Microsoft

Planning and Preparing for Microsoft SharePoint Hybrid



Jeremy Taylor

www.dbooks.org

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: 978-1-5093-0242-0

First Printing

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 Reviewer: Neil Hodgkinson; 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



Microsoft

www.dbooks.org

Contents

Foreword ..... **vi**
Introduction ..... **vii**
Acknowledgments vii
Free ebooks from Microsoft Press viii
Errata, updates, & book support viii
We want to hear from you viii
Stay in touch viii
Chapter 1: Microsoft cloud overview **1**
Microsoft cloud services background 1
Office 365 1
Microsoft Azure 2
Why hybrid? 3
What is SharePoint hybrid? 3
The importance of hybrid in digital transformation 4
Overview of SharePoint hybrid capabilities 4
Cloud hybrid search 4
Hybrid sites features 4
Why Microsoft? 5

Security ... 6
Transparency ... 6
Money-back-guaranteed enterprise-grade Service Level Agreements ... 7
Chapter 2: Azure and Office 365 for SharePoint hybrid ... 8
Microsoft cloud services ... 8
Azure Active Directory ... 9
Azure AD Domain Services ... 9
Azure AD Join ... 10
Identity models ... 11
How does Office 365 and Azure work? ... 13
Choosing the right Office 365 plan ... 14
FastTrack for Office 365 ... 14
Getting started ... 14
Configuring hybrid overview ... 15
Chapter 3: Architecture, authentication, and authorization ... 17
Architecture topologies ... 17
Hybrid HA planning ... 18
Azure AD Connect HA ... 19
SSO considerations ... 19
ExpressRoute planning ... 20
Scenarios for SharePoint on-premises and Azure with ExpressRoute ... 21
Azure Site Recovery ... 21
Standby farms ... 22
Planning for multiforest directory scenarios ... 22
Hybrid network ports and protocols overview ... 23
Identity models in SharePoint hybrid (user authentication) ... 23
The federation authentication process ... 23
Open Authorization and server-to-server authentication ... 25
Azure ACS ... 26
S2S authentication trust between SharePoint and SharePoint Online ... 26
What is identity management? ... 28
Planning source of authority ... 29
Authorization: planning access ... 29
Plan SharePoint Online access ... 30
Plan for users outside the organization to access resources ... 32
Plan for administrators ... 33
Chapter 4: Platform hygiene preparation ... 34
Planning requirements and functionality ... 34

www.dbooks.org

Environment preparation ... 35
Office 365 readiness checks ... 35
User identities and directory preparation ... 36
Active Directory schema ... 37
External domain name ... 37
Internal domain name ... 39
Multiforest environments ... 40
Name resolution (DNS) ... 40
SSL certificates ... 42
Server requirements ... 43
Network requirements ... 46
Client application preparation ... 48
SharePoint on-premises requirements ... 49
IdFix DirSync Error Remediation Tool ... 49
Supported operating system ... 50
Operating the IdFix tool ... 51
Directory auditing ... 52
Capacity planning ... 53
Chapter 5: Synchronizing users to the cloud ... 54
Directory synchronization ... 54
Azure Active Directory Sync ... 55
Azure AD Sync ... 55
Azure AD Connect ... 55
MIM 2016 ... 56
Azure AD Connect preparation ... 56
Domain verification ... 56
Cloud user ID verification ... 57
IdFix cleanup ... 57
Activate Directory synchronization ... 57
Password write-back ... 59
Azure AD Connect configuration ... 60
Verification ... 67
Troubleshooting synchronization issues ... 69
Managing directory synchronization ... 71
Starting and stopping synchronization ... 72
Managing Azure AD by using Windows PowerShell ... 72
Chapter 6: SharePoint hybrid single sign-on ... 74
SSO ... 74

