f5545522fb3798e14d1844e6
  SubjectAltName: DNS Name=*.contoso.com, DNS
Name=contoso.com
  Cert: 8a7983ec05323fad0edbf5c4fc1ed558ab4d5a84
  Element.dwInfoStatus =
CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2)
  Element.dwInfoStatus =
CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
  Element.dwErrorStatus =
CERT_TRUST_IS_NOT_TIME_VALID (0x1)
  CRL 0186:
    Issuer: CN=DigiCert SHA2 Secure Server CA,
O=DigiCert Inc, C=US
    ThisUpdate: 10/05/2016 18:03
    NextUpdate: 17/05/2016 18:00
    CRL: 5ad51d5a8ada6cc2da927440972cb076d02d6a70
  Issuance[0] = 2.16.840.1.114412.1.1
  Application[0] = 1.3.6.1.5.5.7.3.1 Server
Authentication
  Application[1] = 1.3.6.1.5.5.7.3.2 Client
Authentication

```

Finally, at the end of the output file, a simple explanation for the problem with the certificate is provided.

A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file.
0x800b0101 (-2146762495 CERT_E_EXPIRED)

Expired certificate

After analyzing the certificate, you are armed with enough information to know whether it

needs to be replaced. If you recall, when configuring hybrid search in particular, there are multiple certificates involved and certificate management can often be controlled by another part of the business. Using `certutil.exe` to validate and record information about any certificates before using them will help you to set up appropriate steps to alert the business to the certificate renewal period. Replacing expired certificates is covered in the Chapter 7

Validating the Active Directory Federation Services infrastructure

Active Directory Federation Services (AD FS) is key to assisting with single sign-on (SSO) in Office 365; however, it doesn't play a direct role in the implementation of hybrid scenarios. However, there are some redirection scenarios such as Hybrid Sites and Microsoft OneDrive that could break if AD FS is not working. With that in mind, you are encouraged to test that AD FS is working by simply signing in to the portal by using a federated account. If AD FS sign-in is working, this is not going to be the source of a broken hybrid deployment. If AD FS is not operating as expected, you should follow the Microsoft Premier Field Engineer troubleshooting guidance at

<https://blogs.technet.microsoft.com/askpfeplat/2015/06/14/adfs-deep-dive-troubleshooting/>.

Hybrid workload troubleshooting

There are many SharePoint server and Office 365 hybrid workloads described throughout this book, and most if not all are dependent on the prerequisite topics we have already discussed in this chapter. Over time with the adoption of hybrid deployments, support has been sought among the community via forums and social media. In addition to this, the same hybrid support cases have been raised in Microsoft by users of hybrid workloads. This next section will review some specific troubleshooting techniques and common problems for each of the workloads.

Troubleshooting account

There is one important factor you must understand before beginning troubleshooting. To set up hybrid workloads, the signed-in user must have a degree of administrative control over the feature being configured. For example, to configure or test a site collection–level result

source, you must be a site owner or administrator.

When we look at hybrid troubleshooting, you must have this same level of administrative control over the feature being tested. You also must be correctly synchronized, licensed, and permissioned for that feature in Office 365 SharePoint Online. Testing with a nonsynchronized account or an account without license or permission will prevent accurate troubleshooting of the problem. A classic example of this is trying to use a Domain Administrator account for testing: this account is never synchronized to Azure Active Directory in Office 365 and therefore cannot reproduce the problem in the same context as a regular user. You can use the Fiddler tool to demonstrate this and other authentication issues for hybrid scenarios. We highly recommend Fiddler as a primary troubleshooting tool here; it can provide some valuable pointers to help isolate the potential cause of the problem. If you use Fiddler to compare the difference between a valid and invalid troubleshooting account, it will help you to learn to use the tool for other scenarios.

Let's get underway. Sign in as a domain administrator to an on-premises search center that is configured for outbound hybrid search

and submit a search query. This results in an unauthorized exception, as illustrated in Figure 6-5.

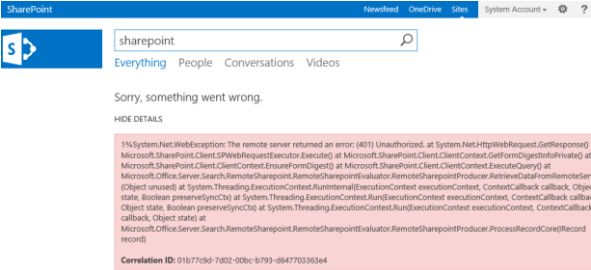


Figure 6-5: SharePoint Enterprise Search center showing an unauthorized request from the search engine.

If you look at the Fiddler trace for the same request, you can see a similar access denied response from the Query Processor, which is evidenced by the two 401 responses depicted in Figure 6-6.

#	Result	Protocol	Host	URL	Body	Caching	C
1	401	HTTPS	sharepoint.contoso.com	/sites/Search/_api/contextinfo	16		ts
2	401	HTTPS	sharepoint.contoso.com	/sites/Search/_api/contextinfo	0		
3	200	HTTPS	sharepoint.contoso.com	/sites/Search/_api/contextinfo	542	private...	a
4	200	HTTPS	sharepoint.contoso.com	/sites/Search/_v8_bin/dent.svc/ProcessQuery	721	private	a

Figure 6-6: Fiddler trace for unauthorized request to the Office 365 search service.

Fiddler can be extremely useful for debugging multiple web-based applications; however, in hybrid scenarios, the best forensic evidence is actually presented back to the administrator or

user within the browser itself. This will become clearer as we look at the troubleshooting concepts in the remainder of this chapter.

Chapter 8 discusses hybrid account management and practice.

Troubleshooting hybrid search federation

By far the most commonly implemented hybrid feature of SharePoint Server and SharePoint Online is hybrid search federation. This might be as a result of it being the first hybrid workload delivered for SharePoint Online, but it is also a reflection of the benefit it offers to organizations working within the Office 365 space.

The simplest of all search federation scenarios is, of course, outbound query federation wherein the local search service on-premises forwards a user-submitted search request to the remote search service in SharePoint Online. Although this is the simplest scenario, it is actually identical to the query federation process used in inbound query federation and when deploying the Cloud Search Service Application. Let's begin by looking at the first steps in troubleshooting the most common of all hybrid search-related problems: seeing no search results. Before

loading up your toolkit and doing a deep forensic investigation, there are two simple built-in tests that you absolutely should do first.

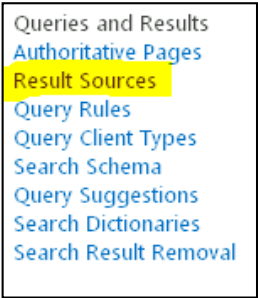
Testing the result source

All query federation requests are sent to the Remote SharePoint Endpoint URL defined in the result source configuration (see Chapter 2). To facilitate successful connections to Search Service Applications, there is a test functionality that will simulate the remote call and provide the results to the person doing the testing. Result source has an Edit Control Block (ECB) that gives administrators a way to view, copy, and edit the source. In addition to this, there is an additional row labeled Test Source.

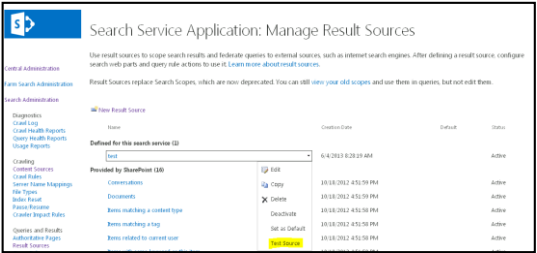
Selecting this option issues a query for “Microsoft” against the result source through the Query Processor. While running the query, a message box appears with the statement, Testing *<name of source>*. After the test is complete, the results are displayed in the message box. The message box has a Cancel button that lets you end the test without viewing the results. Administrators can perform this test on result sources configured at the Search Service Application level, site collection, and web level; the procedure is the same for all. Complete

the following steps to carry out this test in the Search Service Application:

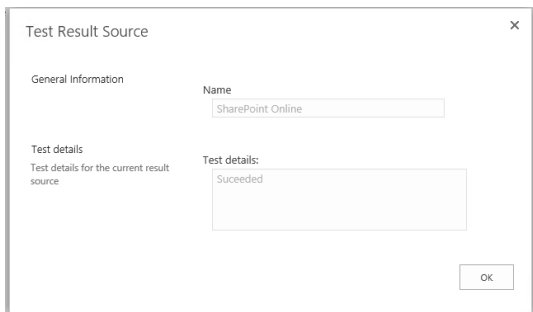
- 1. On the Central Administration home page, in the Application Management section, click Manage service applications.
- 2. In the navigation pane on the left, click Result Sources.



- 3. On the Manage Result Sources page, click Test Source, as shown here:



4. After the test is complete, the results will be displayed in the Test Result Source dialog box.



Here are a few of the common errors that you might see when testing result sources (see also Figure 6-7):

- **404 – URL not found** This error displays a message stating that either the location URL is typed incorrectly or it is not configured correctly. Options presented are Edit and OK.
- **ID3242; The security token could not be authenticated or authorized** This error indicates that the certificate used for the on-premises Security Token Service (STS) and uploaded to ACS to complete the S2S trust is invalid and usually implies it has expired.

- **401 – Unauthorized** This error displays a message stating that the credentials provided could not authenticate against the URL and need to be corrected. Options presented are Edit and OK.

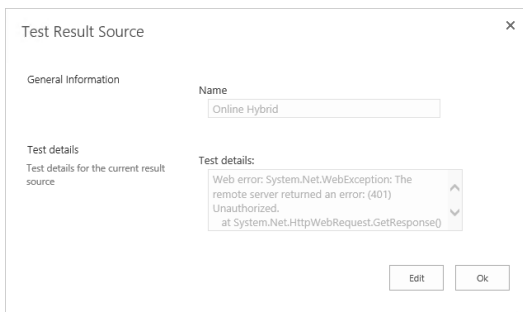


Figure 6-7: The Test Result Source dialog box.

The error messages that are returned give you an indication of what needs to be fixed to restore hybrid search functionality.

Testing Query Builder

You typically use Query Builder for supplementing the search query with additional parameters and then to test the response. You also can use Query Builder to validate your search configuration and gather troubleshooting information if required. Like the result source testing, you can validate the query at multiple

places including Central Administration for the Search Service Application, site collection, and web level. Here we walk through testing at the site-collection Level:

1. On the Site Settings page, in the Site Collection Administration section, click Search Query Rules.
2. From the Select Result Source list box, select any result source.
3. Click Add New Query Rule.
4. On the Add New Query Rule page, click the Add Result Block option.
5. On the Configure Result Block page, click the Launch Query Builder button.
6. From the Select A Query list box, choose the result source for SharePoint Online
7. In the box next to {Subject Terms}, type a search term of your choice, and then click Test Query. (Hint: "*" is also a valid search term)

Relevant search results will be displayed in the Search Result Preview window if your configuration is valid, as demonstrated in Figure 6-8. If there are problems with your

configuration, troubleshooting information will be displayed.

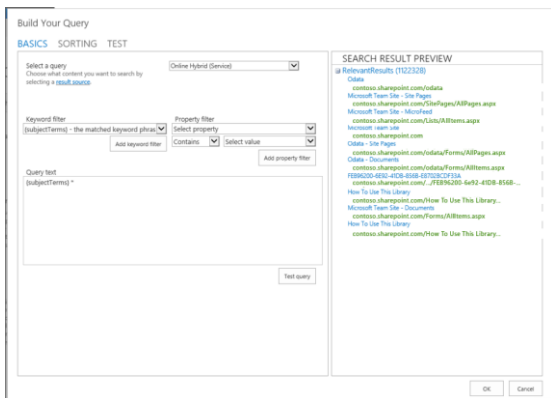


Figure 6-8: Query Builder being used to validate a query rule configuration.

If there is a problem with the configuration of the query federation setup, you might see some errors. These errors might be the same as those observed when testing the result source or you might see different ones.

Typically, the Query Builder will display a stack trace, such as that shown in Figure 6-9, which can be very valuable in diagnosing the problem should there be one.

configure them to maximize the data collected for hybrid-specific categories.

The easiest way to do this is to use Windows PowerShell, as demonstrated here:

1. Open a SharePoint Management Shell session and run the following command for all of the aforementioned parameters:

```
Set-SPLogLevel -EventSeverity verbose -  
TraceSeverity verbose -Identity"SharePoint  
Foundation:App Auth","SharePoint Foundation:  
Application Authentication"."SharePoint  
Foundation: Authentication Authorization  
","SharePoint Foundation: Claims Authentication"
```

2. Before you reproduce the issue, run the command that follows to start a new logfile. A new logfile makes it easier to extract the relevant ULS logs from the troubleshooting period.

```
New-SPLogFile
```

3. After you are done gathering the logs, you should then run the command that follows to reset the logging back to default. This avoids generating huge log files unnecessarily, which can lead to drive space issues.

```
Clear-SPLogLevel
```

Tracing a hybrid federated search query through ULS Logs

The following ULS log examples demonstrate a user, johndoe@contoso.com, issuing a search for the word "Hybrid" on a search center configured for outbound query federation:

```
04/29/2016 16:45:29.55 NodeRunner.exe
(0x10D4) 0x170C SharePoint Foundation
Claims Authentication airze
Verbose Current identity context: '{"nameid":"s-1-5-21-2907032475-1458376993-4227282505-2527",
"nii":"urn:office:ldap:activedirectory", "upn":"johndoe@contoso.com", "userId":"0#.w|contoso\\johndoe", "app
liesTo":"http://os1/"}' 496d5f8e-fd2e-484c-af40-9a6a84c752bb
```

The name identifier issuer (nii) claim indicates here that we are using Windows authentication because the nii parameter has the value of urn:office:ldap:activedirectory.

If the name identifier was issued by a [SAML](#) identity provider, the nii value will be similar to urn:office:ldap:trusted:samlprovidername, where *samlprovidername* is the name of the SAML provider.

```
04/29/2016 16:45:29.55 NodeRunner.exe
(0x10D4) 0x170C SharePoint Foundation
Claims Authentication airzh Medium
Using UPN ' johndoe@contoso.com' for SMTP claim
496d5f8e-fd2e-484c-af40-9a6a84c752bb
05/29/2016 16:45:29.55 NodeRunner.exe
(0x10D4) 0x170C SharePoint Foundation
Application Authentication ahilz
```

```
Verbose Created OAuth2 bearer credentials:
{"claims":{"nameid":"s-1-5-21-2907032475-1458376993-4227282505-2527","nii":"urn:office:idp:activedirectory","upn":"johndoe@contoso.com","smtp":"johndoe@contoso.com"}}
496d5f8e-fd2e-484c-af40-9a6a84c752bb
```

The “Using UPN for SMTP” line shows up if UPN matches SMTP (which it frequently does). The remainder of the ULS logs will show a progression through the query federation process, as shown in the following log extracts, culminating in a Received results for query response:

```
04/29/2016 16:45:30.25 NodeRunner.exe
(0x10D4) 0x170C SharePoint Foundation
Application Authentication ahi15
Verbose OAuth2 S2S Bearer Token:
eyJ0eXAiOiJKV1QiLCJhbGciOiJub251In0...<content
truncated for clarity>
xODEiLCJuYW1laWQiOiJLTETNS0yMS0yOTA3MDMyNDc1LTE0NTgz
Nz YSOTMtnNDIyNzI4Q1J5eXdIVkNmTWY3ZmRRIn0
496d5f8e-fd2e-484c-af40-9a6a84c752bb
05/29/2016 16:45:31.05 NodeRunner.exe
(0x10D4) 0x170C SharePoint Foundation
Application Authentication age6e
Verbose Authenticating OAuth2 Bearer challenge.
496d5f8e-fd2e-484c-af40-9a6a84c752bb
05/29/2016 16:45:31.05 NodeRunner.exe
(0x10D4) 0x170C SharePoint Foundation
Application Authentication airzp Verbose
Using delegated user OAuth2 bearer credentials.
496d5f8e-fd2e-484c-af40-9a6a84c752bb
05/29/2016 16:45:31.05 NodeRunner.exe
(0x10D4) 0x170C SharePoint Foundation
Application Authentication age6i Verbose
Issuing OAuth2 S2S token for identity '00000003-0000-00ff1-ce00-000000000000/intranet.contoso.com@f954db15-77c8-4e18-9ac2-aa4570164a78'. tokenType: 1
```

```

496d5f8e-fd2e-484c-af40-9a6a84c752bb
05/29/2016 16:45:31.05 NodeRunner.exe
(0x10D4) 0x170C SharePoint Foundation
Application Authentication aiiws Verbose
Built client name identifier: 00000003-0000-0ff1-
ce00-000000000000@f954db15-77c8-4e18-9ac2-
aa4570164a78 496d5f8e-fd2e-484c-af40-
9a6a84c752bb
05/29/2016 16:45:31.05 NodeRunner.exe
(0x10D4) 0x170C SharePoint Foundation
Monitoring nasq Verbose
Entering monitored scope (Issue OAuth2 user
delegation token). Parent Authenticate OAuth2 Bearer
challenge 496d5f8e-fd2e-484c-af40-
9a6a84c752bb
05/29/2016 16:45:31.05 NodeRunner.exe
(0x10D4) 0x170C SharePoint Foundation
Application Authentication age6k
Verbose Getting OAuth2 actor token for identity
'00000003-0000-0ff1-ce00-000000000000/
intranet.contoso.com @f954db15-77c8-4e18-9ac2-
aa4570164a78'. 496d5f8e-fd2e-484c-af40-9a6a84c752bb
05/29/2016 16:45:31.91 NodeRunner.exe
(0x10D4) 0x170C SharePoint Server Search
Query ad7p4 Verbose
QueryRouterEvaluator: Received results for query
HYBRID 496d5f8e-fd2e-484c-af40-9a6a84c752bb

```

You should use the preceding ULS extracts as a reference point for troubleshooting your own hybrid experiences. The logs show a successful authorization and query response from SharePoint Online. The information you gather from the ULS logs on your own SharePoint farm will be invaluable to a Microsoft support professional should you be unable to remediate it yourself; save these logs and submit them with a case.

Scenario-based troubleshooting

When you have problems with hybrid scenarios there are many different probable causes and each has its own remediation. We will go ahead and look at some common errors and problems that you might come across in configuring and maintaining a hybrid deployment, but this is by no means an exhaustive list. The blog here documents a series of hybrid problems and their fixes or workarounds. It is frequently updated with new solutions to problems as they are discovered. You can find the articles at <https://blogs.technet.microsoft.com/beyondsharepoint/2016/06/13/welcome-to-beyond-sharepoint/>. We will now review a number of commonly seen problems and their resolutions.

Expired STS certificate

When the STS certificate has expired, the system is not able to issue a valid security token for the request.

```
05/11/2016 15:46:44.54 w3wp.exe (SP01:0x143C) 0x1478
SharePoint Foundation Topology 8311 Critical An
operation failed because the following certificate
has validation errors: Subject Name:
CN=sp01.contoso.com Issuer Name: CN=sp01.contoso.com
Thumbprint: CC1727BDFADD43A1330C55331B4FE829E9B821F1
```

Errors: NotTimeValid: A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file. 59277b9d-1dbc-00bc-b793-d61ba24c5c3d

05/11/2016 15:46:44.56 w3wp.exe (SP01:0x0630) 0x0FF8 SharePoint Foundation Claims Authentication 8306 Critical An exception occurred when trying to issue security token: ID3242: The security token could not be authenticated or authorized. 59277b9d-1dbc-00bc-b793-d61ba24c5c3d

This situation can arise when a new self-signed or public-signed certificate is used to configure the hybrid setup. These certificates will have an expiry date, unlike the default STS certificate, which does not. We discuss replacing the STS and ACS Trust certificates in Chapter 8.

The errors here will manifest when a user attempts to invoke any hybrid scenario that relies on the S2S Oauth2 trust between on-premises SharePoint and the Azure ACS.

Hybrid features that utilize this S2S trust are the following:

- Outbound query federation
- Inbound query federation
- Hybrid Business Connectivity Services
- Hybrid Sites Features when initiated by using the Hybrid Picker

If you suspect that you have provided all the required permissions and configuration details for the accounts that are utilizing the hybrid workloads, check for these errors in the ULS logs and begin a certificate validation process before looking for additional sources of error.

Search Service Application proxy in partitioned mode

Another surprisingly common problem seen with outbound hybrid search in particular is when a farm has been built to support multitenant properties. This could be deliberate for a company doing on-premises hosting or by accident when community available scripts have been used as the baseline for an automated farm build. When a Search Service Application is deployed to support multitenancy, it is configured in partitioned mode. If this partitioned mode is set on either the Search Service Application or the service application proxy, it will attach an on-premises subscription ID to the outbound search query. This subscription ID is unique to the on-premises farm and therefore does not exist in SharePoint Online, resulting in a Not Found error. If you check Query Builder, the error will be as shown here:

```

1 3/4 System.Net.WebException: The request was
aborted: The request was canceled. --
>Microsoft.SharePoint.IdentityModel.OAuth2.SPOAuth2E
rrorResponseException: The remote server returned an
error: (404) Not Found. at
Microsoft.SharePoint.IdentityModel.OAuth2.SPOAuth2Cl
ient.GetResponse(Uri stsurl,
OAuth2AccessTokenRequest message) at
Microsoft.SharePoint.IdentityModel.OAuth2.SPOAuth2Cl
ient.RequestOAuthToken(Uri stsUrl.
OAuth2AccessTokenRequest request) at stsInfo,
OAuth2EndpointIdentity endpointIdentity) at
Microsoft.SharePoint.IdentityModel.OAuth2.SPOAuth2Se
curityTokenManager.GetRawBearerToken(String
nameIdentifier,
SPSecurityTokenServiceConnectionInformation stsInfo.

```

And the following exception is logged in the ULS log:

```

An exception occurred during OAuth2 request to <url
specific to your site>
The remote server returned an error: (404) Not
Found. at System.Net.HttpWebRequest.GetResponse() at
Microsoft.SharePoint.IdentityModel.OAuth2.SPOAuth2Cl
ient.GetResponse(Uri stsUrl,OAuth2AccessTokenRequest
message)

```

It might be that the on-premises Search Service Application has been deliberately provisioned in partition mode, and if that is the case, you should be aware that hybrid features are not designed to work in this situation. In addition, it is not considered to be a supported configuration. If the configuration as a partitioned service was not intended, the fix is to flip the tenantization properties of the service application and proxy into a non-tenantized

mode. You can do this by using Windows PowerShell as follows (for further information you can review the Microsoft support article at <https://support.microsoft.com/kb/2989740>):

```
$proxy = get-spenterprisesearchserviceapplicationproxy
$proxy.Properties["Microsoft.Office.Server.Utilities
.SPPartitionOptions"] = 0
$proxy.Update()
$ssa = get-spenterprisesearchserviceapplication
$ssa.SetProperty("IgnoreTenantization",1)
$ssa.Update()
```

Inbound hybrid user rehydration fails

When you issue inbound hybrid calls from Office 365 to SharePoint on-premises, that call is sent along with your identity claims. The claims are used to rehydrate your account context so that the call can complete using your permissions in the on-premises farm. The April 2014 Cumulative Update to SharePoint Server 2013 made a change to support audiences across alternate access mappings for hybrid scenarios. This change introduced an unfortunate regression that broke a key component of this rehydration feature, namely OrgID claims mappings.

If you are planning to deploy SharePoint on-premises and configure inbound Hybrid Search to return results in SharePoint Online from a

Microsoft SharePoint Server 2013 on-premises environment, this regression will show up when a user performs a query from a SharePoint Online site. Only results from the SharePoint Online sites are displayed and no results are returned from SharePoint Server 2013 on-premises.

If you follow the guidelines that we just presented and use a result source or query rule to investigate the problem, the response will look something like this:

```
SharePoint Foundation Claims Authentication af3zp
Unexpected STS Call Claims Saml: Problem getting
output claims identity. Exception:
'System.InvalidOperationException: Exception of type
'System.ArgumentException' was thrown. Parameter
name: value ---> System.ArgumentException: Exception
of type 'System.ArgumentException' was thrown.
Parameter name: value at
Microsoft.SharePoint.Administration.Claims.SPIdentity
Providers.GetIdentityProviderType(String value) at
```

If you are implementing hybrid BCS, this issue will also give you problems, albeit they will manifest in a different error:

The following error occurred: The internet facing URL for the LobSystem (External System) returned an authentication error. Error was encountered at or just before Line: '57' and Position: '20'.

The clue here to what is wrong is the message Problem getting output claims identity. With the OrgID Rule mapping missing, we have no way to recognize an incoming claim. Without

being able to recognize the claim, we have no means of rehydrating the user account to one that can be recognized on-premises.

Microsoft has documented the fix for the problem as a knowledge base article, which you can access at

<https://support.microsoft.com/kb/3000380>.

To fix the issue, you can use Windows PowerShell to add the claims mapping back to the system, as demonstrated here:

```
$config = Get-SPSecurityTokenServiceConfig
$config.AuthenticationPipelineClaimMappingRules.AddIdentityProviderNameMappingRule("OrgId Rule",
[Microsoft.SharePoint.Administration.Claims.SPIdentityProviderTypes]::Forms, "membership",
"urn:federation:microsoftonline")
$config.Update()
```

As of this writing, this remains a problem in the most recent update to SharePoint Server including the release build of SharePoint Server 2016 (Version 16.0.4327.1000). We recommend implementing the fix as part of your standard build process for SharePoint Server until such a time as Microsoft incorporates the fix in a product update.

Mismatched certificates on inbound configuration

Configuring secure inbound connections for hybrid scenarios is more complex than simple outbound connectivity. Inbound connections are used when deploying BCS hybrid and also inbound hybrid search federation. To protect the on-premises environment from casual browsers or network port sniffing, Microsoft strongly recommends a multiple certificate approach to securing the endpoint. This of course means that you have a bigger change to go through when renewing and deploying these certificates. If any one of these certificates has expired, you have a problem, but also there are requirements for two of these certificates to match exactly, and if they don't match, you have a different problem. In each case, though, certificate problems mean broken hybrid scenarios.

We have looked at validating expired certificates already. The response from mismatched certificates is different, however, and results in an access denied response. If you imagine the scenario, this is equivalent to presenting the wrong user name and password at a sign-in

prompt. Testing with Query Builder yields the following response:

```
1%System.Net.WebException: The remote server
returned an error: (401) Unauthorized. at
System.Net.HttpWebRequest.GetResponse() at
Microsoft.SharePoint.Client.SPWebRequestExecutor.Exe
cute() at
Microsoft.SharePoint.Client.ClientContext.GetFormDig
estInfoPrivate() at
Microsoft.SharePoint.Client.ClientContext.EnsureForm
Digest() at
Microsoft.SharePoint.Client.ClientContext.ExecuteQue
ry() at
Microsoft.Office.Server.Search.RemoteSharepoint.Remo
teSharepointEvaluator.RemoteSharepointProducer.Retrie
veDataFromRemoteServer(Object unused) at
System.Threading.ExecutionContext.RunInternal(Execut
ionContext executionContext, ContextCallback
callback, Object state, Boolean preserveSyncCtx) at
System.Threading.ExecutionContext.Run(ExecutionConte
xt executionContext, ContextCallback callback,
Object state, Boolean preserveSyncCtx) at
System.Threading.ExecutionContext.Run(ExecutionConte
xt executionContext, ContextCallback callback,
Object state) at
Microsoft.Office.Server.Search.RemoteSharepoint.Remo
teSharepointEvaluator.RemoteSharepointProducer.Proce
ssRecordCore(IRecord record)
```

You cannot download the Secure Store certificate to check it, so the easiest way to validate for mismatched certificates being the cause of the problem here is simply to obtain a copy of the certificate again and upload it again to the Secure Store in Office 365 SharePoint Online. Then, check if the ThumbPrint matches the certificate configured for certificate preauthentication on the reverse proxy.

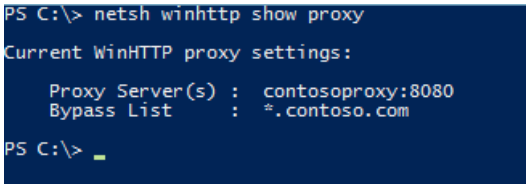
Alternatively, just republish the SharePoint web application again on the Web Application Proxy, using the latest copy of the certificate for client preauthentication. You need to ensure that it is the exact same one you uploaded to Office 365 SharePoint Online Secure Store. Also, it's important to note that when uploading the certificate to the Secure Store, Office 365 does not validate that you provided the correct password, only that the two passwords you typed match. Make sure you use the correct password for the certificate private key. If working on a remote console, make sure the keyboard isn't remapping keys; for example, commonly the " and @ characters and the £ and # are reversed on an English GB keyboard versus an US English keyboard.

Outbound proxy authentication

With outbound hybrid search-based scenarios, there is a requirement for components of the SharePoint farm on-premises to be able to access the Internet. In particular, this is true for outbound query federation, for which the search query processor needs to be able to contact the Office 365 SharePoint Online root site collection. It is also important in the Cloud Search Service Application for which the crawler needs to be able to contact the Search Content Service

hosted in Azure and, if query federation from on premises has been configured, the Query Processor also requires outbound access to the Office 365 SharePoint Online root site collection.

Many companies still implement proxy infrastructure for a variety of reasons, and if you are having outbound search federation problems, check the proxy settings on the servers in the farm running the query processing component by using the netsh command at an elevated command prompt, as illustrated in Figure 6-10.

A screenshot of a Windows command prompt window with a dark blue background and white text. The prompt shows the command 'netsh winhttp show proxy' being executed. The output displays the current WinHTTP proxy settings: 'Current WinHTTP proxy settings:' followed by 'Proxy Server(s) : contososproxy:8080' and 'Bypass List : *.contoso.com'. The prompt ends with 'PS C:\> _' where the underscore represents a cursor.

```
PS C:\> netsh winhttp show proxy
Current WinHTTP proxy settings:
    Proxy Server(s) : contososproxy:8080
    Bypass List      : *.contoso.com
PS C:\> _
```

Figure 6-10: Using the Netsh command to check the proxy configuration on a Query Processor server.

When this command returns a value, it is very common to find that this is the cause of outbound access-denied errors or onboarding connectivity issues. As Figure 6-11 demonstrates, clearing the setting is simple, again by using netsh.

```
PS C:\> netsh winhttp reset proxy
Current WinHTTP proxy settings:
    Direct access (no proxy server).
PS C:\> _
```

Figure 6-11: Using the netsh command to reset the system proxy to default, which is no proxy.

Testing again usually results in the problem being resolved.

OneDrive and site redirection issues

The one drive redirection process is pretty difficult to get wrong, but we do come across situations in which misconfiguration causes problems or users do not get the correct configuration to be able to participate. Chapter 4 covers the correct way to configure the OneDrive redirection and hybrid sites setup, so if you are having issues with these features, we recommend reviewing the setup before seeking additional reasons for something being wrong.

An uncommon source of OneDrive redirection issues is a failure to initialize the MySite, which leaves the user in a broken state, not able to migrate to OneDrive for Business even if the user is configured as a member of the audience

selected for migration. You can detect the state of the OneDrive configuration for users by reading the user profile properties via Windows PowerShell.

```
$ca = Get-spwebapplication -  
includecentraladministration | where  
{$_ .IsAdministrationWebApplication}  
$spsite = $ca.url  
$site = Get-SPSite $spsite  
$context = Get-SPServiceContext $site  
$upsa = New-Object  
Microsoft.Office.Server.UserProfiles.UserProfileMana  
ger($context)  
$profile = $upsa.GetEnumerator()  
$profile
```

Then, validate the following fields:

```
$userprofile.PersonalSiteFirstCreationError  
$userprofile.HybridRemotePersonalSiteHostUrl
```

A value in the `PersonalSiteFirstCreationError` could indicate a provisioning problem occurred when the user first requested the creation of her OneDrive for Business site. As the administrator, you have a simple choice to make here. Try to fix the issue or just delete the offending broken OneDrive and ask the user to try again.

Assuming that you do delete the OneDrive, you should validate the

`HybridRemotePersonalSiteHostURL` before asking the user to re-create her OneDrive for Business, as depicted in Figure 6-12. This value should match the MySite Host url for the Office

365 tenant where the hybrid features are being implemented.

```
PS C:\> $userProfile.RemotePersonalSiteHostUrl.AbsoluteUri
PS C:\> $userProfile.HybridRemotePersonalSiteHostUrl.AbsoluteUri
https://contoso-my.sharepoint.com
PS C:\>
```

Figure 6-12: Validating the RemotePersonalSiteHostUrl value.

As long as this value matches the expected value and the hybrid settings are configured as required, the user can re-create her OneDrive for Business and will redirect to Office 365.

The type name for the Secure Store provider is not valid

If you are configuring a hybrid BCS scenario, you have implemented the option to use the on-premises Secure Store Service Application as the credential store for access to the on-premises data, as shown in Figure 6-13.

Authentication
The authentication type required by the OData data source.

☐ Don't use authentication
☐ Use user's identity
☒ Use credentials stored in SharePoint on-premises
☐ Use OData Extension Provider

Secure Store Target Application ID:

Authentication Mode

- Impersonate Custom Identity
- Impersonate Window's Identity
- Impersonate Custom Identity Digest
- Impersonate with Client Certificate

Internet-facing URL
The internet facing URL that

Figure 6-13: Configuring the Hybrid BCS Secure Store authentication mode.

A common problem observed here manifests itself as a somewhat misleading error message in the user interface on the SharePoint BCS Management page when trying to import the BCS Model file. The error is The Type Name For The Secure Store Provider Is Not Valid. This comes about when using SharePoint Server 2013 on-premises and occurs because of the difference in build version between on-premises and SharePoint Online. SharePoint Online has been running on Build Version 16 code for quite some time now, and you need to factor that in to the on-premises deployment

The fix for this issue is to make a change in the web.config of your on-premises SharePoint Server 2013 web application to make it compatible with SharePoint Online. Here's how to do that:

```
<dependentAssembly xmlns="urn:schemas-microsoft-com:asm.v1">  
<assemblyIdentity  
name="Microsoft.Office.SecureStoreService"  
PublicKeyToken="71e9bce111e9429c" culture="neutral"  
>  
<bindingRedirect oldVersion="16.0.0.0"  
newVersion="15.0.0.0" />  
</dependentAssembly>
```

This change causes the model file to be validated against the SharePoint Server 2013 or Version 15 of the secure store binaries and prevent the error occurring.

Cloud Search Service Application is working, but expected items are not returned when querying

In this scenario, users are able to sign in to the Office 365 or on-premises search center and issue a successful search query. However, some expected items are not available in the search results even though the users have access to the items in on-premises.

This situation is very specific to the Cloud Search Service Application and can occur under some very specific conditions. To understand how this problem can arise, we need to look a little deeper at the ACL mapping process in the Search Content Service.

The ACL mapping process takes incoming ACLs from on-premises crawled content and matches the entries in the ACL with the equivalent entry in Office 365 Azure Active Directory. If no match is found, the entry is dropped from the ACL before the item is pushed to the search farm for processing. This can result in an unexpected situation as follows:

Contoso is using the cloud Search Services Application to crawl an on-premises site collection in SharePoint Server 2013. A new sales team Active Directory group is created and the site collection administrator adds their group to the site collection. Shortly after the group is granted access to the site, a search crawl runs that picks up the security change on the site from the SharePoint Server change log, successfully crawls the site, and feeds the changes to the Search Content Service in Office 365. Only after the crawl has run is the new Active Directory group synchronized to Office 365 Azure Active Directory during the scheduled synchronization process.

The preceding scenario will mean members of the new sales team group cannot find the information they were given permission to when searching. The crawl executed prior to the group being synchronized, which means that although

the ACL change was sent to the search content service, it would be dropped by the ACL mapper because no equivalent group could be found in Office 365 Azure Active Directory. Only after the group was synchronized does the group claim appear in Office 365 Azure Active Directory, but because the crawl has already occurred, it is too late to pick up that change and update the ACLs on the item in Office 365 Search Index. To remediate the problem, a full crawl or a security only crawl is required.

This problem could arise fairly frequently because there is no synchronization between crawl/content processing and the Azure AD Connect scheduling. So, unfortunately, if a crawl starts too early, Security Identifiers (SIDs) for unsynchronized users and groups are left untranslated and won't match the user or group claim in the user's token. Chapter 6 addresses this topic in further detail.

To help isolate the cause of this problem you should check the following steps:

- Check the crawl log in the on-premises Search Service Application to be certain that the item has been crawled successfully.
- Authenticate to SharePoint online as an affected user.

- Navigate to https://contoso.sharepoint.com/search/_api/search/query?querytext='*&Properties='QueryId entityDiagnostics:t' Where *contoso* is replaced by your tenant name

The very end of the XML output from this query (Figure 6-14) contains all the user claims that security trimming will receive, and if you don't see the Active Directory group claim that grants the user permission to the content, the items will always be missing from search results due to regular security trimming action.



Figure 6-14: The user claims diagnostics query output.

The claims for a user (user1) can be compared with the known groups applied to the on-premises content. If the expected group is

missing, this points to the root cause being the problem described previously.

Microsoft Support Assistance with Cloud Search Service Application

The previous scenario described a query-related problem and provided some guidelines for remediation. In this scenario, we will look at the crawler side and how you can gather information from the on-premises Search Service Application so that Microsoft support can assist your troubleshooting efforts.

Typical reasons to follow this procedure are when you suspect the problem might be on the index side, such as stale or duplicate search results. This will require you to open a case with Microsoft support; the support professional will then send you a Windows PowerShell script that will gather some information about the specific items of concern.

Figure 6-15 shows an example of the output.

```

C:\> get-hybriddocumentinfo.ps1 -displayurl https://sharepoint.contoso.com/sites/tradhybrid
-----
DocID: 54
7d22a080-2665-458c-85d5-d26862e29fc6/sp-site/763c1332-58ac-45da-a011-a010461372eb/0f08a534d6d2fbc026f7a3bfe70f95af87971871450304bcd018a970e93127
-----
displayurl : https://sharepoint.contoso.com/sites/tradhybrid
AccessURL  : STS4://sharepoint.contoso.com/sites/tradhybrid
Tenant     : 7d22a080-2665-458c-85d5-d26862e29fc6
SPIDindexType : sp-site/763c1332-58ac-45da-a011-a010461372eb
SCS Client ID : 0f08a534d6d2fbc026f7a3bfe70f95af87971871450304bcd018a970e93127
Last seen by crawler : 03/16/2016 12:04:49
-----
DocID: 57
7d22a080-2665-458c-85d5-d26862e29fc6/sp-site/763c1332-58ac-45da-a011-a010461372eb/10fae5755da082d6e77c2aa2f200f0182041b4346545e4648df79f844b7c5b9a
-----
displayurl : https://sharepoint.contoso.com/sites/tradhybrid
AccessURL  : STS4://sharepoint.contoso.com/sites/tradhybrid
Tenant     : 7d22a080-2665-458c-85d5-d26862e29fc6
SPIDindexType : sp-site/763c1332-58ac-45da-a011-a010461372eb
SCS Client ID : 10fae5755da082d6e77c2aa2f200f0182041b4346545e4648df79f844b7c5b9a
Last seen by crawler : 03/16/2016 12:04:49
-----
DocID: 62
7d22a080-2665-458c-85d5-d26862e29fc6/sp-site/763c1332-58ac-45da-a011-a010461372eb/d1959d99631548eb413efaf8028ab4b4e2eaf2acf16e9c9526caa77044116a58
-----
displayurl : https://sharepoint.contoso.com/sites/tradhybrid
AccessURL  : STS4://sharepoint.contoso.com/sites/tradhybrid
Tenant     : 7d22a080-2665-458c-85d5-d26862e29fc6
SPIDindexType : sp-site/763c1332-58ac-45da-a011-a010461372eb
SCS Client ID : d1959d99631548eb413efaf8028ab4b4e2eaf2acf16e9c9526caa77044116a58
Last seen by crawler : 03/16/2016 12:04:13

```

Figure 6-15: Output from get-HybridDocuemntInfo.ps1 showing a query for an index in the Office 365 Search Index and subsequent response.

When you run the script, you are prompted to supply the displayURL for the item. If the item is located in the search index, the response will include data about the item processing and unique identity in the Office 365 search index. You need to supply this information to your Microsoft support professional, who can then assist you with the specific problem at hand.

Summary

Troubleshooting is never an exact science. At times, it involves a lot of guesswork to find some clues that point you down the right track. Being able to understand the moving parts of a hybrid workload and the interdependencies between core elements and the feature itself is critical to developing a good troubleshooting approach. In this chapter, we focused on aspects that occur

most frequently and moved toward the less common. By eliminating the most common issues first you get a better understanding of what has possibly gone awry. Good use of troubleshooting tools where required can help you; however, the out-of-the-box SharePoint tools provide a lot of detailed debugging information that you can use to determine the source of the problem.

Administering Microsoft SharePoint hybrid by using Windows PowerShell

The content of this chapter is aimed at providing SharePoint and Microsoft Office 365 administrators with a set of post-deployment tools and operational practices to ensure that they can maintain the health and relevance of the hybrid platform for their end users.

Introduction

So far, this book has concentrated on the design, deploy, and configure aspects of a hybrid life cycle, looking into the different workloads, what they offer the business, and how we deploy them. This was then followed by troubleshooting the deployments and how to move forward when things go wrong. In an ideal world, we wouldn't need to look at troubleshooting our deployed infrastructure, but, as we know, ideal life is never the same as real life and the inevitable happens. Hardware breaks and must be replaced, certificates expire, users come and go, all leading to an interesting life for the administrator, and even more exciting when you throw hybrid deployments into the mix.

In this chapter, we focus on the latter half of the hybrid deployment life cycle, concentrating on the areas that fall within the Run, Maintain, and Operate categories, which are described here:

- **Run** The run state is the steady state of the deployment when it is in mainstream support for a production workload and is running efficiently.
- **Maintain** The maintain phase identifies the ongoing and periodic maintenance activities that support the run state. Allowing the

platform to operate to its peak by having effective maintenance tasks.

- **Operate** Operational aspects include the day-to-day tasks an administrator might perform during the run state. These activities can include onboarding new users and adding new sites.

Together these three states, if done well, will provide a business with an effective hybrid solution that is available to the users, is reactive to change when necessary, and can accommodate the demands of a business over time.

To be able to manage Office 365 effectively, you should become familiar with Windows PowerShell and especially the cmdlets related to SharePoint server and Office 365. There are a number of compelling reasons to make Windows PowerShell the priority when administering your tenant and the SharePoint Online features, not only for the hybrid workload aspects. Here are just a few of those reasons:

- Azure Active Directory module for Windows PowerShell can reveal additional information that you cannot see with the Office 365 admin center.

- Office 365 has features that you can configure only by using Windows PowerShell.
- Windows PowerShell is great at performing bulk operations.
- Windows PowerShell is great at filtering data.
- Windows PowerShell makes it easy to print or save data.
- Windows PowerShell lets you manage across server products.

Read the article at

<https://technet.microsoft.com/library/dn568034.aspx> to review these features in further detail along with examples. As you work through this chapter, we will provide additional examples that demonstrate the benefits enjoyed by Office 365 administrators by using Windows PowerShell.

Getting started with Windows PowerShell and Office 365 administration

Windows PowerShell is not baked into the Windows server operating system, and to be able to fully administer the Office 365 Tenant as well as SharePoint Online with Windows PowerShell, you need to download and install some additional components. You can separate these components into two groups. The first group contains the components for managing the Office 365 tenant and Microsoft Azure Active Directory. The second group contains the component needed for administering the SharePoint Online features within the tenant.

Let's look at the first group.

Installing Azure Active Directory module for Windows PowerShell

To provide support for administering the Office 365 tenant, you must download and install two components:

- **Microsoft Online Services Sign-In Assistant** This provides end-user sign-in

capabilities to Microsoft Online Services, such as Office 365. This is a prerequisite for Azure Active Directory module for Windows PowerShell installation. You can download it from

<https://www.microsoft.com/download/details.aspx?id=41950>.

- **Azure Active Directory module for Windows PowerShell** This is the Windows PowerShell module with which you can remotely manage Azure Active Directory.
<http://go.microsoft.com/fwlink/p/?linkid=236297>.

We would recommend validating that these components are installed on any workstation that will be used to administer the Office 365 tenant, including when administering hybrid features from the SharePoint server farm itself.

You can choose to manually download and install these components every time you configure a workstation, or place the script that follows in a shared location with the downloaded installers. Running the script checks for the presence of each component and installs it on the workstation if it is not already installed.

```
# This script installs the two required prerequisites:
```

```
# AdministrationConfig-EN.msi and msoidcli_64.msi.
# It is assumed that these are available in the
# same folder as the script itself.
# See the following links for downloading manually:
# - http://www.microsoft.com/en-us/download/details.aspx?id=41950
# - http://go.microsoft.com/fwlink/p/?linkid=236297
```

```
function Install-MSI {
param(
    [Parameter(Mandatory=$true)]
    [ValidateNotNullOrEmpty()]
    [String] $path
)
    $parameters = "/qn /i " + $path
try{
    $installStatement = [System.Diagnostics.Process]::Start( "msiexec", $parameters )
    $installStatement.WaitForExit()
}
catch{
    Write-Warning "Manual installation of prerequisites required."
}
}
$scriptFolder = Split-
Path $script:MyInvocation.MyCommand.Path
$MSOIdCRLRegKey = Get-ItemProperty -
Path "HKLM:\SOFTWARE\Microsoft\MSOIdentityCRL" -
ErrorAction SilentlyContinue
if ($MSOIdCRLRegKey -eq $null)
{
if(Test-Path $scriptFolder+"\msoidcli_64.msi"){
    Write-Host "Installing Office Single Sign On
Assistant" -ForegroundColor Yellow
    Install-MSI ($scriptFolder +
```

```

"\msoidcli_64.msi")
    Write-Host "Successfully installed!" -
Foreground Green
    }
    else{
        Write-Warning "Office Single Sign On Assistant
installer not downloaded !"
    }
else
{
    Write-Host "Office Single Sign On Assistant is
already installed." -Foreground Green
}
$MSOLPSRegKey = Get-ItemProperty -
Path "HKLM:\SOFTWARE\Microsoft\MSOnlinePowershell"
-ErrorAction SilentlyContinue
if ($MSOLPSRegKey -eq $null)
{
    if(Test-Path
$scriptFolder+"\AdministrationConfig-EN.msi"){
        Write-Host "Installing AAD PowerShell" -
Foreground Yellow
        Install-MSI ($scriptFolder +
"\AdministrationConfig-EN.msi")
        Write-Host "Successfully installed!" -
Foreground Green
    }
    else{
        Write-Warning "AAD PowerShell installer not
downloaded !"
    }
}
else
{
    Write-Host "AAD PowerShell is already

```

```
installed." -Foreground Green  
}
```

This script could be included in the initialization section of any Windows PowerShell scripts developed by Office 365 administrators. It will ensure that the required components are correctly deployed each time you run the script.

Connecting to Office 365

After you have successfully deployed the prerequisite components for administering your Office 365 tenant, it is time to make an authenticated connection to Azure Active Directory by using a Global Administrative account. For a description of the different administrative roles in Office 365, go to https://support.office.com/article/Assigning-admin-roles-in-Office-365-eac4d046-1afd-4f1a-85fc-8219c79e1504?ui=en-US&rs=en-GB&ad=GB#_choose_an_admin.

To connect to Office 365, use the Connect-MsolService cmdlet, as shown in Figure 7-1.

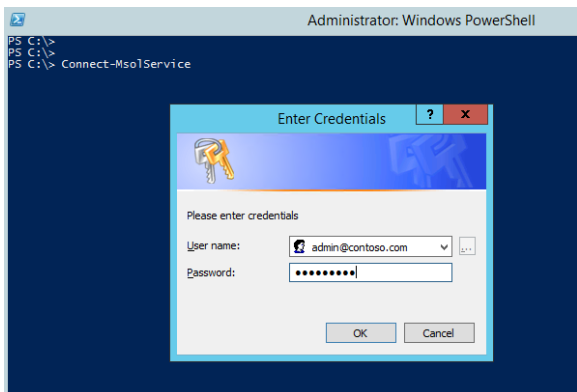


Figure 7-1: Sign in to Office 365 by using the Connect-MsolService cmdlet.

When prompted to sign in, provide credentials appropriate to the function that you want to administer. For full end-to-end administrative access, authenticate with a Global Administrator account.

If sign-in is successful, your session is now connected to Office 365 Azure Active Directory in the context of your Global Administrator account. A global administrator has access to all administrative features and is the only administrator who can assign other administrative roles to users. You can have more than one global administrator in your organization. By default, the person who signs

up to purchase Office 365 becomes a global administrator.

Note The Global Administrator account is often referred to as just the Global Admin or sometimes as the Tenant Admin.

After you are signed in as the global administrator, you can perform any function within the tenant. When you sign in for the first time, you will go through a series of steps and wizards to assist in setting up the tenant with the look and feel you want, the services you require, and any other initial tasks needed to complete the setup. After the setup tasks are done, you will be in the run, maintain, and operate phases to which you were introduced earlier in the chapter.

Probably the most common activities you will undertake as a global administrator relate to the management of identities within the tenant. In the next section, we will look at some of the tasks a global administrator can accomplish with Windows PowerShell and highlight where this task would be difficult or impossible to complete in the Admin Center.

Managing identity in Office 365 and Azure Active Directory

Azure Active Directory (also known as Azure AD) is Microsoft's multitenant cloud-based directory and identity management service. SharePoint server and Office 365 take a dependency on this service to support the provision of hybrid features to subscribers of the SharePoint Online service. Hybrid features are not fully functional unless Office 365 Azure Active Directory has been populated with the user and group identities from the on-premises Windows Active Directory.

Adding a new Active Directory domain to Office 365

The global administrator is responsible for implementing the configuration of Office 365 to support populating the Azure Active Directory with the on-premises user and group accounts. Adding a domain to Office 365 would normally be part of the setup process; however, there are some circumstances for which you might need to add additional domains, such as a company

merger or acquisition with new users in a different domain.

To do this, you first must add an on-premises Active Directory domain with Office 365. You can do this in the UI, but you also can do it through Windows PowerShell.

To add a new domain to your tenant, you can use the `New-MsolDomain` cmdlet. You use the `-Name` option to define the domain name and the `-Authentication` option to define the type of domain, which is either `Managed` or `Federated`.

After you enter the new domain into Office 365, you need to validate it by using the `Get-MsolDomainVerificationDns` cmdlet. This will respond with the DNS record you should use to validate ownership of the domain. After adding the record (TXT or MX) to DNS, you can verify the new domain by using the `Confirm-MsolDomain` cmdlet.

After you've confirmed the domain, the next step is to turn on directory synchronization, which you can do by using the `Set-MSOLDirSyncEnabled` cmdlet, specifying the `-EnableDirSync $true` parameter. Finally, you can use the `(Get-MsolCompanyInformation).DirectorySynchronizationEnabled` cmdlet to confirm that directory

synchronization has been activated successfully. Figure 7-2 details the end-to-end process.

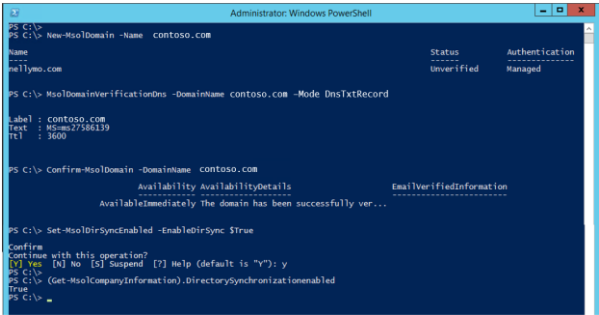


Figure 7-2: A Windows PowerShell session detailing the process for adding a new domain to Office 365.

After you have added and verified the domain successfully and you’ve set up directory synchronization, you can follow the steps at <https://msdn.microsoft.com/library/azure/jj573653.aspx> to deploy the Azure Active Directory Connect (AD Connect) tool in your on-premises environment and synchronize the user and groups.

Forcing directory synchronization

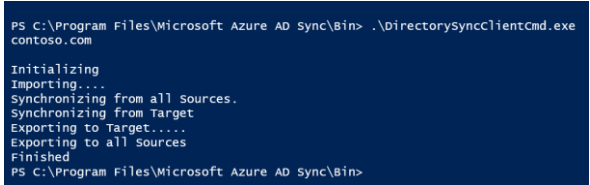
Azure AD Connect is the current recommended synchronization client for Azure Active Directory, and like its predecessors, DirSync and AAD Sync, it does have an associated Windows PowerShell

cmdlet that you can use to force directory synchronization. This cmdlet takes a parameter called `PolicyType` to indicate the type of synchronization required:

```
Start-ADSyncSyncCycle -PolicyType Delta (force
immediate delta sync)
Start-ADSyncSyncCycle -PolicyType Initial (force
immediate full sync)
```

It also has a Windows Scheduled Task, which by default runs every three hours and will perform the synchronization, but if you want to run it manually, you must run

`DirectorySyncClientCmd.exe`, which is located in the directory `C:\Program Files\Microsoft Azure AD Sync\Bin`, as shown in Figure 7-3.