AD FS ... 75
Web Application Proxy ... 76
Configuration steps of AD FS ... 76
Working with subdomains ... 77
Secure Sockets Layer Certificates ... 77
DNS settings ... 79
Configuring AD FS ... 79
Azure AD Connect ... 80
The Active Directory Federation Services Configuration wizard ... 84
Installing AD FS by using Windows PowerShell ... 85
The Web Application Proxy Configuration Wizard ... 86
Configuring Web Application Proxy by using Windows PowerShell ... 87
High availability ... 87
Verification ... 87
Windows service startup checklist ... 88
AD FS verification ... 88
Web Application Proxy verification ... 89
SSO verification ... 89
Verify SharePoint online SSO ... 90
Verify settings by using Azure AD Connect ... 91
Validate your AD FS configuration ... 92
Troubleshooting SSO issues ... 94
Azure AD Connect Health ... 98
About the author ... 100

www.dbooks.org

Foreword

Whether you're looking to the cloud as your future, long-term run state or simply want to bring cloud innovation to your datacenter, proper planning and preparation are paramount to your success. *Planning and Preparing for Microsoft SharePoint Hybrid* provides the background and information you need to get started in this new reality.

As both technology and connectivity continue to advance at an exponential rate, the world is becoming a giant network and people are becoming more hyperconnected, whether through consumer technologies we're already familiar with, such as Facebook and Twitter, or commercial experiences such as Microsoft Office 365. This connectivity means information is created and travels faster than ever, making it possible for us to accomplish more, in an increasingly collaborative way.

The new "currency" of information has led to an explosion of data, and in today's economy, saving money and gaining efficiencies remain important goals for organizations of all sorts. Enterprises are engaged in the continuous search for leading-edge solutions and ways to drive innovation, grow their businesses, and support changing user expectations as new employees enter the workforce.

Whether it's the proliferation of devices making the workforce more mobile or the expectation that technology helps us to create more intelligent social connections, the cloud provides boundless potential for scalable, always-available services. Along with this exponential growth in information comes a need to derive more insights from data and more connectivity to that data.

In response to these expectations, cloud services like SharePoint Online in Office 365 provide an attractive alternative to on-premises business solutions; however, for a variety of reasons, organizations might want or need to deploy specific solutions in the cloud while still maintaining their on-premises SharePoint environment. These reasons can span a broad gamut: corporate and/or regulatory compliance, data sovereignty or sensitivity concerns, or even a significant investment in customization.

On the other hand, some organizations might want to gradually move their existing on-premises SharePoint services to the cloud, using a staged migration in which on-premises SharePoint workloads are moved to SharePoint Online one at a time. Hybrid functionality balances these needs and makes it possible for an organization to maximize ROI and extend its on-premises investments to the cloud by integrating services such as people and content discovery, data connectivity, compliance, and more that empower users implement greater business mobility.

For IT, hybrid provides the foundation for the transformation from systems administrators to value-added service brokers, balancing the needs for compliance and security with those of their users, while providing powerful capabilities and solutions through technology such as Microsoft Azure AD Connect, Microsoft Identity Manager, and familiar scripting scenarios with Windows PowerShell.

This e-book helps IT, end-to-end, with best practices to move toward a common goal shared by so many organizations today—to be cloud-ready and future proof.

Bill Baer, senior product manager (SharePoint), Microsoft

Introduction

Microsoft SharePoint hybrid deployments are rapidly becoming popular with Microsoft's investments on increased SharePoint productivity, not only in your own environment (on-premises) but also collaborating in new ways through the largest and most advanced cloud service platform in the world—Microsoft Office 365 and Microsoft Azure. SharePoint hybrid is about connecting SharePoint on-premises to Office 365 and Azure to extend capabilities, enhance collaboration, and drive innovation forward.

This book is part of a series to provide readers from all over the world with a guide on how to connect SharePoint on-premises to Microsoft's cloud services. You will gain insight into planning, architecture, configuration, and management of SharePoint hybrid. This book covers foundational topics with which you will learn more about Office 365 and Microsoft Azure, architecture planning, platform hygiene and preparation, directory synchronization, and how to configure a seamless single sign-on experience for users.

Microsoft has undergone various compliance and regulatory certifications to meet a broad set of international, government, and industry-specific standards. This will continue to accelerate the adoption of SharePoint hybrid in the coming years as markets become more familiar with the business benefits and service offerings.

Acknowledgments

Thanks to my wife, Sylvia, who has endured the long nights, weekends, and taking care of the children while I was writing this book. Words cannot express how thankful I am for your love and support during this time. Thanks also to my daughters, Nasia and Amarissa, for being so patient with me, foregoing their play time with daddy so that he could write his "SharePoint book." Thanks to my parents, Sam and Dawn Taylor, who gave me the opportunity to freely work with laptops, desktops, networking, and website design during my teenage years, giving me a solid understanding of core skills in IT.

This book would have not been possible without Rosemary Caperton from Microsoft Press. Thank you for making the process an awesome experience for me and for the invaluable feedback that has helped me throughout the book. Many thanks to everyone at Microsoft Press who worked so hard to make this book a reality. To my editors, Bob Russell and Dianne Russell from Octal Publishing, Inc., thank you for your contributions and support throughout this book.

A big thanks to Neil Hodgkinson from Microsoft, who in addition to being the fantastic technical reviewer for this book has also been a great mentor for all things SharePoint hybrid. Your support has been invaluable throughout this book.

Finally, 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.

www.dbooks.org

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/planningsharepointhybrid/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.

CHAPTER 1

Microsoft cloud overview

This chapter provides a background on Microsoft's cloud service offerings—specifically, Microsoft Office 365 and Microsoft Azure—and how Microsoft has positioned itself as a leading technology supplier for businesses globally. It introduces the concept of the hybrid cloud with specific focus on Microsoft SharePoint. SharePoint hybrid offers new and efficient ways of working. It highlights the importance of SharePoint hybrid in the roadmaps of digital transformation in businesses.

Microsoft cloud services background

Microsoft's Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) offerings have grown to be a leading cloud service for millions of businesses worldwide. New capabilities and improvements are added to Office 365 and Microsoft Azure at a rapid pace based on market requirements and direction. SharePoint leads the way as a productivity tool that millions of businesses, nonprofit organizations, educational institutions, and governments around the world use for collaboration. SharePoint Server 2016, a cloud-ready version, increases productivity to another level, and now you can achieve this remarkable productivity by implementing a SharePoint hybrid deployment. It is important to highlight the experience and maturity that Microsoft brings to the SharePoint hybrid platform.

Office 365

Office 365 is Microsoft's SaaS offering. It was launched on June 28, 2011 and was a successor to the Microsoft Business Productivity Online Suite (MSBPOS), which was consumed by small, medium, and large enterprise customers. Office 365 has become the favorite cloud platform due to its secure and advanced integration services to organizations.

Office 365 has positioned Microsoft as an experienced cloud service provider with datacenters located around the globe and millions of customers worldwide.

www.dbooks.org

Using Office 365, you can consume ready-to-use applications hosted on the high-performing and secure Microsoft infrastructure. Office 365, through its subscription plans, offers Office desktop client software that provides value and increases productivity to users. With Office 365, you can effortlessly work from any office, in almost any country or region, with nearly any mainstream device. You also have the option to collaborate and communicate in real time online through its SharePoint, Exchange, and Skype for Business services. Your productivity is maximized when you can work offline and then seamlessly synchronize your work when you go back online.

Capabilities in Office 365 are being released at a rapid rate, giving you access to the newest innovations online to stay ahead, without the increased costs associated with maintaining your own IT development workforce. With the recently launched Office 2016 suite of applications, organizations have access to the most comprehensive productivity suite of cloud services and collaboration tools ever.

As with any SaaS offering, customers are not burdened with capital outlays or ongoing operational costs, because they do not need to worry about installing their own server infrastructure, networking, or customized applications. Instead, they subscribe to a flexible Office 365 SaaS offering and scale it as their business needs grow.

Microsoft Azure

In early 2010, Microsoft launched Windows Azure, which was renamed Microsoft Azure in early 2014. Azure provides customers with enterprise-grade Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offerings, unlike any other cloud service provider.

IaaS makes it possible for your business to extend its datacenter into the cloud and affords greater control over the management of the server infrastructure hosted in Azure datacenters.

PaaS gives you and your development teams the ability to consume premade templates offered on Azure. Azure offers a comprehensive virtual networking service, application-ready server platforms, and user directory services.

You have the option of uploading your own virtual machine (VM) images created on-premises or you can select from a growing range of preconfigured VM templates from within Azure. Having pre-configured server and application tiers allows for rapid deployment of highly scalable infrastructure while simultaneously cutting provisioning costs.