```
PS C:\Program Files\Microsoft Azure AD Sync\Bin> .\DirectorySyncClientCmd.exe
contoso.com

Initializing
Importing....
Synchronizing from all sources.
Synchronizing from Target
Exporting to Target.....
Exporting to all sources
Finished
PS C:\Program Files\Microsoft Azure AD Sync\Bin>
```

Figure 7-3: Using the `DirectorySyncClientCmd.exe` to force directory synchronization.

When the domain synchronization is complete, you can manage the users and groups by using Windows PowerShell.

Managing Office 365 users and groups

As the global administrator of your tenant, you are responsible for the management of the users and groups that are synchronized from the on-premises Active Directory. Just having these users and groups synchronized is not enough for them to be able to participate fully with the services available in the tenancy. For users to consume any of the Office 365 applications, they must be properly licensed. This licensing also extends to users consuming the services in hybrid configuration.

Before you can think about licensing, though, you need to consider the user accounts. For the users themselves, it is rare to find an enterprise deployment that does not use Azure AD Connect to perform directory synchronization, but it does happen. In those cases, you need to know how to create users manually, and Windows PowerShell offers far and away the most capability in that area.

To create new user accounts, the global administrator can use the `New-MsolUser` cmdlet. The example that follows creates one new user. You should note that we have not supplied a password for the account. When the cmdlet

returns, it will respond with a password for the user, which can be sent via regular email or even forwarded directly to the user by piping the output to the Send-SMTPMail cmdlet, as demonstrated here and in Figure 7-4:

```
New-MsolUser -UserPrincipalName
"johndoe@contoso.onmicrosoft.com" -City Seattle -
State WA
-Country USA -DisplayName JohnDoe
```

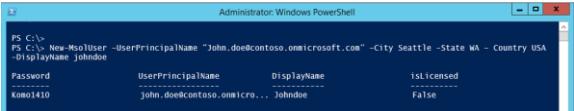


Figure 7-4: Output from the New-MsolUser cmdlet.

Clearly, creating a new Windows PowerShell line for every user in the company would be very tedious, so we can be creative and take advantage of some simple Windows PowerShell looping techniques to add users in bulk. In the example that follows, we use a comma-separated values (CSV) file to feed the parameters into the New-MsolUser cmdlet. Most commonly, this approach is seen where, for example, a Microsoft Excel spreadsheet has been used to collect information about the users and exported to a CSV file for consumption. Again, the output here will result in multiple user IDs being created and a password generated for

each, as depicted in the following code snippet and Figure 7-5:

```
$users = Import-Csv C:\Office365Users.CSV
$users | ForEach-Object {
New-MsolUser -UserPrincipalName $_.UserPrincipalName
-City $_.city -State $_.State -Country $_.Country -
DisplayName $_.DisplayName }
```

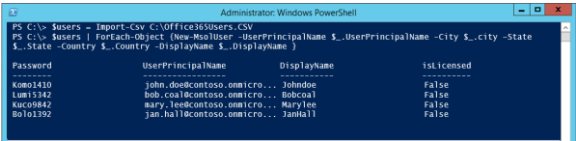


Figure 7-5: Using a CSV file as a source to create multiple new users.

One thing you can observe here is that all these user accounts are created in an unlicensed state. Before the users can consume the Office 365 services, they need an appropriate license.

You can assign licenses in the Office 365 Admin Center, and in some cases you can assign licenses to multiple users at the same time; however, for very large directories for which the Admin Center becomes unwieldy, Windows PowerShell comes to the rescue.

To assign a license to a user, use the following syntax in Windows PowerShell:

```
Set-MsolUserLicense -UserPrincipalName "<Account>" -
AddLicenses " <AccountSkuId>"
```


To confirm the license assignment, check the licenses status of the user

```
(Get-MsolUser -UserPrincipalName  
"<Account>").Licenses.ServiceStatus
```

This example assigns a license from the contoso:ENTERPRISEPACK (Office 365 Enterprise E3) licensing plan to the unlicensed user johndoe@contoso.com and then validates that the license assignment is successful:

```
Set-MsolUserLicense -UserPrincipalName  
"johndoe@contoso.com" -AddLicenses  
"contoso:ENTERPRISEPACK"  
(Get-MsolUser -UserPrincipalName  
"johndoe@contoso.com").Licenses.ServiceStatus
```

You can't assign multiple licenses to a user from the same licensing plan. If you don't have enough available licenses, the licenses are assigned to users in the order in which they're returned by the Get-MsolUser cmdlet until the available licenses run out. At that point, an error is returned indicating that a license could not be assigned because the maximum number of allowable licenses has been reached.

To assign a license to many unlicensed users, use the following syntax:

```
$ApplyLicenses = Get-MsolUser -All -  
UnlicensedUsersOnly [<FilterableAttributes>]  
$ApplyLicenses | foreach {Set-MsolUserLicense -  
ObjectId $_.ObjectId -AddLicenses "<AccountSkuId>"}
```

This example assigns licenses from the contoso:ENTERPRISEPACK (Office 365 Enterprise E3) licensing plan to all unlicensed users:

```
$AllUnlicensed = Get-MsolUser -All -  
UnlicensedUsersOnly  
$AllUnlicensed | foreach {Set-MsolUserLicense -  
ObjectId $_.ObjectId -AddLicenses  
"contoso:ENTERPRISEPACK"}
```

This example assigns those same licenses to unlicensed users in the Tech department in the United States:

```
$TechDept = Get-MsolUser -All -Department "Tech" -  
UsageLocation "US" - UnlicensedUsersOnly  
$TechDept | foreach {Set-MsolUserLicense -ObjectId  
$_.ObjectId -AddLicenses "contoso:ENTERPRISEPACK"}
```

Finally, when users leave the organization, their licenses are freed up when the accounts are deleted; however, you might need the account to be available for audit or compliance reasons but you want to release the license to another user. Here's how to do that:

```
Set-MsolUserLicense -UserPrincipalName  
johndoe@contoso.com -RemoveLicenses  
"contoso:ENTERPRISEPACK"
```

Be aware, though, that removing all licenses from a user can result in lost data when the access to services is revoked.

After you set up the licenses for your users, you can look at some of the other functions that you can control with Windows PowerShell.

At this point, you have created users, or synchronized them into the Office 365 Azure Active Directory tenant, and assigned them licenses to work with the available services. If you have used Azure AD Connect, the Active Directory groups from on-premises will also be available for use within the Office 365 tenant. However, you might have non-synchronized accounts, or want to have some additional groups available in Office 365 Azure Active Directory.

Group management is straightforward: the following example shows how you can create a New Azure Active Directory Group for the Marketing Executives. Figure 7-6 shows the response to the cmdlet.

```
New-MsolGroup -DisplayName "Marketing" -Description "Marketing Executives"
```

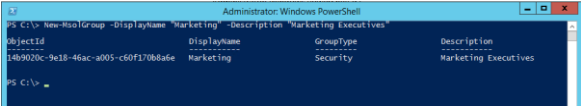


Figure 7-6: Windows PowerShell cmdlet for creating a new Azure Active Directory group.

After you have the groups you need, you can add users to them by using the ObjectIDs of the Group and User, as shown here and in Figure 7-7:

```
Add-MsolGroupMember -GroupObjectId 14b9020c-9e18-46ac-a005-c60f170b8a6e -GroupMemberObjectId db140d26-434e-452d-9b0e-c03b888f9377
```

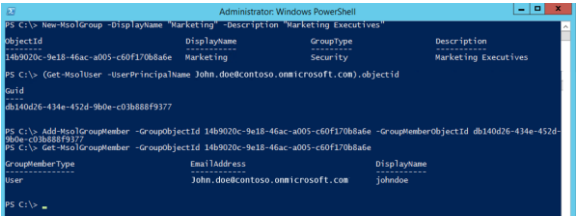


Figure 7-7: The steps to add a user to a group in Azure Active Directory.

Over time, the global administrator will not only add users, but delete them, too. The clean-up of accounts can be somewhat less than straightforward. As an example, accounts that are deleted from the Office 365 Admin Center will be moved to the User recycle bin before they are permanently deleted in 30 days. If the global administrator wants to purge these accounts permanently before the 30 days has elapsed, he can only do this by using Windows PowerShell. There are some scenarios for which user account deletion becomes complicated; for example, if the userid has been reused post deletion. To

gain a deeper understanding of the user and group clean-up process, we recommend reviewing the details in the article available at <https://support.microsoft.com/kb/2619308>.

This section has covered some basic user and group administration in Office 365 Azure Active Directory; there are many more cmdlets and scenarios that global administrators need to be aware of to perform well in the role. For further information on additional administration options, go to <https://msdn.microsoft.com/library/azure/jj151815.aspx>.

Managing SharePoint Online by using Windows PowerShell

In the preceding sections, we learned a little about managing Office 365 Azure Active Directory by using Windows PowerShell. The scope available to the administrator is broad and, in fact, Windows PowerShell should always be the preferred way to manage the tenant as a whole.

But, what about managing the individual services that make up the wider Office 365 Suite as a whole. To begin, what about SharePoint Online and how we manage the users, groups, and sites within the SharePoint administration sphere of responsibility.

Installing the SharePoint Online Windows PowerShell module

SharePoint Online global administrators use the SharePoint Online Management Shell to manage site collections, configure the SharePoint Online services, configure SharePoint Online company-level settings, and get logs from data connections between SharePoint Online and other services through Business Connectivity Services (BCS). To do this, you first must install the prerequisites and the module by using the following steps:

1. If not already deployed to the administrator's workstation, deploy Windows PowerShell 3.0
(<http://go.microsoft.com/fwlink/p/?LinkID=244693>).
2. Download and install the SharePoint Online Management Shell

(<http://go.microsoft.com/fwlink/p/?LinkId=255251>).

After installing the SharePoint Online module, start a Windows PowerShell session and connect to SharePoint Online by using the Connect-SPOService cmdlet, as demonstrated in Figure 7-8.

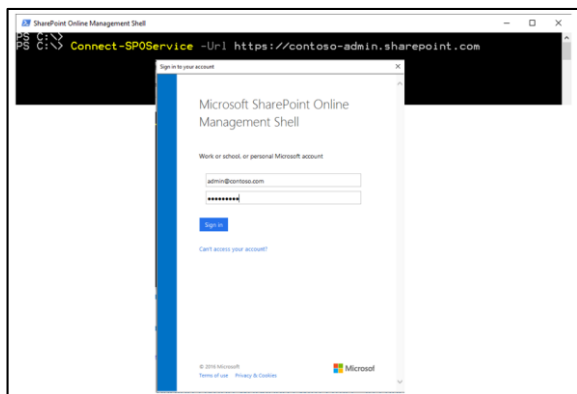


Figure 7-8: The Connect-SPOService cmdlet.

After you're authenticated, you can perform a number of tasks oriented toward site and user management.

For global administrators who are managing a tenant that has hybrid connections to on-premises, there are some requirements to ensure that the features operate as expected. For

example, Outbound Hybrid Search federation requires that the users all have access to the Remote URL specified in the SharePoint Search Result Source. We can check these permissions by using the SharePoint Online Windows PowerShell module and correct them if necessary.

The `Get-SpoSiteGroup` cmdlet (Figure 7-9) can show all of the user accounts and Azure AD groups that have been added to the SharePoint site-level groups. With this information, the global administrator can determine whether a change is needed to configure access for the corporate users.

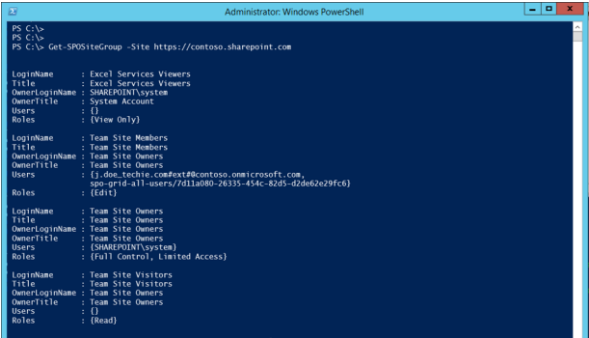


Figure 7-9: Running the `Get-SPOSiteGroup` cmdlet.

From Figure 7-9, we can see that the SharePoint Online built-in role `spo-grid-all-`

users/<tenant> has been granted access to the Team Site Members group. This role is the Everyone Except External Users group and is automatically added to the team Site Members group in SharePoint Online, which grants contribute rights to “Everyone.” With this default configuration, all users should be able to use Outbound Hybrid query federation, but it is worth checking because some companies will not want to grant this level of access to the Everyone group, instead customizing the role memberships to suit their needs. Microsoft suggests retaining this permission or adding the Everyone to a group with perhaps Read-Only instead of Contribute if there are concerns about the level of access.

SharePoint Online Windows PowerShell provides the global administrator with a multitude of cmdlets to be able to manage the Sharepoint users, groups, and sites within the tenant. There is currently no provision for managing the Service Application–level tenant features by using the SharePoint Online Windows PowerShell module; you must do this in the SharePoint Admin Center. To view the list of currently available Windows PowerShell cmdlets, go to the Microsoft TechNet article at <https://technet.microsoft.com/library/fp161397.aspx>.

Managing hybrid workloads by using Office 365 and SharePoint Online Windows PowerShell

Now that your tenant is created and configured how you want it, you can spend some time to look at the options available to administer and operate the Hybrid workloads for SharePoint Server and Office 365. The Azure Active Directory and SharePoint Online Windows PowerShell modules do not provide any hybrid-specific cmdlets to administer hybrid workloads. Hybrid, by its nature, requires the administrator to be aware of many different but related technologies. This includes SharePoint on-premises Windows PowerShell as well as the SharePoint Online and Azure Active Directory flavors. This is demonstrated readily when you begin to look at validating one of the core dependencies for all-out hybrid workloads, the Server-to-Server (OAuth2) trust between SharePoint on-premises and Office 365 Azure Active Directory.

Hybrid administration

You can find a detailed guide to implementing the server-to-server (S2S) trust in Chapter 1, but from a run/maintain/operate standpoint, it is important that the global administrator is able to direct this deployment and use the validation steps for ongoing maintenance and management, including updates and changes when required.

The S2S trust is established by using a certificate exchange mechanism. You can use different types of certificates to establish this trust (as is explained in Chapter 1):

- Built-in SharePoint security token service (STS) certificate
- Self-signed certificate
- Certificate issued by a public Certification Authority (CA)

The built-in SharePoint STS certificate, if used for this purpose, does not have an expiration date; however, self-signed certificates and certificates issued by a public CA always do. Depending on the choice used for the deployment, the administrator will need to be aware of certificate

expiry notifications and how to test and replace these certificates if necessary.

Examine the S2S trust certificate

You can examine the certificates used in the trust by first extracting the current SharePoint STS certificate using the `Get-SPSecurityTokenServiceConfig` cmdlet. This is then followed by retrieving a matching Service Principal Credential from Office 365 Azure AD by using the `Get-MsolServicePrincipalCredential` cmdlet. The Output from the script will indicate the validity of the certificate and whether the trust is in place and able to support hybrid workloads.

Copy the following script, save it as `ValidateMsolServiceAppPrincipal.ps1`, and then run it:

```
$StsThumbprint = (Get-SPSecurityTokenServiceConfig).LocalLoginProvider.SigningCertificate.thumbprint
$StsCertificate = get-item -Path CERT:\localmachine\my\$StsThumbprint
$StsCertificateBin = $StsCertificate.GetRawCertData()
$StsCredentialValue = [System.Convert]::ToBase64String($StsCertificateBin)

$MsolServicePrincipalCredential = Get-
```

```

MsolServicePrincipalCredential -AppPrincipalId
"00000003-0000-0fff1-ce00-000000000000" -
ReturnKeyValues $true | Where-Object {$_.Value -eq
$StsCredentialValue}
    if($MsolServicePrincipalCredential){

        # Check for valid date
        if($MsolServicePrincipalCredential.EndDate -gt
(get-date) -and
$MsolServicePrincipalCredential.StartDate -lt (get-
date)){
            write-host "Msol Service Principal is found
and is Valid until
:"$MsolServicePrincipalCredential.EndDate -
ForegroundColor Green
        }
        Else{
            write-warning ("Msol Service Principal is
found but expired on " +
$MsolServicePrincipalCredential.EndDate + " You
should update the ACS trust certificates for hybrid
workloads to function" )
        }
    }
else{
    write-warning "No matching Msol Service
Principal found for the local farm. Hybrid
workloads will not function correctly on this farm"
}

```

The image in Figure 7-10 indicates the different responses from the script, based on the certificate status. Success here means hybrid

workloads are possible on the current farm configuration.

Warnings need to be investigated and remediated. If no Msol Service Principal is found, you can follow the steps in Chapter 1 to deploy one.

If the Msol Service Principal has expired, you need to replace it.

```
PS C:\> C:\ValidateMsolServiceAppPrincipal.ps1
Msol Service Principal is found and is valid until : 5/22/2017 12:00:00 PM
WARNING: Msol Service Principal is found but expired on 05/05/2016 12:00:00 You should update the ACS trust certificates for hybrid workloads to function
WARNING: No matching Msol Service Principal found for the local farm. Hybrid workloads will not function correctly on this farm
```

Figure 7-10: All possible outputs from the ValidateMsolServiceAppPrincipal Windows PowerShell script.

Replace the S2S trust certificate

When the certificate used for S2S trust with SharePoint on-premises and Azure Active Directory expires, you need to replace it. Typically, this will happen only if you have used a self-signed certificate or a certificate obtained from a public CA; the built-in SharePoint STS certificate does not expire.

We recommend deploying the new certificate first to reestablish the S2S trust before deleting the old certificate credential. To deploy the new certificate and create a valid credential, you

follow a subset of the steps from the initial setup process, as demonstrated in the code sample that follows. You will need to obtain the .pfx and .cer versions of the replacement certificate before proceeding.

```
# Import MSOnline Modules
Import-Module MSOnline -force -verbose
Import-Module MSOnlineExtended -force -verbose

#Log on as a Global Administrator for Office 365
Connect-MsolService

#Define the variables. pfx for sts replacement, cer
for O365 Upload

$stscertpfx="c:\certs\sts_cert.pfx"
$stscertcer="c:\certs\sts_cert.cer"
$stscertpassword="*****"
$spoappid="00000003-0000-0fff1-ce00-000000000000"

#Update the Certificate on the STS
$pfxCertificate=New-Object
System.Security.Cryptography.X509Certificates.X509C
ertificate2 $stscertpfx, $stscertpassword, 20
Set-SPSecurityTokenServiceConfig -
ImportSigningCertificate $pfxCertificate

#Restart IIS and the SPTimer Service so STS Picks
up the New Certificate

& iisreset
& net stop SPTimerV4
& net start SPTimerV4
```

```
#Generate the new credential from the replacement
certificate

$cerCertificate = New-Object
System.Security.Cryptography.X509Certificates.X509C
ertificate2
$cerCertificate.Import($stscertcer)
$cerCertificateBin =
$cerCertificate.GetRawCertData()
$credValue =
[System.Convert]::ToBase64String($cerCertificateBin
)

#Register the On-Premise STS with new certificate
as Service Principal in Office 365

New-MsolServicePrincipalCredential -AppPrincipalId
$spoappid -Type asymmetric -Usage Verify -Value
$credValue
```

After you have replaced the on-premises SharePoint STS certificate and uploaded and set the new credential as a service principal, you can clean-up the old credentials.

Cleaning expired credentials

To do this, you again use Windows PowerShell to identify the expired certificates registered as credentials in SharePoint Online. It is very important to identify only the expired certificates and not just assume that you can remove all of them except the new replacement certificate.

Other hybrid workloads might be in play that have added their own credentials to Office 365. For example, if you have multiple hybrid connections from different on-premises farms, each connection will use its own credential.

The following script locates all of the `MsolServicePrincipalCredentials`, which are registered against `Microsoft.SharePoint`; enumerates all the expired certificates; and then removes them:

```
$prin = Get-MsolServicePrincipal | Where-Object{$_.DisplayName -eq "Microsoft.SharePoint"}

$cred = Get-MsolServicePrincipalCredential -AppPrincipalId ($prin).AppPrincipalId -ReturnKeyValues $false | Where-Object{$_.EndDate -lt (get-date)}
foreach($credential in $cred){
    if($credential.keyid){
        Remove-MsolServicePrincipalCredential -ObjectId $prin.ObjectId -KeyIds $credential.KeyId
    }
}
```

There are other aspects to checking your hybrid environment health, but these fall into more of a housekeeping/routine checks and balances scenario.

Service Principal Names

When a credential is registered for a service in Office 365 it is registered with a Service Principal Name (SPN) against the AppID for Office 365.

The churn in this area is expected to be low; however, if new hybrid experiences are brought on board, you might find some drift here. Equally, as is discussed in Chapter 6, checking for duplicate or overlapping SPNs is important to reduce the risk of incidents related to SPN problems. The following script displays the SPNs registered for the Office 365 AppID:

```
#Validate SPNs setup properly in Azure Active Directory
$app = Get-MsolServicePrincipal -AppPrincipalId
"00000003-0000-0ff1-ce00-000000000000"
$app.ServicePrincipalNames
```

Service Application Health

As discussed throughout this book, all of the hybrid workloads are based on an S2S trust between SharePoint server and Office 365 Azure Active Directory, and this also involves registering a new app principal in the on-premises app registry. Hybrid scenarios dependent on profile rehydration require the user profile properties to be correct, so in addition to the app support, you also need to ensure that the user profile service application is properly configured and online, and also that the directory synchronization service is operating correctly. The code that follows demonstrates how you can do this.

```

# Validate Dirsync
$msolcompany = Get-MsolCompanyInformation
$IsDirSyncEnabled =
$msolcompany.DirectorySynchronizationEnabled
$IsDirSyncEnabled
$LastDirSyncTime = $msolcompany.LastDirSyncTime
$LastDirSyncTime
Get-MsolUser -UserPrincipalName user1@contoso.com |
ft
Get-MsolUser -UserPrincipalName user2@contoso.com |
ft

#Validate User Profile Service Application Status
$upa=Get-SPServiceApplication | where-object
{$_ .TypeName -match "User profile Service
Application"}
$upa.status

$app=Get-SPServiceApplication | where-object
{$_ .TypeName -match "App Management Service
Application"}
$app.status

$sub=Get-SPServiceApplication | where-object
{$_ .TypeName -match "Microsoft SharePoint Foundation
Subscription Settings Service Application"}
$sub.status

#Validate on premises ACS Proxy

$proxy = Get-SPServiceApplicationProxy | ?
{$_ .TypeName -eq "Azure Access Control Service
Application Proxy"}
$proxy | ft Name, Status, MetadataEndpointUri -
autosize

```

Managing the hybrid workloads by using Windows PowerShell

You have already seen that there is a lot of administrative work to do even before you get to the administration of the hybrid workload itself. Fortunately for the administrator, much of the hybrid-specific administration is a one-off configuration activity, but there are some tasks that you might need to revisit from time to time.

Administering Microsoft OneDrive for Business

OneDrive for Business and Sites Hybrid Configuration is set up either through the SharePoint Central Administration user interface or by using the Hybrid App Picker. There are some Windows PowerShell cmdlets available to administer and inspect the features after setup.

Get-SPO365LinkSettings

The `Get-SPO365LinkSettings` cmdlet retrieves the configuration settings for the Hybrid OneDrive, Sites, and App Launcher features. The hybrid App Launcher is only available on SharePoint

Server 2016, so you get a slightly different output depending on the platform on which you run the cmdlet. Figure 7-11 shows the response from SharePoint Server 2013.

```
PS C:\>
PS C:\> Get-SPO365LinkSettings

Audiences                : {OneDrive Onboarding}
MySiteHostUrlMaxLength   : 2048
MySiteHostUrl             : https://contoso-my.sharepoint.com
RedirectSites            : True
IsEnabledForEveryone     : False

PS C:\>
```

Figure 7-11: The response to the Get-SPO365LinkSettings cmdlet on SharePoint Server 2013.

Figure 7-12 shows the response from SharePoint Server 2016.

```
PS C:\>
PS C:\> Get-SPO365LinkSettings

Audiences                : {}
MySiteHostUrlMaxLength   : 2048
MySiteHostUrl             : https://contoso-my.sharepoint.com
RedirectSites            : True
HybridAppLauncherEnabled : True
IsEnabledForEveryone     : True

PS C:\>
```

Figure 7-12: The response to the Get-SPO365LinkSettings cmdlet on SharePoint Server 2016.

In the SharePoint Server 2013 settings (Figure 7-11) you can see an Audience Rule has been applied to the One Drive and sites redirection, whereas for SharePoint Server 2016 (Figure 7-

12), there is no Audience defined and the `IsEnabledForEveryone` property is `True`.

Set-SPO365LinkSettings

You can use the `Set-SPO365LinkSettings` cmdlet to update the settings for the Hybrid Links Configuration. Again, the `HybridAppLauncherEnabled` property is available only on SharePoint Server 2016. You can set all of the other properties by using this cmdlet.

Test-SPO365LinkSettings

The final cmdlet in this SPO365 family is the `Test-SPO365LinkSettings` cmdlet. This cmdlet does a very simple validation check to confirm that the provided `MySiteHostUrl` parameter does indeed point to a valid MySite Host template in SharePoint Online. Figure 7-13 shows the response.

```
PS C:\>
PS C:\> Test-SPO365LinkSettings -MySiteHostUrl https://contoso-my.sharepoint.com
PS C:\>
PS C:\>
PS C:\>
PS C:\> Test-SPO365LinkSettings -MySiteHostUrl https://contoso.sharepoint.com
Test-SPO365LinkSettings : The remote site https://contoso.sharepoint.com/ does not use the my site host template.
at [line:1 char:1]
> Test-SPO365LinkSettings -MySiteHostUrl https://contoso.sharepoint.com
-----
+ CategoryInfo          : InvalidData: (Microsoft.Office...estLinkSettings:SPO365TestLinkSettings) [Test-
SPO365Link
Settings], InvalidDataException
+ FullyQualifiedErrorId : Microsoft.Office.Server.UserProfiles.PowerShell.SPO365TestLinkSettings

PS C:\>
```

Figure 7-13: The response from `Test-SPOLinkSettings` with Valid and Invalid output.

The output from the `Test-SPO365LinkSettings` cmdlet is worth noting. First it does not check

the value of the `MySiteHostUrl` in the feature itself; you must provide the URL to test when prompted or as a parameter on the cmdline.

The test itself just checks that the site for which you provided the URL has a MySite Host template applied to it. If the site is a valid MySite Host, the cmdlet returns nothing as when you first ran the cmdlet. If the site is not a valid MySite Host, you will get a response and an exception as per the second time you ran the cmdlet (see Figure 7-13).

Administering Cloud Search Service Application

Chapter 2 explains how to set up and configure the Cloud Search Service Application.

Configuring this feature by using Windows PowerShell is no different in reality from configuring a regular Search Service Application except in two key areas. The Cloud Search Service Application does not provide a means to purge items from the Office 365 search index, nor does it provide a simple way to determine the total number of searchable on-premises items in the Office 365 search index.

Managing search item removal and index purge

In SharePoint 2013 and SharePoint 2016, items are deleted from the on-premises search index when they are deleted from the content that is being indexed, when the administrator removes a start address from the content sources, or when the administrator completely removes a content source. The deletion happens in different ways and SharePoint uses crawl policies to dictate this process. You can find documentation on crawl policies at [https://technet.microsoft.com/library/hh127009\(v=office.14\).aspx](https://technet.microsoft.com/library/hh127009(v=office.14).aspx). The following list details the different ways in which you can remove items from the SharePoint Search Index during normal on-premises-only operational use:

- When a SharePoint item is flagged in the change log as deleted, the crawler signals that deletion during a crawl and that ultimately leads to the item being removed from the search index.
- When a non-SharePoint item is deleted—for example an item in a file share—this is picked up as an item not found by the next crawl of that content and eventually removed from the search index.

- When a start address is removed from a content source or an entire content source is removed, this initiates a different process: a delete crawl. The delete crawl systematically removes all items from the search index that fall under the start address(es) being removed.
- Finally, an index reset can remove items from the search index but this approach is nonselective and results in a complete purge of the indexed items. More important, it also removes the crawl history from the crawl databases.

Just like an on-premises only Search Service Application, the Cloud Search Service Application will send signals to the Office 365 search index to remove items from the index. However, the fourth process in the preceding list, index reset, is a very different animal in the Cloud Search Service Application. If an administrator selects index reset in the Cloud Search Service Application, the crawl history is purged from the crawl databases but no signal is sent to Office 365 to purge the items from the Office 365 search index. This will result in orphaned indexed items with no effective means of removal. Until the April 2016 cumulative

update (CU) for SharePoint Server 2013 and the June 2016 CU for SharePoint Server 2016, that is.

When we say no effective way of removing the orphaned search items, there were in fact two ways to accomplish this:

- First, delete the content sources to trigger a delete crawl to run. Next, re-create the content sources and then reindex everything on-premises. Of course, reindexing everything is not efficient; it takes time and if items have been deleted from the on-premises content you still run the risk of missing orphans in the Office 365 search index.
- Another option is to call Office 365 support and raise a ticket to ask for an index purge, something that takes time, and again is inefficient for the task at hand. The message here from Microsoft is, please, please do not ever click index reset on a Cloud Search Service Application. In fact, a new warning (see Figure 7-14) has been added to the index reset function for this exact reason.

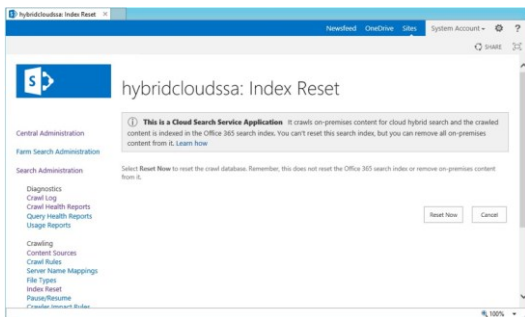


Figure 7-14: The Index Reset page of the Cloud Search Service Application.

In the April 2016 CU for SharePoint 2013 and the June 2016 CU for SharePoint Server 2016, a new method has been added to the PushTenantManager, a component of the Cloud Search Service Application. The new method is DeleteAllCloudHybridSearchContent, and an example script using it is provided here:

```
<#
.SYNOPSIS
    Issue a call to SPO to delete all external
    content indexed through Cloud hybrid search. This
    operation is asynchronous.
.PARAMETER PortalUrl
    SharePoint Online portal URL, for example
    'https://contoso.sharepoint.com'.
.PARAMETER Credential
    Logon credential for tenant admin. Will prompt
    for credential if not specified.
```

```
#>
param(
    [Parameter(Mandatory=$true,
HelpMessage="SharePoint Online portal URL, for
example https://contoso.sharepoint.com.")]
    [ValidateNotNullOrEmpty()]
    [String] $PortalUrl,
    [Parameter(Mandatory=$false, HelpMessage="Logon
credential for tenant admin. Will be prompted if
not specified.")]
    [PSCredential] $Credential
)

$SP_VERSION = "15"
$regKey = Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Office
Server\15.0\Search" -ErrorAction SilentlyContinue
if ($regKey -eq $null) {
    $regKey = Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Office
Server\16.0\Search" -ErrorAction SilentlyContinue
    if ($regKey -eq $null) {
        throw "Unable to detect SharePoint
installation."
    }
    $SP_VERSION = "16"
}

Add-Type -AssemblyName
("Microsoft.SharePoint.Client,
Version=$SP_VERSION.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c")
Add-Type -AssemblyName
("Microsoft.SharePoint.Client.Search,
Version=$SP_VERSION.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c")
```

```

Add-Type -AssemblyName
("Microsoft.SharePoint.Client.Runtime,
Version=$SP_VERSION.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c")

if ($Credential -eq $null)
{
    $Credential = Get-Credential -Message "SPO
tenant admin credential"
}

$context = New-Object
Microsoft.SharePoint.Client.ClientContext($PortalUr
l)
$spocred = New-Object
Microsoft.SharePoint.Client.SharePointOnlineCredent
ials($Credential.UserName, $Credential.Password)
$context.Credentials = $spocred

$manager = New-Object
Microsoft.SharePoint.Client.Search.ContentPush.Push
TenantManager $context
$task =
$manager.DeleteAllCloudHybridSearchContent()
$context.ExecuteQuery()

Write-Host "Started delete task
(id=$($task.Value))"

```

When running the script, the administrator needs to authenticate with a valid Office 365 SharePoint Online Global Administrator account. You can optionally provide the PortalUrl on the

command line or type it when the script prompts you to provide it, as shown in Figure 7-15.

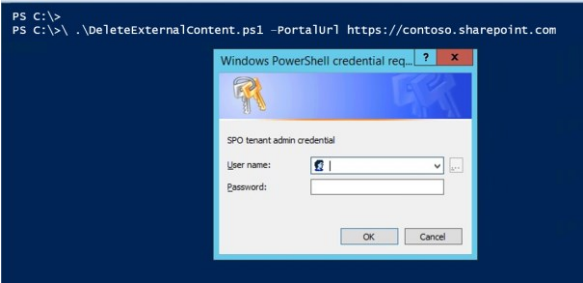


Figure 7-15: Running the DeleteExternalContent Windows PowerShell script.

After a valid credential is supplied, the script responds with a simple message, as shown in Figure 7-16.

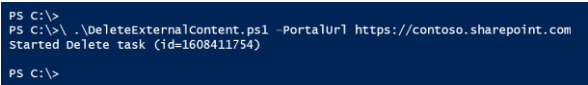


Figure 7-16: The completion of the DeleteExternalContent Windows PowerShell script.

Record this task ID because you might need it if you call Microsoft support should the process for any reason fail. The task is asynchronous; that is, you can leave it to continue running in the Office 365 Search Farm and it will eventually complete.

After this final step, you will receive no more feedback, but you can track the effect of the task by running a search query for the managed property `IsExternalContent=1` from the SharePoint Online search center. If you run a query to record the number of items displayed by this managed property before you begin the purge command and continue running it a couple of times after the purge is started, you will see a steady decrease in the number of items in search results. Ultimately, there will be no results for the managed property `IsExternalContent=1`, which confirms the deletion.

We have deliberately not tried to provide estimates or predictions for the time taken to purge a specific number of items from the Office 365 index because this will vary based on a number of factors. Needless to say, it will take as long as it takes.

Counting the searchable items from on-premises content sources

One thing every search administrator wants to know is the total number of searchable items that are in the index. In Office 365 today, this is not something that is available to the global administrator, nor is it in the Cloud Search

Service Application. The number of searchable items displayed in the on-premises Search Service Application administration page will always remain at zero. To determine the number of items successfully added to the Office 365 search index, the administrator needs to examine the Crawl Log and then click the Databases tab, as illustrated in Figure 7-17.

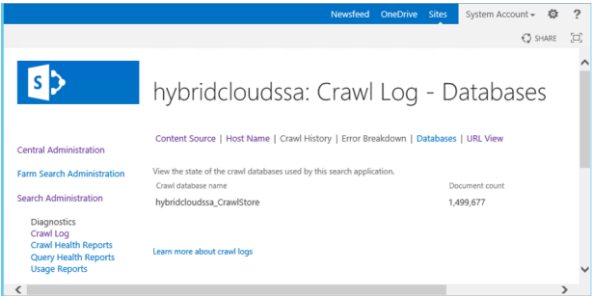


Figure 7-17: The Crawl Log page in Cloud Search Service Application, filtered on the Databases to show the Document Count.

Within the databases tab is a list of all the CrawlStore Databases for the Cloud Search Service Application. By summing up the Document count for each database, you can get a clear picture of the total number of items indexed, as shown in Figure 7-17.

Summary

Throughout this chapter, we have shown examples of relatively simple Azure Active Directory management using Windows PowerShell and extended that to the specific actions available in the SharePoint Online Windows PowerShell module. Moving on from simple Windows PowerShell, we have examined the options available for the global administrator to perform housekeeping on the baseline configuration for Hybrid, such as validating the trusts and the service application architecture. Finally, we reviewed some of the high-impact critical operations for hybrid-specific workloads.

Microsoft SharePoint hybrid deployment recommended practices

This chapter provides recommended good practice guidance for deployment and configuration of the components that make up the hybrid user experience. From the deployment of the right-sized identity management infrastructure through choosing the right options for each

hybrid workload and configuring the underlying Microsoft SharePoint farm to support the requirements for the business, you'll find some very useful advice for creating and managing your hybrid environment.

Introduction

Professionals in many industries talk about the right way to do things and the IT industry is no different. Too often this is mistakenly referred to as the "Best Practice" approach, when really there is no such thing as a best practice, only common practice and preferred approaches. If you ask any SharePoint consultant to deploy a SharePoint server farm to a "Best Practice" configuration, the chances are you will get a number of different implementations but with a common baseline. Any consultant worth the name will actually come back with several questions before committing to designing the farm. The design should reflect the best requirements for the purpose of the business

and not try to conform to a one-size-fits-all paradigm.

The groundwork and planning needed prior to implementing hybrid deployments of SharePoint server and Microsoft Office 365 is no different from that of a regular on-premises or Office 365-only project. The needs of the business must be taken into consideration before embarking on a design process to ensure that the deployment is fit for the purpose. When considering the business needs for specific hybrid functionality, you need to accommodate not only the feature itself, but the dependencies and requirements to support the feature across both on-premises and Office 365.

For this chapter, we will work through the planning phases of the hybrid deployment, providing guidance and recommended practices at each stage.

Performance management

Microsoft has produced a Microsoft Virtual Academy course on Office 365 Performance Management at <http://aka.ms/tunemva>, which covers the breadth of the suite. In this section,

we will focus on the aspects of Office 365 performance as it pertains to hybrid scenarios.

Network and connectivity

The single most common factor that all IT projects depend on is the underlying network and connectivity between the components that support the application being deployed. Office 365 hybrid projects are no different, and it is important that the team responsible for implementation has done its due diligence by ensuring that any additional network load or communication routes, if required, are included in the project scope.

As already discussed throughout this book, Office 365 hybrid scenarios are based on connectivity between on-premises SharePoint servers—and to some degree also on connectivity between the subscriber's client PC—and Office 365. Microsoft has introduced a SharePoint Online testing tool that can provide some very valuable information not only to the client, but also for performing some rudimentary testing between SharePoint on-premises servers and Office 365. This tool is the Microsoft Office 365 Client Performance Analyzer and you can get it at <https://support.office.com/article/Office-365-Client-Performance-Analyzer-e16b0928->

[bd38-423b-bd4e-b8402bc106aa?ui=en-US&rs=en-US&ad=US](https://www.microsoft.com/en-us/download/details.aspx?id=38423). The tool is particularly useful for testing over a period of time because it can take scheduled tests to validate the connectivity at different times of the day.

After downloading and running the tool, a results screen appears that contains some key information. The core information that we care about in the hybrid world is that the ports we need to communicate to Office 365 are open and that the network performance characteristics meet or exceed the minimum bar for optimal operation. Figure 8-1 shows the tool running from an on-premises SharePoint 2013 server.

Microsoft Office 365 Client Performance Analyzer		
Office 365		
Property	Value	Expected Value
Application Type	Sharepoint	-
Client Operating System	Microsoft Windows Server 2012 R2 Datacenter	-
Client Memory (GB)	14	-
Client CPU (Cores)	4	-
Run from Country	US	-
Run from State	US_WASHINGTON	-
Unique Internet Service Provider Id (ASN)	8075	-
Run from Internet Service Provider (ISP)	Microsoft Corporation	-
TCP port 80 (HTTP)	OPEN	OPEN
TCP port 443 (HTTPS)	OPEN	OPEN
TCP port 587 (SMTP)	OPEN	OPEN
TCP port 993 (IMAP)	OPEN	OPEN
TCP port 995 (POP)	OPEN	OPEN
DNS server name	UnKnown	-
DNS server ip address	104.146.150.25	-
DNS resolution time (ms)	1	<= 25
Network hops to Office 365 service	7	<= 25
Network latency to Office 365 service using ICMP ping (ms)	0	<= 275
TCP Ping packet loss (%)	0	0
Network latency to Office 365 service using TCP ping (ms)	0.88	<= 275
Network latency to Office 365 service using HTTP ping (ms)	74.3	<= 1000
HTTP Latency to CDN (ms)	22.6	<= 1000
HTTP Proxy server	Not Found	-
HTTPS Proxy server	Not Found	-
Proxy Authentication Enabled	NO	NO
TCP Maximum Segment Size	1440	>= 1300
TCP Window Scaling Option	YES	YES
TCP Selective Acknowledgment Option	YES	YES
CDN download bandwidth (Kbps)	176149	>= 1024

Sharepoint
5/24/2016 11:23:01 AM
Download result file (.xlsx)
Show Trace Route Details

Figure 8-1: Output from the Office 365 Client Performance Analyzer.

From a purely hybrid standpoint, following are the key elements that we care about:

- **TCP Port 443** This needs to be open to support connectivity between SharePoint on-premises and Office 365 for all hybrid scenarios. For example, outbound hybrid search will need to communicate to the SharePoint online root site in order to reach the search web services.
- **Network latency** Several latency values are reported by the tool, from DNS latency to HTTP ping and CDN latencies. All of these values individually contribute to the experience of the end user and for hybrid scenarios, you want to have the lowest possible latencies between the on-premises servers and Office 365. High latencies lead to poor performance and the potential for timeouts.
- **HTTP/HTTPS proxy** Proxied connections can cause bottlenecks and access issues for communication between SharePoint on-premises and Office 365.
- **TCP settings** A number of TCP settings are important for optimal communication performance between SharePoint on-premises and Office 365.

Of these issues, two of them need further explanation as to recommended practice.

Outbound proxy connections

Some businesses have policies specifying that all outbound Internet traffic should be routed via a proxy device in order to support access control and traffic monitoring. Unfortunately, this can introduce adverse side effects for hybrid scenarios, especially when proxies require authentication or modify the TCP headers. For example, if the accounts running the Query Processor (`noderunner.exe`) do not have unsolicited outbound access, outbound query federation will fail due to the proxy requiring authentication.

The Client Performance Analyzer tool indicates any proxy configuration in the report. You can also use a Windows PowerShell command-line window or regular Windows command-line window to gather proxy information from the server by using the `netsh` command and, if necessary, reset the proxy configuration to Direct access. Figure 8-2 shows how to do this. To open a Windows PowerShell command-line, click the Start icon and begin typing **PowerShell**. When the PowerShell option appears, right-click it and then, on the shortcut menu, choose Run As Administrator. To use Windows command-line, again click the Start icon and begin typing **CMD**.

When the command-line option appears, right-click it and choose Run As Administrator.

Note You can manage the proxy configuration of the server centrally via Active Directory Group Policy. You might need to coordinate with the Active Directory administrators to ensure that the required proxy configuration is correctly enforced.



```
PS C:\>
PS C:\> netsh winhttp show proxy

Current WinHTTP proxy settings:

    Proxy Server(s) : proxy.contoso.com:8080
    Bypass List      : *.contoso.com

PS C:\> netsh winhttp reset proxy

Current WinHTTP proxy settings:

    Direct access (no proxy server).

PS C:\> _
```

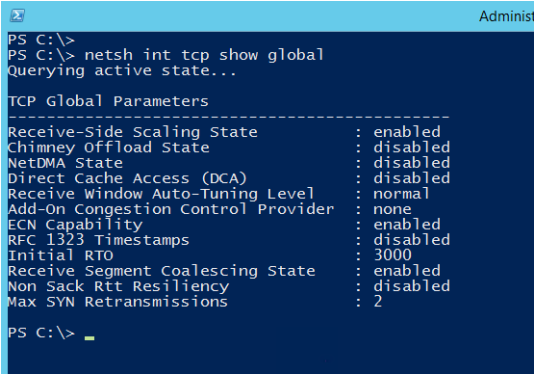
Figure 8-2: Using netsh to gather and then reset the winhttp proxy configuration.

The netsh command is a command-line scripting utility with which you can display or modify the network configuration of a computer that is currently running. You can find more information at <https://technet.microsoft.com/library/bb490939.aspx>.

TCP settings

For good network communication efficiency, the TCP settings are critical. In particular, ensuring that TCP scaling is turned on is important to make the most of the available bandwidth, especially in higher-latency connection scenarios. You can again use netsh to determine whether TCP scaling is on, as shown in Figure 8-3. The Receive Window Auto-Tuning Level should be set to Normal to support TCP scaling. You can read more about the impact of TCP scaling in this blog article

<https://blogs.technet.microsoft.com/onthewire/2014/03/28/ensuring-your-office-365-network-connection-isnt-throttled-by-your-proxy/>



```
PS C:\> netsh int tcp show global
Querying active state...

TCP Global Parameters
-----
Receive-Side Scaling State      : enabled
Chimney Offload State          : disabled
NetDMA State                   : disabled
Direct Cache Access (DCA)     : disabled
Receive Window Auto-Tuning Level : normal
Add-On Congestion Control Provider : none
ECN Capability                 : enabled
RFC 1323 Timestamps           : disabled
Initial RTO                    : 3000
Receive Segment Coalescing State : enabled
Non Sack Rtt Resiliency        : disabled
Max SYN Retransmissions        : 2