> **More info** According to the Gartner report "Magic Quadrant for Cloud Infrastructure as a Service," Microsoft is the only vendor positioned as a Leader across both Application Platform as a Service and Cloud Storage Services for the second consecutive year. To read the full report, go to https://azure.microsoft.com/blog/microsoft-the-only-vendor-named-a-leader-in-gartner-magic-quadrants-for-iaas-application-paas-cloud-storage-and-hybrid.

If your organization has a skilled group of developers, they'll be happy to know that Azure supports the most comprehensive selection of programming languages, frameworks, databases, and tools. This means that your developers can build Azure-hosted personalized applications in environments they're familiar with: JavaScript, Python, .NET, PHP, Java, and Node.js.

With Azure, you can build and host mobile apps for Windows, iOS, and Android devices. Server operating systems can be Windows or even Linux—this provides your customers with flexibility and freedom of choice. Because Azure offers a powerful, automated self-service platform, businesses can scale applications to any size automatically and provision the required resources in minutes.

Why hybrid?

Unlike some cloud providers that make you choose between your datacenter or their cloud service, Office 365 and Azure accommodate "hybrid" integration of cloud services with your existing IT environment. This means that you can keep existing business infrastructure server assets in place, avoiding the need to move or migrate to the cloud at the onset.

With hybrid cloud solutions, your business reaps the benefits from the best of both worlds—more leading-edge productivity options in the cloud, all while still maintaining control over existing business applications served on-premises.

With Office 365, your business or organization can take advantage of a hybrid model to securely collaborate and operate beyond the boundaries of the traditional corporate network. Using SharePoint Online, you can enhance your existing SharePoint on-premises investments with cloud-capable services.

With Azure, implementing a hybrid model means decreased time-to-market for your business solutions thanks to the rapid provisioning of underlying server platforms to support those solutions.

What is SharePoint hybrid?

SharePoint hybrid is like an extended service topology that spans your on-premises SharePoint farm and integrated Office 365 collaboration capabilities such as SharePoint Online, Yammer, and One Drive for Business. You can extend your datacenter into Azure to host servers and custom applications. Because Office 365 does not allow custom applications to be installed on it, Azure is available from an IaaS and PaaS tier to host those applications.

SharePoint Online offers real-time document collaboration authoring in the cloud, SharePoint site hosting, records management, interfacing data from a remote source, and user profile management.

IT professionals familiar with SharePoint on-premises will appreciate the cloud-integration investments that Microsoft has made for SharePoint Server 2016. New customers will realize the benefits of a hybrid cloud–ready SharePoint Server 2016 platform, whose on-premises cousin has for years been among the most popular productivity tools for users around the world.

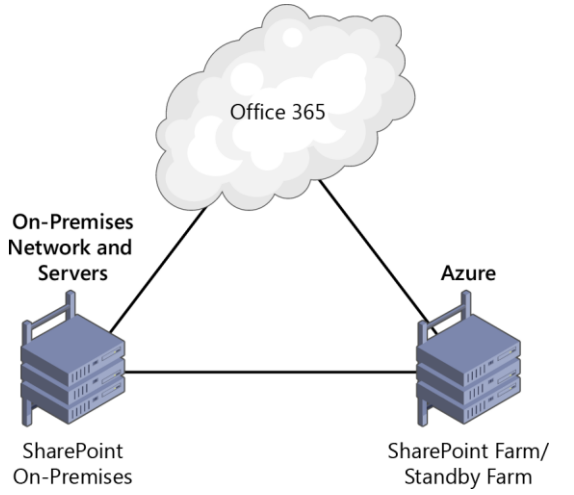


Figure 1-1: A SharePoint hybrid environment with Azure as an optional extended datacenter hosting a standby farm.

www.dbooks.org

The importance of hybrid in digital transformation

For some organizations, the hybrid approach might be the first step in exploring cloud functionality at their own pace. For other organizations that are making the transition to the cloud, a hybrid environment can serve as an interim step to the end state, offering a gradual, controlled migration. Other organizations might prefer a hybrid environment as the end state, a perpetual topology to cater to the dynamically changing business and user collaboration workloads.

New customers considering SharePoint Server 2016 can be assured that major investments have been made with cloud-inspired, feature-rich capabilities and a trusted platform.

Businesses benefit from higher performance that comes as a result of the localized presence of Azure datacenters, with Azure generally available in 22 regions around the world.