PS C:\>
```

Figure 8-3: Output of the netsh int tcp show global command showing the TCP Global parameters

and in particular the value of the Receive Window Auto-Tuning Level.

The second TCP setting we care about is Selective Ack (or SACK). This setting is turned on by default for Windows servers and clients but occasionally might be turned off for compatibility reasons with older networking equipment. It is very rare to discover it turned off, but it can happen. Selective Ack improves network transmission efficiency by reducing the number of retransmissions required to recover lost packets. You can find more information on this setting at <https://support.microsoft.com/kb/224829>.

Microsoft OneDrive for Business and OneDrive Sync Client

The configuration of OneDrive for Business as a hybrid workload is a relatively straightforward procedure, requiring just a redirection URL and optionally an audience to maintain a list of users who are onboarded for redirection. With the OneDrive for Business Next Generation Sync Client, you can connect and synchronize files from your OneDrive for Business. Optionally, you can add additional accounts to the OneDrive for Business Sync Client to synchronize those accounts to the local machine. The impact of

turning on this capability for a large number of users at the same time can be quite dramatic, so Microsoft recommends a staged approach depending on the use case at hand. There are two scenarios that exist here:

- Users who are completely new to OneDrive for Business
- Users with more mature OneDrive usage who are likely to have content in their OneDrive for Business already.

The two scenarios are quite different in terms of impact on the network. For new OneDrive users connecting to the service, the amount of network traffic should be relatively small and synchronization will occur for new content as it is moved into the OneDrive folder on the client or directly via the OneDrive for Business browser experience. The more mature user fits into two further subcategories: users who have OneDrive for Business in the cloud but do not have the Sync Client turned on; and those who have both the OneDrive and the Sync Client in place. In both cases, the scenario that you want to avoid is if many people are synchronizing a lot of content at the same time. This is because OneDrive for Business libraries have a very large capacity (1 TB), which means that there could be a lot of network traffic if a large number of

people are carrying out initial synchronization simultaneously.

Having an effective strategy for managing the user experience and the network impact is important. You can implement control in two ways.

- Use audiences in SharePoint on-premises to control the number of users who can use OneDrive for Business at the same time. This staged approach is recommended by Microsoft so that a subscriber to Office 365 can assess the impact on the network and wait until a steady state is reached before enabling more users.
- In an upcoming release of the next generation Sync Client, the percentage of local bandwidth available for uploading content will be manageable centrally. You can do this by using Active Directory Group Policy; the new client has a Network tab, as shown in Figure 8-4, indicating the applied settings similar to that of the consumer version. Note that these controls will change in the actual released client version. For more details after release, go to <https://support.office.com/article/Administrative-settings-for-the-OneDrive-for-Business->

[Next-Generation-Sync-Client-0ecb2cf5-8882-42b3-a6e9-be6bda30899c.](#)

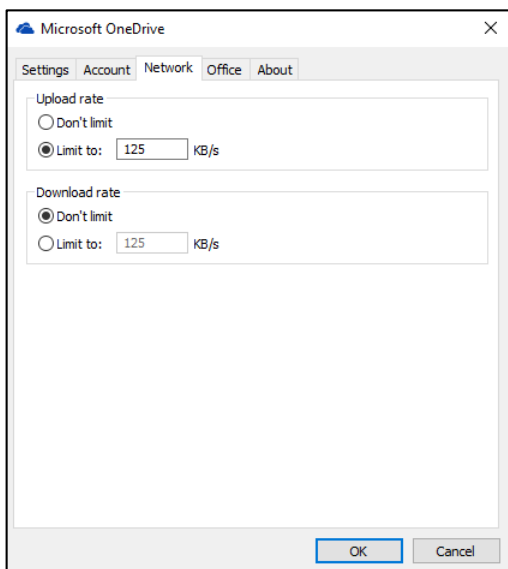


Figure 8-4: OneDrive for Business next generation sync client Bandwidth Controls for upload and download rate. Keep in mind that this is a preview screenshot; the final release will have different controls.

Security

Hybrid scenarios depend heavily on communication between SharePoint on-

premises and SharePoint Online, Microsoft Azure Active Directory, and other Office 365 services, with much of that communication being across the public Internet. When we consider the aspects of this communication, foremost in the mind is security and ensuring that the content of the transmission cannot be intercepted and used with malicious intent. This communication flow contains user claims tokens, search queries, line-of-business (LoB) data and other potentially private information. You need to provide appropriate in-transit encryption of the data by using certificates.

Hybrid scenarios are also dependent on trust relationships between remote resources. Office 365 needs to know that requests from on-premises users are coming from a trusted source. Likewise, SharePoint on-premises needs to trust the source of inbound requests. You use certificate exchange to establish this trust, and client certificates to ensure the identity of the incoming on-premises request.

With this many certificates, understanding the different options and following recommended practices will make life easier for the administrator.

Certificate planning and ongoing management

The use of certificates in hybrid scenarios is widespread, from establishing server-to-server (S2S) trusts to encrypting publishing web application endpoints and providing client preauthentication. Each has its own requirements and preferred options. Let's take a look at these choices now.

S2S trust certificates

As we have seen earlier in this book, an S2S trust between SharePoint on-premises and Office 365 Azure Active Directory is a requirement for most hybrid functionalities. To establish this trust, you must use a certificate sourced from one of the following options:

- Self-signed certificate
- Certificate from a public certificate signing authority
- Built-in SharePoint security token service (STS) certificate

Chapter 1 discusses the pros and cons of each type of certificate. Which one you should use will depend on any policy that might be defined by

your security team, such as using only a certificate from a public certificate signing authority. If no such restrictions apply, we recommend using the built-in STS certificate because it has no expiry date and you can use it without disrupting the SharePoint farm availability during deployment.

Secure Sockets Layer certificates

Communications between the SharePoint on-premises and the SharePoint Online services are most likely to traverse the public Internet. With this in mind, securing the communication against malicious threats is critical for safety and privacy. Microsoft secures the Office 365 publicly accessible endpoints by using Secure Sockets Layer (SSL) certificates. For example, SharePoint Online is secured with a wildcard SSL certificate for the domains covered by *.sharepoint.com, as demonstrated in Figure 8-5.

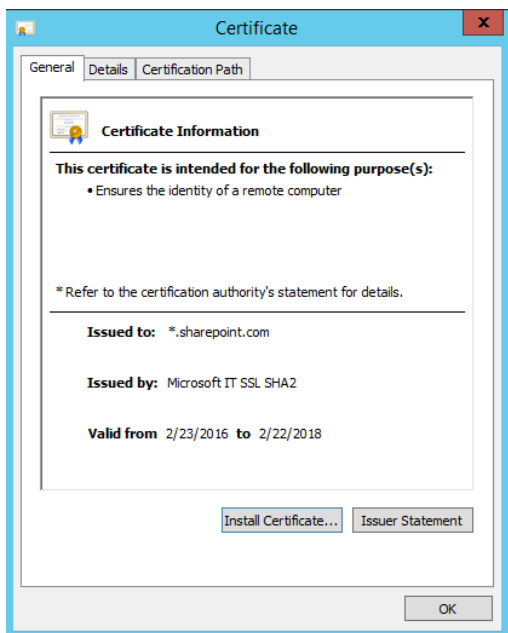


Figure 8-5: Microsoft public wildcard certificate for SharePoint Online.

When securing the on-premises resources you need to decide whether a wildcard certificate is right for you. Again, your security team might have some policies that dictate the choice you make. Here are your options:

- **Entire domain (wildcard) certificate** This is a digital public-key document that can be

applied to a domain and subdomains. This certificate simultaneously covers an unlimited number of first-level subdomains and is therefore a cost-effective approach when you have many subdomains.

- **Multidomain (SAN) certificate** A digital public-key document that can be applied to multiple domain. This certificate covers a number of top-level domains that you must specify when you're requesting the certificate from the certificate authority.
- **Single-domain (single name) certificate** A digital public-key document that applies to a single named domain.

It made perfect sense for Microsoft to choose a wildcard certificate for the SharePoint Online service because there are literally millions of subdomains—at least three per tenant. The cost and management overhead alone makes it a simple decision. With fewer domains to administer, the choice can be different if required.

Ultimately the choice is yours, and you should also keep in mind whether your company is intending to use other Office 365 services which might also require certificates. Combining certificate under the same management

processes can be cost and labor efficient. For example, for Exchange Online, see the following guidelines

<https://support.office.com/article/Plan-for-third-party-SSL-certificates-for-Office-365-b48cdf63-07e0-4cda-8c12-4871590f59ce?ui=en-US&rs=en-GB&ad=GB&fromAR=1>

Client preauthentication certificate

The third type of certificate in use with SharePoint on-premises and Office 365 hybrid is the client preauthentication certificate. Chapter 2 and Chapter 3 both discuss how this certificate is used by the reverse proxy to authenticate the inbound calls from Office 365 to SharePoint on-premises.

This certificate can be of any type, from wildcard, SAN, or single name, but you must use a certificate signed by a public certificate signing authority. A self-signed or domain-issued certificate could not be validated by Office 365, and, as such, you must not use it. Microsoft recommends that you use a unique-purpose certificate for this role to limit the potential for a security breach. If you were to use the same certificate for both client preauthentication and SSL publishing of the on-premises web application, an attacker has only to compromise one certificate to gain complete access to the

web application. Two certificates increase the security of the environment because the second certificate is only present in the SharePoint Online secure store and cannot be extracted after it is uploaded.

User life cycle management

Identity is one of the cornerstones of providing your users with access to corporate data from multiple different platforms. Your identity is the key to gaining access to everything, whether launching a mobile app or a full Software as a Service (SaaS)–based application. You need an identity management solution to ensure efficient management of the user life cycle. Including unifying and synchronizing between your identity repositories and automating and centralizing the process of provisioning resources. The identity solution should be a centralized identity that spans across on-premises and cloud and makes use of identity federation to maintain centralized authentication and securely collaborate with external users and businesses.

One of the most effective tools you can add to the identity solution is self-service experiences

for the end users, whether it is providing simple password reset capabilities or more complex identity management such as control over groups and group membership. Offering single sign-on (SSO) for users across all of the resources they need to access can help make them more productive and provide a seamless experience. Administrators at all levels can use standardized procedures for managing user credentials. Some levels of administration can be reduced or eliminated; for example, some companies might offer a self-service identity portal to support their users. A rich identity management function should support the delegation and distribution of administration capabilities, manually or automatically, among various organizations. For instance, a domain administrator can serve only the people and resources in that domain. This user can do administrative and provisioning tasks but is not authorized to do configuration tasks, such as creating workflows.

Hybrid identity management tasks

By distributing the administrative tasks in your organization, you can improve the effectiveness of administration and enhance the balance of

the workload of an organization. It can even be argued that self-service or delegated administration places the function at the heart of the business. For example, if a user is managing access to an application used by his corporate team, he is more inclined to do an accurate job of maintaining the access than a general administrator who has no connection to the team. Figure 8-6 shows the customary pivot points for an identity management solution.

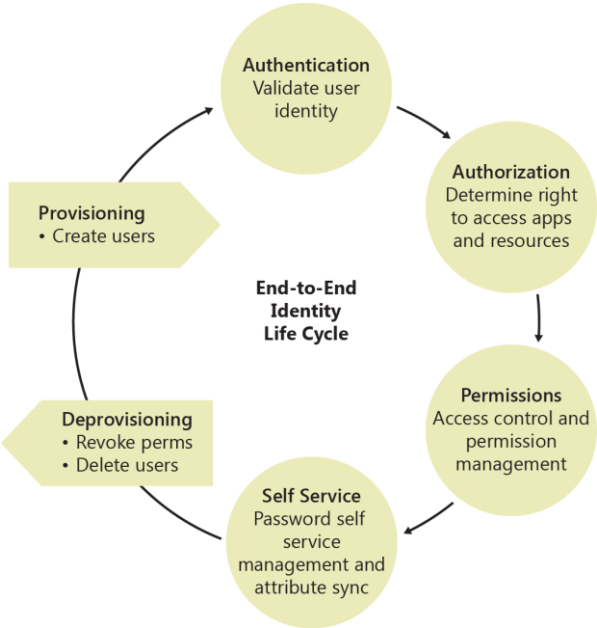


Figure 8-6: Identity management pivots.

The tasks presented in Figure 8-6 will vary from business to business. A solid understanding of the organization's characteristics will help you to determine the details for implementing a hybrid identity management solution. It is important to understand the current repositories being used as the sources of authority for identities and attributes. By knowing those core elements, you will have the foundational requirements, and based on that you can design an effective solution. In most cases, when we look at the identity management needs for Office 365 and SharePoint Online hybrid solutions, we are talking about Windows accounts mastered on-premises and synchronizing those accounts to Azure Active Directory. It is important to think beyond just the user accounts, though, and look a little deeper at the additional configuration steps.

Provisioning

- Does the identity solution support an account access management and provisioning system?
- How will users, groups, and passwords be managed?

- Is the identity life cycle management responsive?
- How long do password updates or account suspension take?

License management

- Does the identity solution handle license management?
- Does the solution handle group-based license management?

Integration with other third-party identity providers

- Can this identity management solution be integrated with third-party identity providers to implement SSO?
- Is it possible to unify all the different identity providers into a cohesive identity system? How and which are they and what capabilities are available?

Synchronization management

Implementing some form of synchronization management is critical to the success of an overall identity management solution. You want your user experience to be as simple and, where

possible, as seamless as it can be. You can help make this happen if you can keep all the identity repositories synchronized to a centralized master. This means the user enters the same password on-premises as she does in the cloud; at sign-in, the password is verified by the identity solution. This model uses a directory synchronization tool.

The capabilities of the Azure Active Directory synchronization tool were analyzed in depth in [*Planning and Preparing for Microsoft SharePoint Hybrid*](#). In this scenario, you are most interested in ensuring that the deployed solution can offer directory synchronization, including password synchronization and also support the configuration of Active Directory Federation Services (AD FS) for SSO if required by the business. Leading on from these simple requirements, you can begin to look at more complex needs and here we are stepping into an area where you need to do some additional research based on the requirements of your particular business.

For a look at the breadth of synchronization tools that are available, go to <https://azure.microsoft.com/documentation/articles/active-directory-hybrid-identity-design-considerations-tools-comparison/>. What will

become clear to you when you read this article is that Microsoft is investing heavily in the Azure Active Directory Connect (AD Connect) tooling, bringing new features to the platform in future releases; for example, today if you wanted to synchronize with Lightweight Directory Access Protocol (LDAP) directories or customer repositories such as Oracle or SQL Server, Microsoft Identity Management is required. In a future release of Azure AD Connect these directories will be accessible without deploying a full-blown Microsoft Identity Management-based solution.

For a fully detailed guide to deploying Azure AD Connect to support your synchronization needs read the article at

<https://azure.microsoft.com/en-gb/documentation/articles/active-directory-aadconnect/>.

Microsoft Identity Manager 2016

Earlier, we discussed some of the features that can help you to provide a rich user life cycle management experience. Microsoft Identity Manager (MIM) 2016 provides many of those features.

MIM 2016 helps you manage the users, credentials, policies, and access within your organization. It also provides a hybrid experience, privileged access management capabilities, and support for new platforms.

This version of MIM provides new features such as Privileged Access Management and support in Certificate Management for REST API access. In Certificate Management, there is now added support for multiforest topologies, a Windows store app for virtual smartcard and certificate life cycle management, updated events, and troubleshooting capabilities. Self-service scenarios now include Account Unlock and multifactor authentication gate for Password Reset.

Hybrid experience

Hybrid reporting in Azure presents your cloud and on-premises data in one place. Also, the self-service Password Reset portal supports Azure multifactor authentication (MFA).

Privileged Access Management

Privileged Access Management controls and manages administrative access by providing temporary, task-based access to sensitive resources. This means that you can give users

only as much permission as necessary, which lowers the chances of a cyber attacker gaining full administrative access. In addition, Privileged Access Management extracts and isolates administrative accounts from existing Active Directory forests.

Search

When we consider the hybrid search scenarios, there are a few things that need to be considered for ensuring that users have a good experience.

Using result blocks provides one end-user experience and is a common approach to identify the remote search index content. The use of search verticals can lead to a much better experience, and we recommend their use wherever appropriate.

Search verticals

The use of search verticals is not new, SharePoint Server actually has several configured on the out-of-the-box search center results page (see Figure 8-7). However, when we bring the concept of hybrid into the picture, these default search verticals are not particularly useful to us.

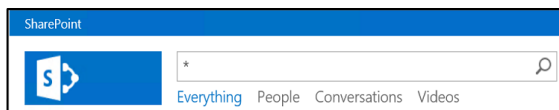


Figure 8-7: Out-of-the-box search center results page search verticals.

We need to configure search verticals that are beneficial to the user searching within a hybrid environment. As a consequence of extending the capability of a feature the user is already familiar with, we do not introduce any new adoption barriers or training requirements. The end-user experience is not disrupted in any way. Figure 8-8 shows the search vertical experience for a OneDrive-only search configuration.

For an in-depth look into using search verticals to introduce OneDrive for Business search results into an on-premises search center, but as a search vertical instead of a result block, go to <https://blogs.msdn.microsoft.com/spses/2014/07/05/configure-onedrive-for-business-as-a-hybrid-search-vertical-in-sharepoint-onpremise-search-center-part5/>.

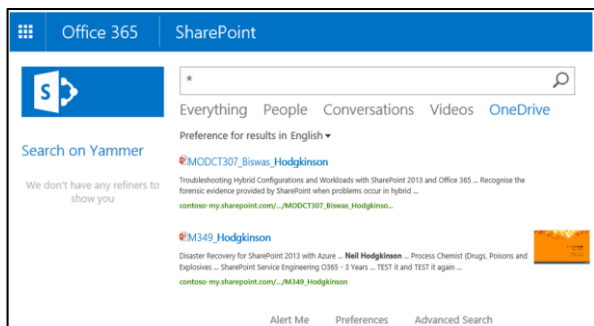


Figure 8-8: Search center results page showing a search vertical configured for OneDrive content only

OneDrive for business is not the only content that can benefit from being available as a search vertical. We can also augment the out-of-the-box verticals such as People and Videos to add context around the location of the items, whether on-premises or in Office 365. For more information on configuring hybrid search verticals read the authors' blog at <https://blogs.msdn.microsoft.com/spses/2015/03/19/configuring-search-verticals-video-conversations-people-for-hybrid-search-experiences-in-sharepoint-2013-and-sharepoint-online-part6/>

Cloud Search Service Application

The Cloud Search Service Application is a relatively new feature, having only become generally available in March 2016. Although the Cloud Search Service Application appears overall much like any other, there are two key aspects to its operation that you need to consider. The first is removal of content, and the second is the Access Control List (ACL) mapping process that supports the security trimming mechanism at query time.

Indexed content removal

Chapter 7 discusses the approach to removing indexed on-premises content from the Office 365 search index. The topic is so important that it deserves a second mention here in the recommended practices for operating the Cloud Search Service Application. We recommend that you take a little time to review Chapter 7 in detail, but to recap, here are the main points:

- Never use Index Reset as a means of purging the on-premises content from Office 365 Search Index.
- You trigger a delete crawl by removing start addresses from on-premises content sources or by deleting the entire content source.

ACL mapping process

In the hybrid world, identity is king, and ensuring that a user's identity is available in multiple places and to all the services the user might use is critical to a good user experience. This requirement is absolutely critical when we consider the user experience in cloud hybrid search, especially the trimming of search results based on the ACLs applied to the items. Figure 8-9 shows a high-level overview of the ACL mapping process.

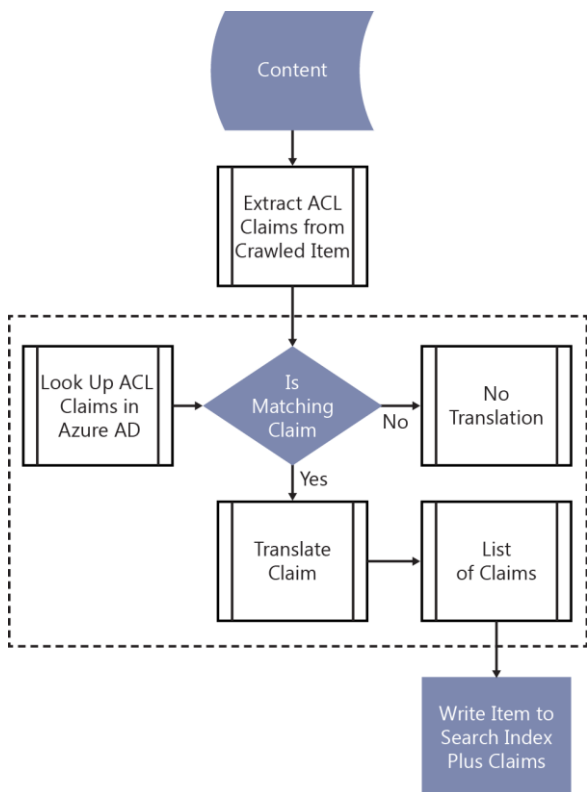


Figure 8-9: Schematic of the ACL mapping process within the Search Content Service.

The Search Content Service in Office 365 has an ACL mapping feature that reads in the ACLs associated with each crawled item and performs

a lookup into Azure Active Directory for a matching entry. If there is a matching entry, the claim is retained, if there is no matching entry, the claim remains untranslated. When all of the entries in the ACL have been processed, the item is sent for processing into the search index along with the translated and nontranslated claims. At query time, only users with user or group claims that match the translated ACL entries will be able to retrieve the item.

The on-premises administrators now need to think carefully about user and search administration, given that the Cloud Search Service Application has a direct dependency on the directory synchronization process. Let's take a look at an example:

Contoso has implemented the Cloud Search Service Application and is crawling an on-premises site collection named `humanresources`. The incremental crawl schedule is every 30 minutes. Contoso is running Azure AD Connect for directory synchronization with a delta synchronization every three hours. A new hire, Molly, is given permission on the `humanresources` site and can successfully sign in and access the site content. After 30 minutes, the incremental crawl runs and the new ACL change due to adding Molly's account to the site is

processed by the Cloud Search Service Application. At this point, however, directory synchronization has not happened, so Molly's account is not yet synchronized to Azure Active Directory. When the ACL mapping process runs for the crawled human resources site, Molly's account is processed from the on-premises ACL entries, but no matching item is found in Azure Active Directory. Therefore, Molly's ACL is not translated and hence cannot be included in the security trimming process at query time. As a consequence, despite having the correct permission to the on-premises content and a crawl of that content has been carried out, Molly is unable to retrieve the items when querying the Office 365 search index.

Even after directory synchronization has taken place and Molly is able to sign in to Office 365, she will not be able to locate the item in the search index because there is no cloud-based retrospective reprocessing of untranslated ACL entries. The humanresources site administrator would need to make a change on the site to trigger a security crawl or else perform a full reindex of the site in order for Molly's user account to be able to retrieve the site contents from search.

This example shows the dependency between the crawl schedule of the Cloud Search Service Application and the synchronization of user accounts to Office 365 Azure Active Directory. administrators need to be aware that adding users directly to sites might require another full crawl of the content if the user does not already exist in Azure Active Directory at the time of the first crawl after the change has been made. If a new user is added to an Active Directory group that is used to secure access to a site, the crawl schedule is less of a concern because the indexed item is secured with a group claim, not a user claim. After the user synchronizes to Azure Active Directory, she will also have that group claim and thus can retrieve items successfully.

The scenario is summarized in the following table:

Access granted method	Directory sync required	Extra full crawl required
User added directly to content	Yes	Yes, if crawl already ran prior to sync No, if sync ran prior to crawl

User added to existing Active Directory group	Yes	No

Another aspect of this ACL mapping process comes into play when considering not just individual user accounts accessing content, but also Active Directory groups and dynamic membership objects such as the Everyone or Authenticated Users groups. There are two issues elements of which you should be aware:

- Some dynamic groups will be remapped to equivalent Office 365 Azure Active Directory groups.
- You cannot synchronize all domain accounts and groups to Office 365 Azure Active Directory.

The first of these is relatively simple to handle. Groups such as the Everyone group and Authenticated Users group, which are often found when an administrator configures blanket access to a resource, will be remapped to different group names by the ACL mapping process in the Search Content Service. Both of these groups will be remapped to the Office 365

Azure Active Directory Everyone Except External Users Group. This means items secured with those Groups on-premises will still be retrievable in an Office 365 Search.

The second item is a little trickier to handle, and it stems from the fact that Active Directory has the concept of built-in users and groups; for example, the Domain Administrator account and the Domain Admins group. These built-in users and groups have a property of `IsCriticalSystemObject` set to true on the account. This automatically prevents the account from synchronizing to Office 365 Azure Active Directory. Figure 8-10 shows the property for an Admin account.

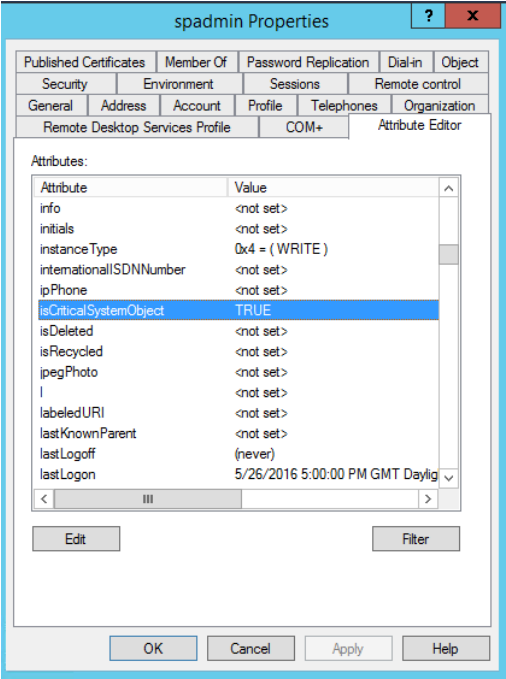


Figure 8-10: User account attributes, with the `IsCriticalSystemObject` property set to `TRUE`.

The importance of this attribute is seen when on-premises content is secured by using built-in groups. For example, a company might secure its local intranet to be accessible to the Domain Users built-in security group. A reasonable thing to do you would think, except in the world of the

Cloud Search Service Application. Content secured by using built-in groups will be crawled and passed to the Search Content Service; however, the ACL mapper will be unable to resolve and match those built-in groups in Office 365 Azure Active Directory. This will result in the group claim not being translated and therefore making all of the content on the intranet site not retrievable by search.

The recommendation, therefore, is that when you deploy the Cloud Search Service Application for a hybrid search experience, you should audit your crawled content and replace all built-in groups in the ACLs with new custom Active Directory groups.

Auditing and transparency

Probably one of the most commonly asked questions when any customer is implementing a hybrid platform is how can they audit or “see” what their users are doing. When the application spans the boundary between on-premises and Office 365, there is a perception that the administrator can see only half of the story, and to some small degree that is true. If, for example, you consider a wholly on-premises solution

consisting of perhaps SharePoint server, Office Online Server, and Provider Hosted Apps, the administrator here has access to multiple data repositories where auditing data is stored or log-file data is available to generate reports. Here are some examples:

- On the SharePoint server, there are the Unified Logging Service (ULS) logs that can provide deep technical forensic information for not only a user accessing the system, but also which services were used by the user after he signed in.
- The Internet Information Services (IIS) logs will provide a profile of user access and file access over time and are the most common source of reporting used to profile a website for traffic statistics.
- On the Office Online Server, there are also ULS logs and IIS logs available to profile the system access. Finally, the Provider Hosted App, if on-premises, can be written to support any form of custom logging or additionally will also have web server logs for the administrator to analyze.

This means that the administrator can build up a complete end-to-end picture of the

authentication and application data flow throughout the on-premises environment.

In Office 365, this is quite different. SharePoint Online, just like on-premises, has ULS and IIS logs, but these are not accessible to the tenant administrator and are configured to help Microsoft support teams assist customers with support tickets. So, what can the tenant administrator do to audit the access to resources or consumption of services in the hybrid world? Well, to begin with, Microsoft has invested heavily in the concept of SPInsights (currently in preview) and the Compliance Portal. Here, the administrator can see reports showing administrative access to resources from both on-premises and Office 365.. You can follow updates to the SPInsights feature here at <https://technet.microsoft.com/library/86e0fc90-0ef8-4c22-9d3b-7af42bf882f1>.

Auditing content access

For the administrators of a hybrid platform, there are a few configuration items that should be considered and modified to suit the needs of the business. It is tempting at first to dial everything up to the maximum, retain every log, and ensure that every log has the smallest of details recorded. In most cases, this is unnecessary and,

in fact, can be somewhat detrimental to the operation. The classic example being an administrator for the on-premises SharePoint server who turns on VerboseEx granularity on the ULS logs and then wonders why his drives are full. VerboseEx mode does indeed capture everything, but it results in enormous log files and can introduce performance penalties on every businesses' SharePoint farms.

You can turn on VerboseEx logging only by using the Windows PowerShell `Set-SPLogLevel` cmdlet, as demonstrated here:

```
Set-SPLogLevel -TraceSeverity VerboseEx
```

We recommend that you use this setting only for troubleshooting scenarios; you should return the logging to default afterward by using the `Clear-SPLogLevel` cmdlet. `Clear-SPLogLevel` has no parameters but just resets the logging to default.

Another topic that frequently catches people out in the on-premises and Office 365 world is the concept of site collection–level audits. You can control many aspects of site collection–level auditing, which is covered in depth at <https://support.office.com/article/Configure-audit-settings-for-a-site-collection-a9920c97-38c0-44f2-8bcb-4cf1e2ae22d2?CTT=5&origin=HA102772739&C>

[orrelationId=1884e905-d8a4-426f-9e19-3827133255ff&ui=en-US&rs=en-US&ad=US](#)

The aspects you should be more concerned about are at the configuration level (see Figure 8-11). Audit logs can take up a lot of space in the content database, so setting the options for trimming the logs is important and should be done in both SharePoint on-premises and Sharepoint Online. Optionally, choose to archive the reports before the data is removed.

Configure Audit Settings

Audit Log Trimming
Specify whether the audit log for this site should be automatically trimmed and optionally store all of the current audit data in a document library. The schedule for audit log trimming is configured by your server administrator. [Learn more about audit log trimming.](#)

Automatically trim the audit log for this site? ☒ Yes ☐ No

Optionally, specify the number of days of audit log data to retain:

Optionally, specify a location to store audit reports before trimming the audit log:

Figure 8-11: Configure Audit Settings page.

Auditing identity management

As well as access to content, the administrator might be interested in auditing sign-in attempts at the federation-services level. You can turn on AD FS success and failure auditing, and it is recommended that you do so for security auditing.

More info To read more about security auditing, go to

https://technet.microsoft.com/library/adfs2-troubleshooting-configuring-computers%28WS.10%29.aspx#bkmk_ConfigureAuditing.

The identity management options were discussed earlier in this chapter, but what you might find of interest from an auditing perspective is how to locate the Azure AD Connect log files. Those files are located in C:\Users\<Installer User ID>\AppData\Local\AADConnect.

You can view administrative actions related to hybrid identity management in the cloud in the Audit and Compliance center logs, which you can access at

<https://support.office.com/article/Search-the-audit-log-in-the-Office-365-Security-Compliance-Center-0d4d0f35-390b-4518-800e-0c7ec95e946c?ui=en-US&rs=en-GB&ad=GB>, again this topic is reviewed in Chapter 9.

Scalability

Hybrid scenarios don't always conform to the same scalability approaches as pure on-premises or pure cloud-based solutions. If we look at the end-to-end hybrid configuration, we can break down the scalability aspects into two key areas:

scaling for the identity management piece, and scaling for the content or user load.

Scaling identity management

Identity management can be further broken down into subsections: directory synchronization and identity federation. For synchronization, the challenge is that Azure AD Connect—indeed all the Azure Active Directory synchronization products—support only single-instance deployments. This means if that machine fails for some reason, you can no longer carry out directory synchronization which could have negative impacts on the user life cycle management workflow. Microsoft recommends having a second server with the Azure AD Connect software installed and with Staging Mode turned on. This staging server will be configured and will have all of the settings ready for synchronization. The metaverse (an intermediate database) is fully populated and ready to export data back to Azure Active Directory when staging mode is turned off. This saves a lot of time when commissioning a new server because it is ready to take over as a backup in the event of the primary server going offline or for primary server maintenance. For scaling-up the single server instance, we find that Azure AD Connect is dependent on memory

and drive as the number of objects being synchronized increases.

Number of AD objects	CPU	Memory	Drive space
<10,000	1.6 GHz	4 GB	70 GB
10,000–50,000	1.6 GHz	4 GB	70 GB
50,000–100,000	1.6 GHz	16 GB	100 GB

As the number of objects in Active Directory increases past 100,000 there is a requirement to implement a full version of SQL Server rather than the default Windows Internal Database (WID).

Number of AD objects	CPU	Memory	Drive space
100,000–300,000	1.6 GHz	32 GB	300 GB
300,000–600,000	1.6 GHz	32 GB	450 GB
>600,000	1.6 GHz	32 GB	500 GB

The other part of the identity management function is when you come to consider federated identities and scaling the federation solution to support the number of users accessing applications, remembering of course that identity federation may be in place for more than just our hybrid solution. Microsoft recommends that you review the published documentation on Azure AD Connect Hardware and Software requirements before deploying a new server. You can find these requirements at <https://azure.microsoft.com/documentation/articles/active-directory-aadconnect-prerequisites/>.

Microsoft has developed a federation services calculator which is useful to determine the number of federation servers you need to support your user population. In reality, this rarely exceeds a requirement for two AD FS servers, and if you consider that we recommend that you deploy two federation servers as a minimum to ensure high availability, this almost becomes a moot point as all corporations will deploy two. This same rule applies to the federation proxies. We will always deploy a minimum of two federation proxies to ensure high availability of the platform.

You can find the federation server calculator on the article at <https://technet.microsoft.com/>

library/gg749917.aspx, which discusses federation server capacity.

Scaling for content

Hybrid solutions are typically driven to make the most of the features offered by cloud-based products, and hybrid SharePoint server with Office 365 is no different. The OneDrive for Business platform is designed to deliver large-scale collaboration and consumer-based storage of personal files, all resident in Office 365 and utilizing Microsoft Azure Storage at the backend; equally, the hybrid Cloud Search Service Application is designed to feed the search index located in Office 365. The common denominator here is that Office 365 takes care of the capacity elements; the company administrator no longer needs to consider the impact of purchasing additional capacity to support the needs of the users. The Cloud Search Service Application is a true hybrid platform in every sense of the word. It has a service architecture that is distributed between SharePoint on-premises and SharePoint Online. With this in mind, you need to look at the scalability aspects of the online components and then how the business requirements might dictate scaling in the cloud.

As is discussed extensively in Chapter 2, there are two functions of the Cloud Search Service Application of which you need to be acutely aware. The first of these is the indexing flow, and for the Cloud Search Service Application, this consists only of the crawler function. Gathered content is sent to Office 365 for processing, and Microsoft will take care of the scaling in that part of the service. We do, however, need to track crawled content just the same way as a regular search service application and that means scaling the crawl databases. The scaling is identical to the on-premises only calculation in that you need to deploy a new crawl database for every 20 million items crawled. Related to the crawler function and item count is the support that Microsoft will provide for the number of items actually crawled with the Cloud Search Service Application. The default number of items each tenant can crawl is one million and is based on the default amount of pooled storage available to a tenant. This pooled storage is augmented by the number of licensed users. For example, if a tenant has 10,000 licenses, each license gains an additional 500 MB of pooled storage. 10,000 user licenses are then equivalent to an additional 5 TB of storage, meaning that the tenant can now index an additional five million items into the Office 365 search index. Here it is defined as an equation:

Indexable on-premises Items = $(1 + (\text{No of licenses} \times 0.0005)) \times 1,000,000$

This equates to 1 million + 1 million for every 2,000 licensed users. Of course, a tenant can have much more indexable content than licenses, in which case, he can choose to purchase additional Office 365 storage for his subscription and add that to the pooled storage account. For example, a tenant has 2,000 users but needs to index 5 million items. It gets 1 million items default plus another million for its 2,000 licenses (500 MB x 2,000) but will need to purchase an additional 3 TB of pooled storage to support indexing a total of 5 million items.

Note The pooled storage in your tenant does not include the OneDrive for Business capacity when calculating the number of indexable items.

On the query side, the administrator needs to consider two things: support for query in a highly available strategy, and query throughput. Search query will always be available from the Office 365 SharePoint Online search center, but if you're federating from on-premises to Office 365, you might want to consider deploying a highly available query capability. A default Search Service Application deployment includes

just one Query Component, adding one or more additional components provide high availability for the search query function. For scaling to the needs of an active user base, additional query servers (beyond the default of one) provide increased throughput in terms of queries per second. In this case, the rules for scaling search on-premises come into play. We advise that you review the article at <https://technet.microsoft.com/library/dn727115.aspx> for guidelines on scaling-out enterprise search functions.

Supportability

As with all Microsoft products and technologies there are guidelines for deployment and use of the products that have supportability repercussions if you do not adhere to the boundaries. Some of these boundaries are purely recommendations and stepping beyond them does not break any conditions for supportability. Others are hard limits to which you must adhere; otherwise, it will affect your ability to seek assistance from Microsoft support services in the event you need help with the feature. We have called out a few such scenarios in the following sections to assist you with maintaining a supported configuration,

OneDrive for Business

OneDrive for Business really consists of two key elements: there is the cloud-based OneDrive library that each licensed user has in Office 365, and there is also the client-side synchronization component (onedrive.exe). If you intend to use the synchronization capability to accommodate offline access to your files on the local PC, there are some limitations you must follow to avoid running into difficulty. These limits are primarily related to the maximum number of items you can synchronize, the characters used in the file names and the depth of the folder hierarchy. For more specific details, read the article at <https://support.microsoft.com/kb/3125202>.

Hybrid Sites and following

When you turn on Hybrid Site following, the end-user experience is different depending on the on-premises farm version.

- With SharePoint Server 2013, the Sites link in a SharePoint server site is redirected to Office 365.
- With SharePoint Server 2016, the Sites tile in the app launcher is redirected to Office 365.

From a supportability standpoint, we recommend that the users always access the followed sites list in Office 365 even though when a user follows a site it is added to the followed list in both SharePoint server and Office 365.

It is important that the users understand that the Hybrid Site and following feature is limited to just that. It does not extend to the site-level newsfeeds or to the document and people following feature.

- Users will continue to have separate newsfeeds in SharePoint server and Office 365, and each will show activities for sites and documents for SharePoint Server and Office 365, respectively.
- Follow documents functionality remains unaffected.
- Follow people functionality remains in SharePoint server only.

Note Existing followed sites lists in SharePoint server are not migrated to Office 365 when you turn this feature on (though any sites in the Office 365 list will remain there). Users will need to follow their SharePoint server sites again, after the feature is turned on.

Hybrid profiles

Hybrid profiles provides users with a single profile in Office 365 where they can maintain all of their profile information. There are a couple of scenarios to be aware of regarding the capabilities of this feature:

- If you choose to use a SharePoint audience when you configure hybrid sites features, nonhybrid users (those not in the audience) retain their SharePoint server profiles, and they also have profiles in Office 365 if they are licensed Office 365 users. This could cause some confusion if the audience is not managed carefully.
- In the past, customers have resorted to a number of custom approaches for populating the user profile properties in Office 365. These approaches are generally based on client-side object model (CSOM) and in the main provided limited capabilities. Microsoft has now released a user profile bulk API for this functionality and we strongly recommend that customers switch to this option because it will be maintained by Microsoft going forward. There is also a synchronization tool that uses the bulk update API.

More info To learn more about the bulk update API, go to <http://go.microsoft.com/fwlink/?LinkId=786318>.

Hybrid search

Chapter 2 discusses supported requirements for certificates for hybrid search scenarios; however, you should be aware of a couple of additional supportability guidelines to hybrid search:

- You can deploy only one Cloud Search Service Application per single SharePoint server farm.
- If a Cloud Search Service Application is deployed to the same farm as an existing Search Service Application, the two applications must not share topologies. For example, you must not deploy a Cloud Search Service Application component onto the same server as an existing search service application component.
- You can deploy the Cloud Search Service Application to multiple on-premises SharePoint Server farms, and each can be connected to the same Office 365 tenant.

This provides support for geo-distributed enterprises.

- If multiple Cloud Search Service Applications are connected to the same Office 365 tenant, they must not crawl the same content, and we strongly recommend that some form of content source naming convention is followed to ensure unique content source names.
- The Cloud Search Service Application does not provide support for custom security trimming, and you must carry out all search schema management at the tenant level. On-premises schema changes will be ignored, and this also means that you cannot use the Extensibility Web Services Callout with the Cloud Search Service Application.

Chapter 7 discusses the approach for purging on-premises content crawled by the Cloud Search Service Application.

- From a support standpoint, we strongly recommend that you use the purge operation only as a last resort and only once.
- After running of the purge process, there is no feedback to the administrator, but running a query by using

IsExternalContent=1 will show a reducing response count as the process completes. Only if the administrator feels the process is stalled or failed should he try again.

- When the purge process is running you must not attempt to crawl on-premises content with the Cloud Search Service Application.

Finally, the Delve experience is only enhanced when using the Cloud Search Service Application. If you're using traditional inbound or outbound hybrid search, there is no detection of on-premises managed properties that can feed the Office 365 search index. Only the Cloud Search Service Application can do this by enhancing Delve with Author and Editor data from on-premises content.

Microsoft SharePoint hybrid and cybersecurity

This chapter is dedicated to addressing cybersecurity concerns of organizations that might be considering the cloud and, more specifically, a hybrid SharePoint environment. As an experienced cloud services provider, Microsoft understands the risks associated with cybersecurity and has invested heavily in ensuring that Microsoft Office 365 and Microsoft Azure have the appropriate security

policies, checks and balances, risk mitigation plans, and operational excellence to provide a secure platform. However, the real risk is when comparatively lower investments in security practices are made by customers who consume the cloud. These risks are heightened in a hybrid context because there are connections across the Internet, mobile workforce, external collaboration partners, and new architectural scenarios. This chapter covers not only the technical aspects of cybersecurity but also touches a bit on governance required to ensure you, as an administrator, are

empowered with controls and context so that you can make an informed risk decision.

Overview

This chapter is dedicated to the security around SharePoint hybrid and addresses concerns of businesses on the broad topic of cybersecurity. Cybersecurity and risk management is at the forefront of many government initiatives.

Programs for increasing the awareness of the threat of cybersecurity is increasing, with large universities and corporations such as Microsoft investing in bringing computer science and security-related education to students. For organizations, it is important to create a security risk-aware workforce, especially when there are remote and mobile workers, external collaboration, and a global presence. Security is a team effort; it is not something you can centralize and forget about.

Let's now have a look to at the various areas of cybersecurity that you need to be concerned about when running a SharePoint hybrid deployment. We will go through some concepts

that might be familiar to you if you are versed in cybersecurity or are an IT professional; however, this chapter is intended for a larger audience, including management and decision makers who are concerned about hybrid security. If you're a SharePoint consultant or SharePoint hybrid administrator, you can use this chapter to highlight the risks, create awareness of the solutions to address those risks, and provide your organization or clients with a strategy for securing their hybrid environments.

Following are some frequently asked questions:

- Is my organization's data safe in Office 365?
- Who in Microsoft has access to my organization's data?
- What is Microsoft doing to protect my data and comply with regulatory requirements?
- How can I verify that Microsoft is doing what it says?
- Where is my Office 365 data located? Does it ever leave my country or region's borders?
- Is my on-premises data exposed to outsider attack in a hybrid environment?

These questions are addressed in this chapter, which includes the combined application of technologies, processes, and controls in place at Microsoft and in your own organization. The last question is an on-going process for you and your organization. The section “Risk remediation” later in this chapter can help you to begin preparing your own risk mitigation security plan.

What is cybersecurity?

Cybersecurity comprises technologies, processes, and practices aimed at defending networks, systems, and the data therein from a breach in security resulting in unauthorized access, change, or destruction. With SharePoint hybrid, we need to consider the devices used to protect the network, applications deployed to scan for software threats, processes for handling proactive and reactive security incidents, management of security and network infrastructure, and good practices for operation excellence, in both on-premises and cloud application. This means that Microsoft and you (as the customer) together are responsible for maintaining your cybersecurity, due to the unique nature of hybrid convergence.

What is a threat

In cybersecurity, a threat is a potential risk to exploit a network, system, or application vulnerability to gain unauthorized access to cause financial theft, intellectual property theft, and other harm. There can be insider threats and outsider threats. A person who performs an activity that exploits a vulnerability or a security hole is referred to as an attacker. A threat can be intentional or unintentional. Other threats in a broader context can include accidents such as fires, natural disasters, and floods. The destruction of data by any sort of means is a threat to business continuity, and you must take adequate risk mitigation measures to minimize these impacts.

What is identity theft

Identity theft is the activity of fraudulently gaining access to secured resources by pretending to be someone else. This can happen by using someone else's name and personal identification information to gain access to secured networks, systems, and data.

Here are some common examples of identity theft:

- **Phishing** This is the practice of sending emails to trick you into revealing your personal information such as passwords.
- **Hacking** This involves gaining unauthorized access to secured networks, systems, and data by exploiting weaknesses in either security practices or in the system. In addition, there is *social engineering* or *social hacking* whereby an attacker is able to gain access by socially manipulating you or your employees through trickery.

What is risk management

In cybersecurity, risk management is the evaluation of cybersecurity risks and predicting the likelihood of these risks occurring. Risk management also spells out the procedures to help avoid or minimize their impact. When building a SharePoint hybrid environment, it is necessary to address the likelihood of potential risks occurring, especially when your users are bringing in their own devices, collaborating on files, and connecting to public Wi-Fi hotspots. What happens if a device with offline synchronized Microsoft OneDrive for Business files is stolen or lost during one of your sales representative's travels? Those are the sorts of risks you need to think about. You will need to

have the necessary knowledge of the security controls available with each risk and apply a suitable remediation strategy to mitigate these risks.

We look at this in greater detail in the section “Risk mitigation strategy and risk remediation” later in this chapter.

What is data encryption

Data encryption is the process of converting data (plain text) into secret code, transporting that data (cipher text), and then, when delivered to its destination, reconverting the cypher text back to readable data so that the intended recipient can view and understand it. The intended reader at the destination needs to have a secret key or password to decipher the text for it to be understandable. Encryption is the most effective way to achieve data security.

What is compliance

Compliance is the state of aligning with guidelines, regulations, and legislation set by outside parties such as vendors, industry organizations, and government bodies. As a cloud provider, Microsoft complies with industry standard regulations, and is designed to meet

regulatory requirements through Office 365. Using Office 365 will also help you to comply with your specific industry regulations. A couple of examples of regulations in the United States are the *Health Insurance Portability and Accountability Act* (HIPAA) and the *Federal Information Security Management Act* (FISMA).

Office 365 security

When transitioning to a SharePoint hybrid environment, you might be concerned with the security of Office 365. For years, you have probably hosted everything yourself in your own facilities by choice, by regulatory factors, or delays in decision making with bureaucracy in your organization. Although these were certainly factors that kept you from looking at a SharePoint hybrid topology, you might find yourself in a position where you need to influence others to evaluate and consider the benefits of SharePoint hybrid. One of the main things to understand and communicate within your organization is the security that Office 365 brings to your SharePoint hybrid deployment. This section sheds light into what Office 365 and Azure security looks like and the great lengths taken to ensure that your data is safe.

As you use Office 365 services and Azure, you can be assured that Microsoft takes the stance that it's your data: you own it and you control it. Microsoft is the custodian of your data, but it remains yours and Microsoft is accountable to you. Figure 9-1 illustrates that the service is built on transparency and control, layered with built-in security by technology, processes, and controls, a strict policy of protecting your privacy with customer controls, and address compliance with various standards, and certifications.

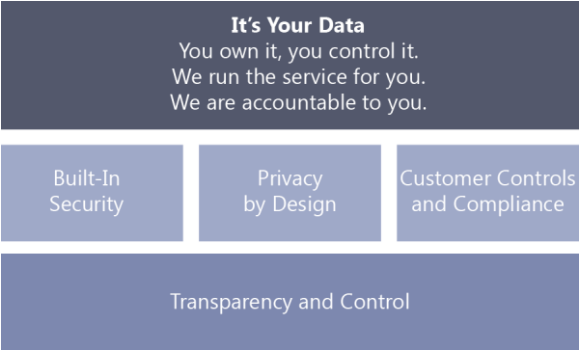


Figure 9-1: Office 365 data security principles.

Note To read the Office 365 Security and Compliance whitepaper, go to <https://www.microsoft.com/download/details.aspx?id=26552>.

To visit the Office 365 Trust Center, go to <http://trust.office365.com>.

Defense-in-depth

Defense-in-depth is an approach to cybersecurity whereby multiple layers of security controls are applied to defend against various security threats. Microsoft applies controls over many layers of defense-in-depth across its cloud services and infrastructure. Applying controls at multiple layers can sometimes involve employing overlapping protection mechanisms, developing risk mitigation strategies, and responding quickly and effectively to attacks when they occur, 24 hours per day, 7 days each week, 365 days a year.

Microsoft maintains a rich set of controls, and a defense-in-depth strategy ensures that if any one area should fail, there are compensating protections in other areas. Figure 9-2 shows the defense-in-depth layers of security that are part of the Office 365 security strategy.

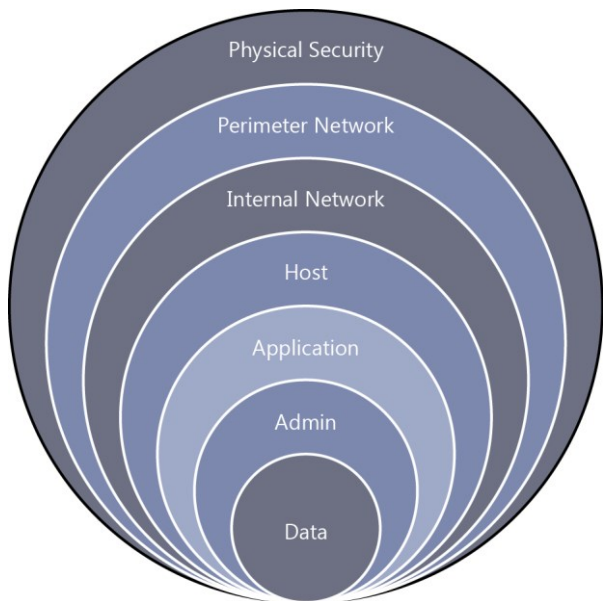


Figure 9-2: Defense-in-depth with Office 365.

Let's look briefly what goes on in each layer:

- **Data** Threat and vulnerability management, security monitoring, access control, data integrity, and encryption
- **Admin** Account management, training and awareness, screening

- **Application** Secure engineering, access control and monitoring, antimalware
- **Host** Access control and monitoring, antimalware, patch and configuration management
- **Internal network** Dual-factor authentication, intrusion detection, vulnerability scanning
- **Perimeter network** Edge routers, firewalls, intrusion detection, vulnerability scanning
- **Physical security** Physical controls, video surveillance, access control

Because Office 365 is a multitenant service, customers might share the same hardware resources, lowering operational costs—this, of course, is one of the primary benefits of cloud computing. Microsoft isolates co-tenant data through Azure Active Directory and has other features specifically designed to secure multitenant environments.

An important part of Microsoft's security capabilities includes an around-the-clock incident response process. In Microsoft, the Security Incident Management (SIM) team responds to potential issues with processes aligned with various international and United

States standards in information security incident management.

SharePoint Online encryption

Earlier, we introduced the concept of data encryption for SharePoint Online, OneDrive for Business, and related services. We'll now take a brief look at how Microsoft implements encryption with stored data (*data at rest*) and data that is being transmitted from one point to another (*data in transit*).

Note Soon, we expect to see functionality with which you, as an Office 365 customer, could bring and manage your own keys to encrypt your data stored in SharePoint Online. This announcement was made on May 4, 2016 at "The Future of SharePoint" event. To read more about it, go to <https://blogs.office.com/2016/05/04/the-future-of-sharepoint>.

Data at rest

You might recall that the release of SharePoint Server 2013 introduced the concept of *shredded storage*. When a file in SharePoint was edited, only the delta of the edit session is stored as a "shred" in the database. With Office 365,

Microsoft uses a per-file encryption system wherein a very small SharePoint Online and OneDrive for Business file might be stored as just one “chunk” or larger file across more chunks. All chunks (or shreds) are encrypted with unique keys (using AES 256-bit encryption), whether they are part of a small file or part of a large file. “Fort Knox” is a term that refers to a system for which chunks (fragments) are moved into randomly distributed and separate Azure storage accounts that are generated on demand. A different key is used to encrypt the deltas of each file as they are modified, resulting in blobs of secured data. Using the Azure Blob store allows for massive scalability of storage and, more important, very strong security at the file level. The set of encryption keys for these fragments of content is itself encrypted by using an independently generated master key (specific to each customer). The encrypted keys are stored in the content database, and the master key is stored in a separately secured and monitored key store. The “map” used to reassemble the file is stored in the SharePoint Content Database (in SQL Server) along with the encrypted keys, separately from the master key needed to decrypt them. Each Office 365 and Azure Storage account has its own unique credentials per access type (read, write, enumerate, and delete).

Each set of credentials is held in the secure Key Store and is regularly refreshed.

Note For Office 365 Government customers (US Government), data fragments are stored in Azure Government Storage. In addition, access to SharePoint keys in Office 365 Government is limited to Office 365 staff who are United States citizens and have been specifically screened. Azure Government operations staff do not have access to the SharePoint Key Store that is used for encrypting data blobs.

To read more about the Office 365 Government Community Cloud, go to <https://technet.microsoft.com/library/office-365-government.aspx>.

Microsoft uses BitLocker as the encryption tool for its data drives that hold customer content in Office 365 and Azure. Microsoft uses Advanced Encryption Standard (AES) 256-bit BitLocker-protected volumes that run Exchange Online, SharePoint Online, and Microsoft Skype for Business applications in Office 365 enterprise. It also is Federal Information Processing Standard (FIPS) 140-2 compliant. These BitLocker-protected drives are encrypted with a full-volume encryption key, which in turn is encrypted with a master key in a highly secured share.

More info For more information about data encryption in OneDrive for Business and SharePoint Online, go to <https://technet.microsoft.com/library/dn905447.aspx>.

Data in transit

When data is transmitted either intraserver, between datacenters, or client-server-client, there are various levels of encryption either active or available for customers to use.

Communication to SharePoint Online and OneDrive for Business between you and the Microsoft datacenter across the Internet uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) connections. All SSL/TLS connections are established by using 2,048-bit keys, with Perfect Forward Secrecy (PFS), and a strong cipher suite. All customer-facing servers negotiate a secure session using TLS with client machines.

If you are interested to view more details on the TLS versions, forward secrecy settings for clients using SharePoint Online, you can run a test using an online analyzer from Qualys SSL Labs at <https://www.ssllabs.com/ssltest/analyze.html?d=microsoft-my.sharepoint.com&hideResults=on>.