Some organizations such as government and financial institutions might have regulatory requirements for localized data locations. Microsoft has worked hard to satisfy these requirements and provide an easy-to-consume Trust Service Portal that has a number of reports and compliance documents based on region or industry.

More info To learn more about Azure services by region, go to https://azure.microsoft.com/regions/#services.

Overview of SharePoint hybrid capabilities

SharePoint hybrid capabilities provide feature-rich collaboration tools that are robust, scalable, and consumable from almost any country or region. These capabilities are aimed at extending on-premises SharePoint with new business productivity tools, and at a low cost compared to implementing them on-premises.

Cloud hybrid search

The new Cloud Search Service Application in SharePoint Server 2016 and 2013 gives you the ability to search content from both on-premises and the cloud in a single search center. A low-maintenance cloud hybrid search aggregates content from both sources and combines results in a single search index in Office 365. You can search the cloud index from either location.

Hybrid sites features

There are a number of new capabilities that are available to organizations considering a SharePoint hybrid deployment. The following sections list the features and summarize their capabilities.

Hybrid profiles

In hybrid profiles, the user profiles exist both on-premises and in Office 365. Hybrid profiles, by default, redirect users to their profiles in Office 365, providing a single place for their profile information. Depending on the Office 365 subscription, profiles might be integrated with Delve.

OneDrive for Business

You can work with files on-premises and in the cloud with OneDrive for Business. This introduces new ways of working with files in OneDrive for Business that are easy to share without you worrying about losing documents as they are hosted and backed up for you. A powerful OneDrive for Business synchronization engine gives users the ability to synchronize offline copies to all major devices available.

Site following

Followed sites from both locations (on-premises and cloud) are consolidated in the SharePoint Online followed sites list. SharePoint Server hyperlinks to the followed sites list and redirects users to the SharePoint Online followed sites list.

Extensible app launcher

The extensible SharePoint Server 2016 app launcher includes several new Office 365 tiles, making it easy for users to get to their Office 365 apps and services.

Hybrid extranet/advanced sharing functionality

Your business can collaborate with partners, taking advantage of reduced complexity and configuration than would otherwise be required with other collaboration tools and methods. With a SharePoint hybrid extranet, partners can connect directly to a members-only site in Office 365, without access to your on-premises environment or any other Office 365 site. You and your partners can access Office 365 extranet sites from anywhere.

Hybrid Business connectivity services

SharePoint Online users can now read and write data against on-premises line-of-business systems, non-Microsoft data repositories, or .NET applications via an on-premises SharePoint farm. You can also present data in SQL Azure databases through hybrid Business Connectivity Services (BCS) connections.

Duet Enterprise Online

Duet Enterprise was jointly developed by Microsoft and SAP. It facilitates interoperability between SAP applications and SharePoint on-premises Enterprise edition. Duet Enterprise Online gives business users the means to read or write SAP processes and information against an on-premises SAP system.

Why Microsoft?

Microsoft is a leading cloud services provider, backed by decades of experience. Customers have the choice to get the first preview of the latest sophisticated (yet simple to consume) features based on its self-service portals. With Office 365 and Azure, the commitments that Microsoft has made with respect to security, privacy, and compliance are second to none. The data that customers create or upload on Office 365 is theirs to own and control. Security, migration, and reverse migration are important considerations for organizations considering moving to cloud and hybrid services, and Microsoft is there to provide the highest levels of support

More info Microsoft provides lists of issues you should consider when evaluating the security and trustworthiness of Microsoft cloud services as you carry out your due-diligence. To access this information, go to https://products.office.com/business/office-365-trust-center-top-10-trust-tenets-cloud-security-and-privacy.

www.dbooks.org

Security

If you're an existing customer, you can consume a new service in preview to help you understand the extent to which you have adhered to Microsoft's security best practices and behaviors. To learn more, go to https://o365securescore.azurewebsites.net.

You can learn how Microsoft addresses compliance, cyber-security threats, disaster recovery, auditing, and the layers of security and controls from this Office 365 security white paper, available at https://go.microsoft.com/fwlink/p/?LinkId=401240.

For the latest information on Office 365 security and compliance, visit the Office 365 Trust Center and the Office 365 Service Trust Portal (available to evaluation and paid customers).