To check how you score, go ahead and run an SSL report on your federation service endpoint; for example, sts.contoso.com.

More info To read more about data encryption in OneDrive for Business and SharePoint Online, go to <https://technet.microsoft.com/library/dn905447.aspx>.

Other encryption tools

Let's now turn our attention to the tools that Microsoft has for customers to encrypt data in Office 365 that you can use for hybrid environments.

Azure Rights Management System

Microsoft offers Azure Rights Management System (RMS) for both Office 365 and on-premises servers and services to encrypt files and messages in transit and at rest. Azure RMS is integrated with Office 365 and recommended for all Office 365 customers. Azure RMS uses industry-standard cryptographic security to encrypt your content. You can also use Azure RMS with your on-premises SharePoint server via the RMS connector that acts as a relay between the on-premises SharePoint server and Azure

RMS. To learn how Azure RMS works, go to <https://docs.microsoft.com/rights-management/understand-explore/how-does-it-work>.

In a default Azure RMS implementation, Microsoft generates and manages the root key that is unique for each tenant. Customers can manage the life cycle of the root key in Azure RMS with SharePoint Online by using a method called Bring your Own Key (BYOK).

Note With Azure RMS, you can view a near real-time log showing all access to the root key at any time. For more information about logging and analyzing Azure RMS usage, go to <https://technet.microsoft.com/library/dn529121.aspx>.

Information Rights Management (IRM)

If you operate on-premises Active Directory RMS server, you can also configure Information Rights Management (IRM) to use an on-premises Active Directory RMS server to encrypt data.

You use IRM to secure communication inside your organization. IRM helps you secure your information by encrypting it and applying an intelligent policy so that only specified people can work on it. With IRM, you can allow only

specific recipients, such as your external business partners, to view a document and apply restrictions so that they are not able to forward it to others. Or, you can mark the document with a classification such as “company confidential,” so that external users cannot view it.

More info To learn more about Active Directory RMS (on-premises), go to [https://msdn.microsoft.com/library/cc747757\(WS.10\).aspx](https://msdn.microsoft.com/library/cc747757(WS.10).aspx).

Note Microsoft strongly recommends that customers utilize Azure RMS to use new features like secure collaboration with other organizations. To read more about migrating from Active Directory RMS to Azure RMS, go to <https://technet.microsoft.com/library/dn858447.aspx>.

Message Encryption

Secure Multipurpose Internet Mail Extension Secure/Multipurpose Internet Mail Extensions (S/MIME) makes it possible for a user to encrypt and digitally sign an email. An email that is encrypted using S/MIME can only be decrypted by the recipient of the email using his private key, which is only available to that recipient. As such, no one can decrypt the emails other than the recipient of the email.

S/MIME is a peer-to-peer encryption system, which means that encryption is implemented peer to peer such that no one “in the middle” can view the contents of an encrypted email, not even the administrator.

Users can compose, encrypt, decrypt, read, and digitally sign emails between two users in an organization using Microsoft Outlook, Outlook Web App, and Exchange ActiveSync clients.

Encryption of email messages and files is possible even when recipients are outside of Office 365 and are using an unknown email client. The recipient needs a Microsoft account or a unique one-time password to authenticate and access the encrypted email message. The recipient can view and respond to the message from his browser on his desktop or mobile devices by using Office 365 messaging encryption apps. The messages will continue to be encrypted.

More info Office 365 Message Encryption (OME) is a mechanism to apply encryption on emails that originate from Office 365. OME requires activation of Windows Azure RMS in the customer’s Office 365 tenant. With OME, tenant administrators can create transport rules that encrypt emails if they match certain criteria. To read more about OME, go to

<https://technet.microsoft.com/library/mt661609.aspx>

Customer Lockbox

In extremely rare circumstances, when Microsoft engineers need to access a tenant's online environment, an approval process called "Customer Lockbox" is followed to grant access to certain engineers for a limited time. This is different from a regular Lockbox approval process that engineers already follow to gain access to Office 365 datacenters. Microsoft engineers don't need standing access to the Office 365 datacenter—they use Lockbox to request time-limited, scoped access to the datacenter. Customer Lockbox takes that mechanism and applies it to customer content as illustrated in Figure 9-3. Customer Lockbox specifically protects customer content. When engineers use (regular) Lockbox to gain access to the datacenter, they can sign in to servers, but they still don't have access to customer content without raising a Customer Lockbox request. If a customer chooses to grant access (or if the customer has not opted in to the approval workflow), the engineer is granted a time-limited, customer-scoped permission to access customer content through well-defined

interfaces. The Microsoft engineers can access your content only if you approve it. For added security, a Customer Lockbox request expires after 12 hours. If you reject a Lockbox request, the Microsoft engineer is unable to access your content. To see who has administrative rights to Office 365, go to <https://www.microsoft.com/online/legal/v2/?docid=24&langid=en-us>.

Note Only in extremely rare circumstances would a Customer Lockbox request occur for which a Microsoft engineer needs access to your content to resolve a service issue. You have complete control if and when you want others to access your content to resolve a service issue if it ever arises.

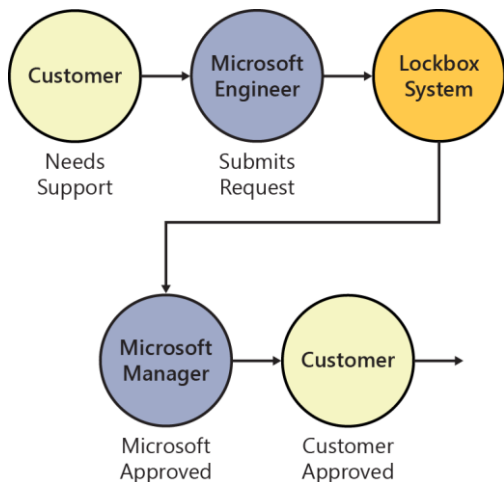


Figure 9-3: Customer Lockbox schematic at Office 365.

SharePoint Insights

Microsoft SharePoint Insights is a new hybrid feature, currently in preview. When it is turned on, this feature uploads unified audit data collected by the on-premises SharePoint Server 2016 Usage and Health Data Service Application to Office 365 to be processed by the Office 365 Unified Auditing Engine. The data uploaded from on-premises to your tenant partition for SharePoint Insights is as secure as your tenancy-specific usage data in Office 365.

After it has been processed, you will be able to view rich audit reports and logs from the new Security & Compliance Center in Office 365. There is also a new Office 365 Management Activity API which supports programmatic access to the report data.

Security & Compliance Center

The Office 365 Security & Compliance Center gives you control via security policies to ensure that your data is safe and secure, giving you control over your data and managing access when required. You can access the Security & Compliance Center by signing in to <https://protection.office.com>.

Data Loss Prevention (DLP) policies help you to ensure that your organization's sensitive information isn't shared with people who shouldn't see it. You can use DLP policies to manage and protect the content your users create and share, without interrupting their workflow.

Through additional features in the Security & Compliance Center, you can take charge of how and when data is stored, used, and retained or removed via retention policies and online archiving of mailboxes.

You have the ability to delegate granular role-based permissions in the Security & Compliance Center, such as the following:

- **Compliance Administrator** Manage settings for device management, DLP, reports, and preservation.
- **eDiscovery Manager** Perform searches and place holds on mailboxes, SharePoint Online sites, and OneDrive for Business locations.
- **Organization Management** Control permissions for accessing features in the Compliance Center and also manage settings for device management, DLP, reports, and preservation.
- **Reviewer** Use a limited set of analysis features in Office 365 Advanced eDiscovery. Members of this group can see only the documents that are assigned to them.
- **Service Assurance User** You access the Service Assurance section within the Security & Compliance Center. Members of this role group can use the section to review documents related to security, privacy, and compliance in Office 365 to perform risk and assurance reviews for their own organization.

- **Supervisory Review** Control policies and permissions for reviewing employee communications.

You also have the ability to create your own groups and assign specific roles due to the nature of some of the data that is made available in the Security & Compliance Center. Again, neither Microsoft nor its support staff have direct and unauthorized access to view the data in the Security & Compliance Center.

The Security & Compliance Center has its own set of Windows PowerShell cmdlets that you can use to manage compliance search, DLP, eDiscovery, and security permissions.

More info To view the available Office 365 Security & Compliance Center cmdlets, go to [https://technet.microsoft.com/library/mt587093\(v=exchg.160\).aspx](https://technet.microsoft.com/library/mt587093(v=exchg.160).aspx).

Security policies—DLP

In the Office 365 Security & Compliance Center, DLP under “Security Policies” helps you to identify sensitive information across SharePoint Online and OneDrive for Business. To protect sensitive information and prevent its accidental disclosure, DLP policies help you to locate and identify information such as financial data or

personally identifiable information (PII) such as credit card numbers, social security numbers, tax file numbers, or passport numbers.

With a DLP policy, you can do the following:

- Identify sensitive information such as PII, across many locations such as SharePoint Online and OneDrive for Business, or monitor specific employees OneDrive for Business sites. Figure 9-4 shows the prepopulated templates for DLP policy creation, making it easy to ensure compliance in your own organization.
- Prevent the intentional or unintentional sharing of sensitive information.

New DLP policy

What information do you want to protect?
Choose what kind of information you want to protect. Select Custom if you want to start from scratch. [Learn more](#)

Custom	Australia Health Records Act (HRIA)
Financial	Canada Health Information Act (HIA)
Medical	Canada Personal Health Act (PHIPA) - Ontario
Privacy	Canada Personal Health Information Act (PHIA) - Manitoba
	U.K. Access to Medical Reports Act
	U.S. Health Insurance Act (HIPAA)

Figure 9-4: The new DLP policy search templates.

More info To read more about DLP policies, go to <https://support.office.com/article/Overview-of->

Search & Investigation

Through the Office 365 Security & Compliance Center, you have the ability to conduct a search and investigation across a variety of sources—SharePoint Online, OneDrive for Business, Azure Active Directory, and Exchange Online. From a hybrid security standpoint, you are able to upload your SharePoint on-premises logs to conduct a truly hybrid search and investigation. This is important for you as an administrator to have access to be able to report on unsanctioned activities not only on-premises but also in Office 365.

Through the Search & Investigation section, you can do the following:

- Conduct a content search based on advanced queries by many different content metadata. You have the ability to export these results to your computer and optionally include versions of SharePoint documents. You can also run an analysis on your search results with Advanced eDiscovery.

- Conduct a search on audit logs from SharePoint Online including uploaded on-premises SharePoint logs. The audit logs contain a lot of activities such as file and folder activities, sharing requests, synchronization activities, site administration activities, user, group, and role administration activities.

Note By default, Audit Log Search is turned off. You would need to manually turn it on in the Audit Log Search section in the Office 365 Security & Compliance Center by clicking Start Recording User And Admin Activities.

- Conduct an investigation via eDiscovery, with which you can create a new case, place a hold on content, conduct searches via your case, and export content.

Compliance with standards and certifications

To get an insight as to how Microsoft cloud services compliance framework is actually structured, you would need to look at the various standards and certifications for which Microsoft has approval. Microsoft has a series of domains that are based on the ISO/IEC 27001 standard, along with specific industry

obligations, such as the Payment Card Industry Data Security Standard and the FISMA NIST SP 800-53 standard. The table that follows provides a glimpse of some of the standards certifications that Microsoft has achieved over the years. (Note: I compiled the information for this table through my own research from a few sources. The information is subject to change.)

Standards certifications	Market	Region
SSAE16 SOC1 Type II	Finance	Global
ISO 27001	Global	Global
ISO 27018	Global	Global
EUMC	Europe	Europe
FERPA	Education	United States
FedRAMP/FISMA	Government	United States
HIPAA	Healthcare	United States
HITECH	Healthcare	United States
ITAR	Defense	United States
HMG IL2	Government	United Kingdom

IRAP	Government	Australia
CJIS	Law Enforcement	United States
Article 29	Europe	Europe
SOC2 Type II	Global	Global
Safe Harbor	Global	Europe

Note The preceding table is for illustration purposes only. You are strongly advised to refer to the Continuous Compliance section of the Office 365 Trust Center at <https://products.office.com/business/office-365-trust-center-compliance> for up-to-date information. When considering Office 365, you should contact Microsoft or your account manager at Microsoft to obtain up-to-date information.

To view the regulatory and compliance documents available based on your industry and region, you need to sign in to the Office 365 Trust Center at <https://trustportal.office.com> and the Azure Trust Center at <https://azure.microsoft.com/support/trust-center>.

Furthermore, if you require, you can also request Microsoft to provide you a summary report of a

third-party certification by an independent auditor.

More info To learn more about where your data is located, go to <https://www.microsoft.com/online/legal/v2/?docid=25>.

To find out more where the Azure datacenter regions are located, go to <https://azure.microsoft.com/regions>.

SharePoint Online Compliance Policy Center

The Compliance Policy Center contains policies that will help you to protect the SharePoint content you require and delete the content you that is no longer needed. After creating a policy, you can assign it to a site collection or template.

You can create and manage deletion policies that can delete documents after a specified period of time. You can then assign these policies to site collections or site collection templates. Policies that include a default rule will be automatically applied without any site administration selection required. The SharePoint Online Compliance Policy Center is a site collection that is created by default for every tenant in Office 365 with its URL in the following

format: <https://contoso.sharepoint.com/sites/CompliancePolicyCenter/default.aspx>.

Advanced Security Management

Office 365 Advanced Security Management is a service for Office 365 enterprise plans to give you greater visibility and control over your Office 365 environment. It is included at no additional cost for Office 365 E5 subscribers. With Office 365 Advanced Security Management, you are able to identify high-risk and anomalous behavior; suspicious usage; detect threats and security incidents; utilize granular controls and security policies available; get enhanced visibility into your Office 365 usage and potentially rogue software; and carry out configuration without installing an end-point agent.

Advanced Security Management also provides an app discovery dashboard with which you can visualize your organization's usage of Office 365 and other productivity cloud services, such as Box, Dropbox, and other cloud storage providers. All you need to do is take the logs from your network devices and upload them via an easy-to-use interface.

To go to the Advanced Security Management service, in the Office 365 Security & Compliance Center, in the Alerts section, click Manage

Advanced Alerts, and then click Go To Advanced Security Management. Alternatively, you could visit Advanced Security Management by signing in, for example, to <https://contoso.portal.cloudappsecurity.com>. Figure 9-5 depicts three alerts in the dashboard that shows an unsanctioned cloud user named “administrator” created in Office 365 that is a matter of concern. We also notice a user named awein@contoso.com signed in from Australia a day ago and then the United States four hours ago—a matter of concern to be investigated. After it has been remediated, you can either dismiss or resolve the alert.

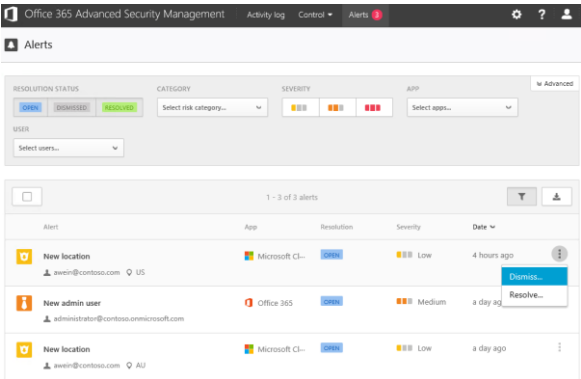


Figure 9-5: Office 365 the Advanced Security Management dashboard.

More info To read more about the enhanced visibility and control with Office 365 Advanced Security Management, go to <https://blogs.office.com/2016/06/01/gain-enhanced-visibility-and-control-with-office-365-advanced-security-management>.

Government accessing your data

Microsoft has stated on many occasions that it is committed to reinforce legal protections for its customer's data. Microsoft does not provide any government with direct, unfettered access to your data nor does it assist any government by providing encryption keys or breaking encryption in anyway. There are no back doors into Microsoft's products and Microsoft takes steps to ensure governments can independently verify this.

If Microsoft receives a government demand for any customer's data, Microsoft will only disclose customer data when it complies with applicable laws and is legally required, and only after attempting to redirect the request to the customer. Microsoft will notify the customer and provide a copy of the demand unless legally prohibited from doing so. Invalid demands are resisted by Microsoft. All requests are explicitly reviewed by Microsoft's compliance team, who

ensure that the requests are valid, reject those that are not, and verifies that it only provides the data specified in the order.

For more information on Microsoft responding to government legal demands for customer data, go to <http://blogs.microsoft.com/on-the-issues/2013/07/16/responding-to-government-legal-demands-for-customer-data>.

To read a blog post titled “Protecting customer data from government snooping” from the office of the General Counsel and Executive Vice President, Legal & Corporate Affairs, Microsoft, go to <http://blogs.microsoft.com/blog/2013/12/04/protecting-customer-data-from-government-snooping>.

Secure Identity Management

Identity Management (IdM) is also referred to as *Identity and Access Management*, and it is important to understand in the context of security, especially in a SharePoint hybrid environment. A well-planned IdM system provides the appropriate individuals with access to the proper content and resources, at the right times, and for the right reasons.

Many attackers focus their efforts on gaining administrative privileges first and then infiltrating the network and servers “sideways.” When they are in with administrative privileges, you have lost control of your system.

Chapter 8 discusses some good practices with respect to IdM and Privileged Access Management in the section “User life cycle management.”

Privileged Access Management

Microsoft Identity Manager 2016 offers a feature called Privileged Access Management (PAM) that controls the temporary granting of administrative access via groups. If you are

concerned about the risk of either external or an insider attack with your IT workforce with privileged access, you should consider PAM. PAM requires you to configure a separate dedicated forest in which it is to reside. The domain in this forest accommodates privileged groups and accounts that are shadowed from one or more of your corporate domains.

According to TechNet, PAM was built on two core concepts:

- Control by managing a user's access, not her credentials, and use Active Directory groups to provide that access
- Extract and isolate administrative accounts from existing Active Directory forests

More info To read more about PAM's principles of operation, go to <https://technet.microsoft.com/library/mt488945.aspx>.

Securing Microsoft Identity Manager 2016 and PAM

If you are considering using Microsoft Identity Manager 2016 with PAM, you would need to ensure that you are following all guidance and

locking down service account privileges that run the Microsoft Identity Manager 2016 and PAM services to an absolute minimum. Planning and securing service accounts is important prior to the configuration of PAM. If not done, the installation will warn you that the service account is not secure in its current configuration and will not prevent you from continuing. Overlooking this security warning is dangerous.

You would need to secure the service accounts that run the REST API Application Pool, Component Service account, and Monitoring Service account. The purpose of this section is to help you address securing your Microsoft Identity Manager environment, and we recommend that you further read on topics to lock down servers and services that handle identity and user profile synchronization.

More info To read more about the planning around security for Microsoft Identity Manager 2016 service accounts and groups, go to <https://gallery.technet.microsoft.com/FIM-2010-Planning-security-4e2a7b2e>.

Relevant threats and risks

Adding more endpoints, mobile work forces, and varying requirements in collaboration comes with a price—the risks increase. You must ensure that you understand the potential risks in a hybrid environment. Fortunately, there are many risk mitigation tools and adequate planning can help minimize security incidents and avoid breaches. Cybersecurity is a huge topic and we cannot delve into too much detail in this e-book, but we will need to take you through some of the relevant threats that might confront your SharePoint hybrid environment.

Social engineering

Social engineering in security is the art of manipulating somebody by means of deception to disclose or perform an action that would divulge confidential information to the attacker. There are a number of types of social-engineering threats that exist. Your company must assess these risks and aim to establish controls such as employee training, information classification and segregation, and remote device security controls to avoid or minimize the impact of this type of threat. The following

subsections provide an overview to a couple of social-engineering techniques.

Phishing/spear phishing

This is when an attacker deceives a user via emails that appear to be genuinely asking for credentials to access a system. When the user attempts to sign in, he is in fact sending valuable personal information to the attacker's bogus site. Consider a scenario in which an attacker sends email to you users asking them to reset their Office 365 credentials because your company determined their passwords were not adequate. A remote user clicks the link in the email, which takes him to a bogus site that looks like an Office 365 site. There, the user is presented with "Old Password" and "New Password" text boxes in which he types his current password.

Note This is often considered as the top risk that you should be concerned about for your organization due to the ease and prevalence of this exploitation. A lot of phishing emails are detected and blocked in anti-spam devices that your organization might have in place. However, all it takes is a few of those emails to get past those devices, and you are at risk of this threat becoming a reality. Deploying multifactor authentication can mitigate this risk.

Pretexting

In a pretexting attack, a scammer masquerades as a genuine and trusted party, where a false circumstance is fabricated to dupe a user into providing access to secured resources; for example, a scammer pretends to be an IT support engineer (from within your company or from Microsoft) and calls users to provide technical support that requires the user to provide user credentials for troubleshooting purposes. Some scammers install remote access software on the unsuspecting user's device and then begin troubleshooting performance issues while installing key-logging software that records all of the keystrokes on the user's device. The user's key-logged information is then periodically sent to a remote server of the scammer—this includes URLs, usernames, and passwords.

Pass-the-Hash attacks

A Pass-the-Hash (PtH) attack is when an attacker captures a user or administrator's credentials by stealing the password *hash*, which is a mathematical representation of the user or administrator's password, not the plain-text password itself. An attacker can then sign in to secured resources as the user by using that

password hash. This type of attack is a growing concern for many organizations. Microsoft has mitigated this risk in the Azure Active Directory Connect (AD Connect) password synchronization security, if you are concerned about synchronizing users from on-premises to Azure Active Directory (synchronized identity model with password synchronization). From a security standpoint, on-premises passwords are never transferred to Azure Active Directory. What happens is that the password hash of users is rehashed before synchronization occurs, protecting passwords against PtH attacks; the lack of access to a local hash prevents unauthorized access to on-premises resources.

Man-in-the-middle attacks

A man-in-the-middle (MITM) attack is when an attacker secretly intercepts your communication exchanged with other parties such as websites. The attacker is able to use tools to route the communication path via the attacker's computer where the communication is decrypted and data such as credentials is stolen. A proxy server is basically an MITM where the client (your desktop or device) connects to the proxy, and the proxy connects to the server (a remote website such as SharePoint Online). The objective of an MITM attack is to intercept communications being

passed from one device to another by taking over the session. MITM attacks can also force your browser into communicating with other websites over HTTP, even though HTTPS is enforced by the webserver, this is called *SSL Stripping*. An attacker can view the entire conversation in plain text, and this is usually done unnoticed by the user. The only indication is that the URL of the site in the web browser will be `http://` instead of `https://`. Some MITM attackers can also choose to tamper with the communications between the two parties.

Conventional wiretapping is similar to an MITM attack; conversations that goes across the “wire” are sniffed (tapped). It could be data or even voice communications.

Important It is critical that end-to-end communication between on-premises servers and Office 365 are encrypted. This also applies for all your remote workforce devices, too, where encrypted communication is critical. The importance of encrypted communications is vital because OAuth tokens are transmitted between servers, and between client and server. These security tokens provide access to content and services in your network and you do not want them to be transmitted in clear text (unencrypted). If you are thinking of SSL offloading anywhere in your network—for

example, between the reverse proxy and your on-premises SharePoint server—you are exposing that segment of your network where the data is unencrypted and can be sniffed on that section of the wire.

Address Resolution Protocol poisoning

When connected to a hotel's wireless Internet connection, or a public Wi-Fi hotspot, you are considered to be a client of the local area network (LAN). When you attempt to connect to a website, for example <https://contoso.sharepoint.com>, there are a number of things your computer must do to resolve that address to find its way through the Internet and reach the sharepoint.com web server. One of the steps involves finding the *next hop* in the LAN, so a computer has an IP address that it needs to communicate with and it looks up an ARP table where IP addresses are associated with a media access control (MAC) address. This is necessary in IPv4 networks to be able to communicate with the gateway of the LAN and be routed to the Internet to its destination. Address Resolution Protocol (ARP) poisoning is also known as *ARP Spoofing* or *ARP Cache Poisoning*. It entails the attacker spoofing

or falsifying the ARP messages over a LAN, which results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network, such as the proxy server or the LAN gateway IP address. This type of attack occurs only on LANs that utilize the ARP. After the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address.

When the ARP cache has been successfully poisoned, each of the victim devices send all of their packets to the attacker when communicating to the other device. This puts the attacker in the middle of the communications path between the two victim devices (hence the term man-in-the-middle). This makes it possible for an attacker to easily monitor all communication between victim devices.

Malware

The term "malware" is a combination of the words "malicious" and "software." It covers all sorts of unwanted code that are malicious in nature and are designed to spread on a compromised system. Malware is basically unauthorized software that is on your employee's devices with which the attacker can

gain access to files or spy on computer activity. There are different types of malware, such as spyware (used for monitoring, spying activity, and key-logging activities) and ransomware (used by attackers to demand money in order for you to regain control of your system).

LAN viruses

In a hybrid environment, your organization's travelling workforce and remote users are vulnerable to viruses that propagate through Wi-Fi networks without any user action.

LAN-based viruses, or *worms*, are self-replicating, self-propagating programs that are spread through the Internet and generally don't require any action on the part of the computer owner to be activated. All they need is a vulnerable wired or Wi-Fi router, or an unprotected connection to the Internet. After the router is infected, some worms are programmed to automatically launch attacks into other Wi-Fi networks that are within its wireless range without any aid from anyone. In large cities, you would have noticed 5 to 10 wireless networks show up in your available network connections. It could be possible that a few of those routers aren't updated to the latest firmware and are thereby vulnerable to these

sorts of worms. Do you trust connecting into any of those wireless networks?

Sniffing

A packet sniffer is an application that can monitor all network traffic in a network. It can “sniff” the data passing through a network (wired or wireless) and determine the source, destination, and content of the data. Some sniffers have additional capabilities to be able to filter out the noise and capture sensitive details like credentials being sent across the network. Other sniffers have the ability to capture and reconstruct files sent or received via email, or uploaded, or downloaded across a network.

Cross-Site Scripting

Cross-Site Scripting (XSS) is malicious code injected into a benign or trusted website. A *Stored XSS Attack* is when malicious code is permanently stored on a server; a computer is compromised when requesting the stored data. A *Reflected XSS Attack* is when a person is tricked into clicking a malicious link; the injected code travels to the server and then reflects the attack back to the victim’s browser. The victim’s computer deems that the code is from a “trusted” source.

Wildcard certificate risks

We discussed the option of using a wildcard SSL certificate in [*Planning and Preparing for Microsoft SharePoint Hybrid*](#) as well as this book for your SharePoint hybrid environment. It is worth mentioning the risk that applies to both wildcard and multidomain certificates, so that you can include appropriate steps in your risk mitigation and remediation plan. By using these types of certificates, you multiply the scope of any potential issues with the certificate because there are multiple sites (including an unlimited number of subdomains) that rely on that single certificate. In the event of someone gaining hold of the private key or if the certificate expires and is not replaced in time, every site using the wildcard or multidomain certificate is affected rather than just one.

Device theft

If your organization has already adopted a “bring your own device” (BYOD) policy or is considering adopting it, you should carefully consider this risk: Device theft is a common risk that poses a great threat to organizations’ sensitive data, especially in a hybrid environment with files synchronized to the local device for offline use. To increase productivity, employees are growing

the BYOD trend by seeking flexibility in working from anywhere. A hybrid deployment with managed devices sanctioned by the organization meets that demand. When it gets BYOD, IT administrators are faced with challenges to be able to manage these mobile devices while ensuring that corporate resources are protected from unauthorized access. Using Microsoft Intune, you can deliver application and device management completely from the cloud, or on-premises through integration with System Center 2012 Configuration Manager, all via a single management console.

More info To read more about Microsoft Intune, go to <https://docs.microsoft.com/intune>.

Threat detection tools

The previous section provided an overview of some of the threats that exist. You can detect and prevent these threats in a number of ways. For most threats, except for some like social engineering, there are third-party solutions available in the form of hardware appliances, cloud-based services, and software products that you can purchase to help with threat detection. They take the form of firewalls, email gateways,

Intrusion Detection Systems (IDS's), Intrusion Prevention Systems (IPS's), and endpoint security. Some security specialist vendors have an advanced threat detection application that sniffs and detects suspicious content in your environment. We recommend that you conduct your own research and evaluation into them and determine if your organization wants to go down that path in addition to organic security controls that your IT security team designs.

Office 365 Advanced Security Management

Office 365 Advanced Security Management helps you to identify high-risk and abnormal usage as well as security incidents in your Office 365 environment. Advanced Security Management learns the user workloads and reports on everything that is of interest from a security perspective. You also can create alerts that are of interest to your organization. We discussed Advanced Security Management earlier in the chapter, so we're not going to dive into too much details here.

The Advanced Security Management site is available through the Office 365 Security & Compliance Center or by signing in directly at <https://contoso.portal.cloudappsecurity.com>.

Microsoft Advanced Threat Analytics

Recently released, Microsoft Advanced Threat Analytics is a self-learning technology that uses behavioral analysis and reports on suspicious behavior that helps identify targeted attacks on your organization. There is no need to set up complex rules at the outset. After it is installed, an intuitive attack timeline lets you see what happened and when, providing you with quick insight into what might be a threat or attack in your network.

More info To read more about Microsoft Advanced Threat Analytics, go to <https://www.microsoft.com/cloud-platform/advanced-threat-analytics>.

Risk-mitigation strategy

A few individuals understanding risks is not enough for an organization, no matter how big or small, to justify the actions and calculate implications if the threat or risk occurs. That's where creating a risk assessment and a risk-mitigation strategy is highly important for small, medium, and large enterprises alike. It is also a great process to cultivate a risk-aware culture in

your organization that will get your colleagues and teams to think about the threats, their likelihood of occurring, and the value of data theft if it were to occur. If you are a small business, you can begin by creating a simple list with the threats identified in this chapter, the likelihood of it occurring, what damage your business could sustain if there were a breach of data or your intellectual property were to get into the hands of a competitor, and your controls around it—whether they be technical, process-driven, or legal.

Microsoft has published a paper titled “Office 365 Risk Management Lifecycle,” which discusses the various phases of the risk management life cycle they undertake for Office 365. Independent verification is done on Office 365 by independent assessors to determine how control objectives are being met. This document is available in the Office 365 Trust Center.

With the right tools and controls in place, you will be able to boost your organization’s confidence by performing your due diligence when adopting a hybrid cloud model. If you are looking at gathering more information on risk principles, management frameworks, and guidelines, you can refer to International

Standards Organization's ISO 31000 at http://www.iso.org/iso/iso_31000_for_smes.pdf.

The activities that will take place as part of your risk-mitigation strategy will include the following:

- Risk identification
 - A threat and vulnerability assessment is conducted on all key control areas to identify internal and external threats.
- Risk assessment
 - After the risks are identified, they need to be categorized in terms of the following:
 - Severity: high to low
 - Likelihood: highly likely to highly unlikely
 - Impact: high to low
- Risk remediation response
 - After the risks are assessed, you would need to develop plans to address these risks either proactively or reactively. Following are the steps that you need to perform as part of the risk management:

- **Respond to the risk** Where you can, avoid, mitigate, accept, or transfer the risk
- **Monitor the risk** Perform real time monitoring, periodic reviews of audit logs, and testing.
- **Report on the risk** Send reports via email, dashboards, and metrics.
- The following table is an example of a simple list to start your risk mitigation strategy:

Risk identification	Risk assessment	Risk remediation response
For example, device theft	Highly likely	Microsoft Intune—full wipe
For example, phishing	Likely	Antivirus & Audit logs review, Quarantine procedure. Rebuild operating system on device.

Risk remediation

When it comes to planning risk remediation solutions, we can group them into three types in a SharePoint hybrid environment: You can remediate or reduce risks by deploying technical solutions in your environment, utilize Office 365 security offerings, and security investments in your organizations personnel.

Technical solutions

Technical solutions cover a variety of areas where you can use blocks, restrictions, and implement policies through a software application, or network device. This list is by no means exhaustive and is meant only to start you on your cybersecurity planning.

Restricting administrative privileges

It is a good practice that your users, both remote and within the corporate network, should not unnecessarily sign in to their devices or desktops using local administrative privileges. This safeguards against the accidental, unintentional, or automatic installation of malicious code through worms and phishing. Using features like

privileged access management in Microsoft Identity Manager 2016 sparingly grants administrative rights for a limited time period in a role-based access system.

Here is what Microsoft does for restricting administrative privileges: Office 365 engineers operate in a just-in-time access mode whereby to gain access to a portion of the network, they need to request access, which is approved based on the engineer's clearance level and authority. This is complementary to Lockbox for access to data. No engineers in any of the Office 365 teams have permanent standing access to any part of the network.

You can also consider using Privileged Access Workstations (PAWs) for administrative functions. PAWs provide a dedicated and highly protected operating system environment for administrators to conduct sensitive tasks. Microsoft IT uses PAWs (internally referred to as "secure admin workstations," or SAWs) to manage secure access to internal high-value systems within Microsoft. To read more about PAWs, go to <https://technet.microsoft.com/library/mt634654.aspx>.

Outdated systems

Devices and computers that have outdated operating system versions and builds pose a risk to a business, given that they are vulnerable due to outdated security code. Performing prompt and regular security updates is absolutely essential even if you are on the latest operating version. Because threats are constantly being discovered and are ever changing, you are advised to have an operating systems update schedule as close to the release date as possible after testing on non-live systems. This includes mobile devices that are easier targets because they aren't usually behind a corporate firewall, nor might they have their enterprise security applications installed under a BYOD strategy that your organization has adopted.

Note Newer desktop and mobile operating systems such as Windows 10 come with Windows Defender. Windows Server 2016, has Windows Defender included in the operating system, providing antivirus, antispyware, network inspection, and antimalware capabilities.

Application control policies

Microsoft uses the term "application control" to describe the approach of explicitly allowing the code that will run on a Windows host.

Application control policies can be applied across your organization's server and desktop environment. Windows Administrators can choose to control applications via group policy to lock down a certain set of application (.exe) files and processes to run on an operating system. No other processes or applications can be run without explicitly allowing it to do so. You should consider application control on especially remote users. You can also look at profiling (auditing) your own servers before you lock down anything. If you are looking for a solution from Microsoft for application control, you could read more about AppLocker for Windows at <https://technet.microsoft.com/library/hh831440.aspx> and the Enhanced Mitigation Experience Toolkit (EMET) at <https://support.microsoft.com/kb/2458544>.

Server hardening

Server hardening is the process of assessing and disabling unnecessary services, applications, and service accounts on servers under your control for the purpose of securing server access. You can also turn on the host-based firewall, restrict

remote access, restrict inbound communication from untrusted environments to servers, or even disallow certain management tools from accessing the servers except from a separate locked down “management” LAN.

Furthermore, you could look at running the Microsoft Baseline Security Analyzer to check for Windows administrative vulnerabilities; weak passwords; audit settings; local users, if any, and their policies; Windows firewall settings; Domain Controller vulnerabilities; IIS administrative vulnerabilities; SQL administrative vulnerabilities; and security updates.

Antivirus

Usually the first line of defense on a desktop device, this is often overlooked on a mobile device. Your organization should consider protecting all desktops, mobile devices, and servers by default. Windows Server 2016 and Windows 10 come with Windows Defender, which protects the server and desktop operating system. You need to also consider a third-party antivirus program for SharePoint Server 2013 and 2016 because there is built-in capabilities in SharePoint to allow for scanning documents on upload or download, or both. A SharePoint antivirus product understands content in a SharePoint content database and is very

different from a file system–level antivirus. Office 365 has antivirus detection as part of its built-in defense in-depth strategy. However, in your SharePoint server environment, you might need to assess the risks where documents uploaded into SharePoint can, of course, contain malware, and after those documents are in a SharePoint database, file system antivirus engines cannot understand or detect malware or infected files found in SharePoint content databases. An example of this is when a mobile or remote user connects to the network and synchronizes or uploads files into SharePoint before her antivirus definitions are updated, or if the antivirus has been administratively turned off and not turned on again. The best defense is to ensure that the local antivirus definitions on the client devices are up to date.

Password policy

Consider enforcing a strong password policy throughout your organization. Brute-force attacks are very common and nothing beats having a complex password in any circumstance when it comes to securing valuable organizational resources. Another thing to note is to avoid exposing your resources where an administrator with a common username such as admin or administrator can sign in to the

network. Identities that have the `isCriticalSystemObject` attribute set to `TRUE` will not synchronize to Office 365 as part of a security measure. You can create an in-cloud user with a user name `administrator@contoso.onmicrosoft.com` or `administrator@contoso.com` in your Office 365 tenancy; however, this is not recommended, so if you have to use such a name, ensure that you have a strong password.

Centralized auditing

You might want to consider collecting all your systems audit events into a centralized system such as a Security Information and Event Management (SIEM) solution for detection and analysis. Typically, a SIEM aggregates logs from heterogeneous systems across various operating systems, databases, and network equipment. Some aggregators help decipher any log data regardless of the source and log format. Consider a SIEM that can perform log forensics for which it matches conversations, correlates events across systems, and draws patterns to users to help you arrive at a conclusion for your investigation.

Asset inventory system

An asset inventory system, also sometimes referred to as a configuration management database (CMDB), is a great way for administrators to keep track of their servers, desktops, network equipment, and remote devices. Ensure that you evaluate and select an inventory system that can automatically update and integrate with your other tools like your change management and monitoring applications. From a security perspective, it will help you know all of the assets that you need to secure from within the organization and your hybrid users such as remote workers.

Office 365 Solutions

When deploying a hybrid environment, there are number of additional security measures you can use to protect against threats.

Multifactor authentication (MFA)

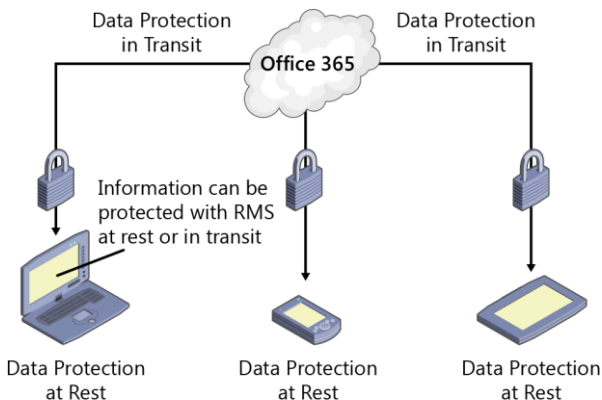
Multifactor authentication (MFA) adds another layer of security. Using MFA, a user logs in with a verification code sent via text or a call to your preregistered mobile phone, or through email.

Microsoft Identity Manager 2016 has a self-service password reset functionality that can use Azure's multi-factor authentication capabilities.

More info To read more about multifactor authentication, go to <https://azure.microsoft.com/documentation/articles/multi-factor-authentication-get-started-cloud>.

Azure RMS

Azure RMS was discussed earlier, but we mention again here as part of a risk remediation solution to mitigate against threats such as MITM attacks, data theft, and unintentional violations of organizational sharing policies. At the same time, any unwarranted access of data in transit or at rest by an unauthorized user who does not have appropriate permissions is prevented via Azure RMS policies that govern that data. Figure 9-6 illustrates devices such as laptops, mobile, and tablets with their data protected at rest and in transit.



You can apply RMS to any file type by using the RMS app

Figure 9-6: Azure RMS providing encryption for data in transit and at rest.

Office 365 OME

Built on Azure RMS, Office 365 OME makes it possible for you to send encrypted messages to people inside or outside your organization, regardless of their email system. Message encryption protects against MITM attacks. To read more, go to <https://technet.microsoft.com/library/mt661609.aspx>.

Remote device management

To remediate against device theft, you can consider Microsoft Intune for remote device management. Intune is the "management arm" of the Microsoft Enterprise Mobility Suite (EMS)—a cost effective way to acquire other cloud services such as Azure Active Directory Premium, Azure RMS, along with Intune.

With Intune, you are able to secure your own devices as well as your employees' devices if your organization has adopted a BYOD strategy.

Some of the primary tools that Intune offers include:

- **Mobile device management (MDM)** This gives you the ability to enroll devices into Intune so that you can provision, configure, monitor, and take actions on those devices such as wiping them.
- **Mobile application management (MAM)** Using MAM, you can publish, push, configure, secure, monitor, and update mobile apps for your users.
- **Mobile application security** As a part of managing mobile apps, Intune provides the ability to help secure mobile data by isolating personal data from corporate data

and allowing the corporate data to be selectively wiped.

More info To evaluate Microsoft Intune, go to <https://docs.microsoft.com/intune/understand-explore/get-started-with-a-30-day-trial-of-microsoft-intune>.

Personnel solutions

An important piece of safeguarding your organization's resources is the workforce. From mobile workers, to IT workers, to executives, securing corporate data is everyone's responsibility. We will now look at a few ways you can plan to create awareness and have the necessary controls in place.

Workforce training

The general workforce needs to be aware of the risks associated with cybersecurity in every organization. When collaborating with other business partners in a hybrid environment, there is increased exposure and users are required to be able to distinguish between attachments and email from a legitimate source and something from a scammer. User education is important on the basis of Internet threats to prevent phishing and social-engineering threats.

Note Consider this scenario: If nine of your staff identify a phishing attack but one of them falls victim, the organization is still compromised. Training your workforce to report phishing attacks can help mitigate the impact of the single employee who fell prey to the phishing attack.

You must also teach users to avoid weak passwords if a technical solution isn't yet in place. Reusing passwords is also not recommended. Consider creating an internal security training session and post it on your intranet so that it can be reused or you can use it in your training videos for new staff.

Security screening employees and contractors

Sensitive environments dealing with classified data, such as the government, usually require screening employees and contractors before they can be given access to work on systems with classified information. Police checks are conducted and detailed personal information of the employee or contractor is checked and vetted by an authorized body. It is also common for organizations to consider scanning identity documents such as passports, and driver licenses of their employees to store for security purposes.

Creating a defense-in-depth system

Consider investing in building a defense-in-depth system for which you have security controls at the various levels of the defense system. An example of Office 365's defense-in-depth system was discussed earlier in this chapter. Your plan does not need to be enterprise grade, but a simplified model can go a long way in your journey toward having secure controls over your organization.

In the United States, there is the Cybersecurity Framework—a voluntary framework developed by the National Institute of Standards and Technology (NIST) and other stakeholders based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructure. The framework provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. You can use it to help identify and prioritize actions for reducing cybersecurity risk, and for aligning policy, business, and technological approaches to managing that risk.

Organizations can use the Cybersecurity Framework to determine gaps in their current cybersecurity risk approach and develop a roadmap to improvement. Organizations can determine activities that are most important to

critical service delivery and prioritize expenditures. To read more about the Cybersecurity Framework by NIST, go to <http://www.nist.gov/cyberframework>.

SSL security

TLS and its predecessor, SSL, are cryptographic protocols that provide communications security over a computer network.

The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating computer applications. Connection encryption is a mechanism for securing in-transit data as it is being transferred between SharePoint and other computers in your enterprise. In previous versions of SharePoint, you could use either SSL 3.0 or TLS 1.0 cryptographic protocols for secure communications; however, SSL 3.0 was later found to have vulnerabilities, making TLS 1.0 the remaining protocol available for use (SSL 3.0 could be disabled).

SharePoint 2016 now handles encryption by default using the newer TLS 1.2 cryptographic protocol for secured connections.

Note SSL and TLS protocols are both commonly referred to as SSL in documentation, sometimes even being grouped together as SSL/TLS. Remember that when we speak of implementing SSL in this book, we mean the TLS 1.1 or 1.2 protocols, not SSL 3.0.

Self-signed certificate security

An SSL certificate has two pertinent functions: encryption of traffic and verification of trust. Whether using a publically signed SSL certificate or a self-signed certificate, you get the benefit of encrypting the data conversation between the webserver and the client. Traffic is sent over an SSL or HTTPS connection regardless of whether the certificate is self-signed or signed by a public Certificate Authority (CA). It is the verification of trust that presents a problem with using a self-signed certificate.

When a client desktop or device browses to a website that has a self-signed certificate, the Internet browser displays a warning that there is a problem with the website's security certificate. The danger of using a self-signed certificate is when users become immune to these warnings messages generated in the browser, leading to dangerous public browsing behavior. A user might continue the behavior of ignoring SSL

warnings or simply trusting any SSL certificate presented to him without checking. It could perhaps be a fake SSL certificate one day, which just might be part of an MITM attack. Or even worse is a phishing email pointing to a fake site with a fake SSL certificate designed to gather Office 365 credentials. Another point to note is that self-signed SSL certificates cannot be revoked as in the case of a public CA issued SSL certificate, because the user's desktop or device has no relationship with the trusted root certification authority of the issuing server.

Client preauthentication certificate security

In Chapter 1 of this book, we configured the server-to-server (S2S) trust with Azure ACS. Recollect that there was a certificate called the client preauthentication certificate that is used by the reverse proxy to authenticate inbound calls from Office 365 to SharePoint on-premises. The authentication takes place when the inbound Office 365 call presents the client certificate that is stored in the Secure Store Service online in Office 365 to the reverse proxy in response to the authentication challenge.

Chapter 8 points out how Microsoft recommends that you use a unique-purpose

certificate for this role to limit the potential for a security breach. The client preauthentication certificate must be signed by a well-known public certificate authority so that Office 365 can validate the trust chain. Using a dedicated certificate means that it will never be accessible to the public, giving you added security.

If a wildcard certificate was used, or another certificate was reused for client preauthentication, the attack surface will increase. If an attacker acquires the private keys of the shared certificate, the attacker can access multiple endpoints in one hit, including the client preauthentication in the S2S trust. It is recommended to use a 2,048-bit length key encryption because this is extremely strong and would require a lot of time to crack using a connected desktop. This is the reason why 1,024-bit length key encryption is being phased out in general.

Furthermore, the client preauthentication certificate is safely stored in the Secure Store Service online in an encrypted database that an attacker cannot extract the certificate from.

Additional security reading resources

To read more about Office 365 mapping of CSA Security, Compliance, and Privacy Cloud Control Matrix requirements, go to

<https://www.microsoft.com/download/details.aspx?id=26647>.

To read more about security in Office 365, download the Security in Office 365 White Paper at

<https://www.microsoft.com/download/details.aspx?id=26552>.

To read more about the Best Practices for Securing Active Directory, go to

<https://technet.microsoft.com/library/dn487446.aspx>.

Test virus - EICAR is a 68-byte .com file detected as "EICAR-Test-File". Be aware that this *is not* a real virus. The test file simply displays a text message and returns the control to the operating system. To perform a test with the EICAR test virus, go to

<http://support.kaspersky.com/viruses/general/459>.

For more information about Microsoft's compliance with popular standards and certifications, see Regulatory Compliance, go to <http://go.microsoft.com/fwlink/p/?LinkID=270210>.

To read more about developing a city strategy for Cybersecurity, go to <http://download.microsoft.com/download/1/B/3/1B3C6BE3-8FA4-40BD-9BD6-640FD2F1F648/City%20Strategy%20for%20Cybersecurity.pdf>.

To read more about a framework for cybersecurity information sharing and risk reduction, go to [http://download.microsoft.com/download/8/0/1/801358EC-2A0A-4675-A2E7-96C2E7B93E73/Framework for Cybersecurity Info Sharing.pdf](http://download.microsoft.com/download/8/0/1/801358EC-2A0A-4675-A2E7-96C2E7B93E73/Framework%20for%20Cybersecurity%20Info%20Sharing.pdf).

About the Authors



Jeremy Taylor is a SharePoint technical specialist based in Canberra, Australia, who has more than 11 years' experience in designing, building and supporting SharePoint farms across the Australian Federal Government, large

enterprises, and small- to medium-sized businesses. Jeremy's skillset is a unique blend of IT and business management. He holds a Bachelor of Business Administration (BBA) degree and Master of International Business (MIB) degree from Macquarie University, Australia, as well as a number of IT certifications since 1999.

Jeremy has a solid infrastructure background in systems administration, architecture, and network infrastructure experience, primarily with Microsoft and Cisco. He is a Microsoft Certified Trainer, Microsoft Certified Solutions Expert in SharePoint, and draws on the depth of his SharePoint, Office 365, and Azure learning at the

Microsoft Certified Solutions Master (MCSM) SharePoint training in Microsoft's Redmond, Washington, facilities.

Jeremy has authored his own SharePoint training courseware for LearnHaus (www.learnhaus.com), an IT training company. He also blogs about SharePoint Administrator-related topics at www.jeremytaylor.net and he is a co-organizer of the Canberra SharePoint User Group. Jeremy spends his free time with his wife, Sylvia, two daughters, Nasia and Amarissa, and still finds time to learn new technologies.

You can contact Jeremy at jeremy@jeremytaylor.net, <http://www.linkedin.com/in/jeremyptaylor>, or follow him on Twitter @jeremytaylor.



Neil Hodgkinson (PhD, MCSM: SharePoint) is a senior program manager in the CXP, CAT team within the Applications and Services Group at Microsoft. Starting his IT career as a SQL and ASP developer almost 18 years ago, Neil naturally

transitioned to SharePoint technologies back in 2000 when Microsoft launched SharePoint Team

Services. He then worked for a global outsourcer as a SharePoint consultant and engineer before joining the PFE organization at Microsoft in 2005. From 2005 onward, as PFE expanded, Neil was the technology lead for SharePoint in EMEA and helped recruit a number of top-class engineers, many of whom are still with Microsoft today. After five years in PFE, Neil spent three years in the Office 365 escalation team as the EMEA lead, during which time he helped transition Business Productivity Online Services (BPOS)-S and BPOS-D off the SharePoint 2007 platform and onto SharePoint 2010, and then eventually to SharePoint 2013 and Office 365.

Neil's passion for customer satisfaction has been a fixture throughout all his roles at Microsoft, and in his current role, he is still heavily engaged in the Office 365 service, helping with customer escalations and acting in an advisory capacity for field teams engaged in customer projects, especially in the areas of hybrid, disaster recovery, search, and Azure. Neil was content owner and instructor for Search, SQL Operations, and Business Continuity Management for MCM and MCSM, delivering this training on multiple rotations.

Neil hails from Manchester, England, and outside of work he is a fan of classic rock music and

modern heavy-metal bands. He also plays Association Football and is an active member of his local karate dojo. He is an annual Tough Mudder runner and enjoys the camaraderie of the mudder nation. Most of all, he enjoys making the most of time at home with his wife of 13 years, Julie, and their three children, Luke, Cerys, and James, having fun and living life.



Manas Biswas is an Office 365 service engineer with more than 12 years' experience in the industry. Manas has worked with SharePoint and related technologies extensively. In 2005, he joined Microsoft and then later became a member of

SharePoint Escalation Services, where his primary area of focus was SharePoint Technologies, assisting customers with technical analysis, deployment, and problem solving. As progress in cloud strategies at Microsoft developed, Manas shifted his attention to Office 365 and Azure, specializing in beta testing and product releases. Eventually he trained his concentration on hybrid infrastructure, deployment, and readiness. Most recently, training, content creation, and readiness

for SharePoint and its cloud workloads have been his key areas of expertise.

Currently Manas is a member of the Office 365 Service Engineering team, focused on search and hybrid configurations. He speaks frequently at technical sessions in conferences like SharePoint Conference, Ignite, MVP Open days, and many Microsoft internal conferences. In addition, Manas is a regular contributor to TechNet and MSDN forums and blogs about Hybrid features at <https://blogs.technet.microsoft.com/beyondsharepoint>.

Manas is based in India. When not working on SharePoint, he is busy either playing Xbox with his son, Manab, or travelling around with his parents as well as his wife, Sabita, enjoying different cultures and experiences.



From technical overviews to drilldowns on special topics, get free ebooks from Microsoft Press at:

www.microsoftvirtualacademy.com/ebooks

Download your free ebooks in three formats:

- PDF
- EPUB
- Mobi for Kindle

Look for other great resources at Microsoft Virtual Academy, where you can learn new skills and help advance your career with free Microsoft training delivered by experts.

Microsoft Press