Transparency

Unlike many other cloud service providers, Microsoft has published its compliance reports and trust documents in an easy to consume manner that you can sort by country/region and/or industry.

Microsoft Cloud Service Trust Portal

The Microsoft Cloud Service Trust Portal provides you with access to information on how the company maintains security, privacy, and compliance specific to your industry and/or region. You can gain insights into security, compliance, and risks around Microsoft's service delivery operations. Perform your risk assurance by using Compliance Reports as well as Trust Documents in the Microsoft Cloud Service Trust Portal. Audit reports across Microsoft cloud services—Azure and Dynamics CRM, along with Office 365, are now being delivered by the Service Trust Portal.

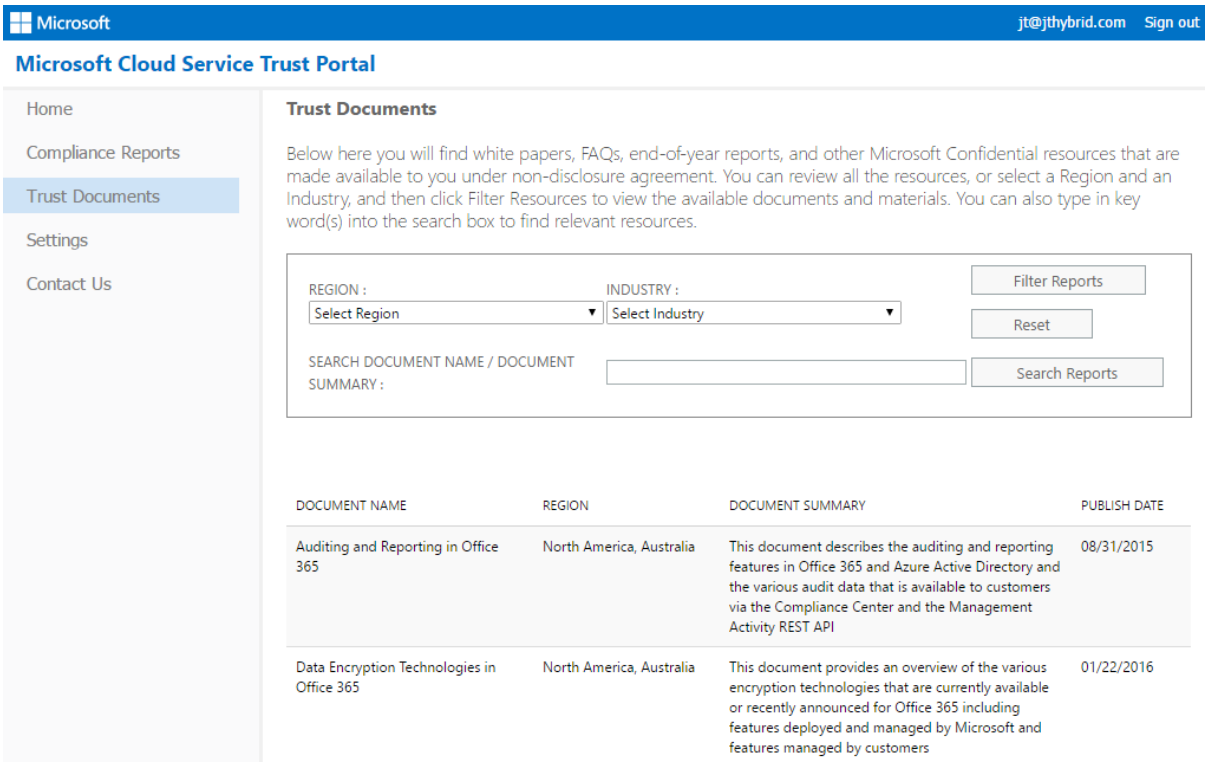


Figure 1-2: The Microsoft Cloud Service Trust Portal contains compliance reports and documents based on region and industry. The portal is only available to trial and paid customers. Viewing government documents requires prior approval from Microsoft.

Money-back-guaranteed enterprise-grade Service Level Agreements

Microsoft offers money-back-guaranteed enterprise-grade Service Level Agreements (SLAs) that set it apart from other cloud service providers. It gives customers the assurance that their data will be available when they need it.

Office 365 SLAs

The SLA for Office 365 is 99.9%. This SLA is financially backed by Microsoft in the form of service credits if there is an unscheduled service downtime lasting more than a certain period of time. For more details, go to https://technet.microsoft.com/library/office-365-service-level-agreement.aspx.

Azure SLAs

You can learn about Microsoft's financially backed SLAs specific to Azure at https://azure.microsoft.com/support/legal/sla/.

For the details regarding SLAs for Microsoft Online Services, including uptime calculators and service outage financial reimbursements for each online service, go to http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37.

www.dbooks.org

CHAPTER 2

Azure and Office 365 for SharePoint hybrid

This chapter expands on the features and capabilities of Microsoft Office 365 and Microsoft Azure with the emphasis on Microsoft SharePoint hybrid. It serves as a guide to help organizations get started with their SharePoint hybrid planning. Topics covered include Azure Active Directory, the hybrid models, supported SharePoint scenarios and subscription plan options. This chapter also provides an overview of the steps to configure a hybrid environment for SharePoint.

Microsoft cloud services

Microsoft offers a range of cloud services across the different tiers—Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)—with Office 365 as its SaaS brand, and Azure as its IaaS and PaaS brand. These cloud service offerings are available for consumption via a monthly billed subscription model. Offerings consist of multiple plans, each plan offering a combination of different services such as SharePoint, Microsoft Exchange, Microsoft OneDrive for Business, Skype for Business, as well as different tiers of storage and resource availability and licensed user limits. Flexible subscription models provide customers with the ability to mix and match a variety of services that are designed to suit their particular needs. The important thing is to make an informed decision on what plans would best suit your organization's existing infrastructure, identity management processes, collaboration requirements, and desired hybrid model.

All of these services are interwoven with a powerful yet fundamental service that integrates the identity and access control to these services. This is done by Azure Active Directory, which is a

backend directory service in the cloud with which all tenants are provided. Customers have the option to purchase an Azure AD premium subscription that provides more powerful capabilities. Understanding Azure AD and its role is important when operating a SharePoint hybrid environment. This book discusses how your on-premises Active Directory interacts with Azure AD and its role in providing hybrid identity and access control in your environment.

Azure Active Directory

Azure Active Directory (Azure AD) is a powerful, multitenant cloud-based directory that Office 365 employs to authenticate users. Its versatility is demonstrated by its varied capabilities such as identity management, multifactor authentication, device registration, self-service password management, self-service group management, privileged account management, role-based access control, auditing, security monitoring, and alerting. Existing Office 365, Azure and Dynamics CRM Online customers (tenants) automatically become Azure AD tenants. Customers can begin using their Azure AD tenant to manage access to thousands of other cloud applications with which Azure AD integrates.

Planning Azure AD and identity management is important to ensure a smooth transition to a SharePoint hybrid environment. You need to understand the implications for your business of the cloud and hybrid models to be able to implement that transition.

In a hybrid environment, Active Directory on-premises objects such as users and groups are required to be synchronized to Azure AD. This makes your on-premises directory the source of authority for users and groups. A SharePoint hybrid environment requires that users and groups are successfully synchronized between your on-premises directory (Active Directory) and your cloud directory (Azure AD). Having cloud-only identities removes the "hybrid" deployment model, so it is important to note that Active Directory on-premises, Azure AD, and the synchronization engine are essential components to a hybrid environment.

As a prerequisite to ensure a successful cloud services deployment, it is important that the on premises Active Directory is in good health and prepared for synchronization to the cloud. This preparation can take the form of sanitization by removing unneeded objects, user attribute planning, and separation of users and groups into organizational units for synchronization. Chapter 4 covers this in greater detail.

If your organization has a large number of users and groups in your Active Directory on-premises, you might want to engage technical assistance—from Microsoft, a Microsoft partner, or third-party consultant—for the initial configuration. Their services might include assistance to sanitize your on-premises Active Directory and help prepare you to synchronize and integrate your users into Azure AD.

Some of your users and groups might also reside in directories outside of Active Directory. These might also be synchronized to Azure AD through tools such as Azure AD Connect and Microsoft Identity Manager 2016 that has capabilities to connect to other Lightweight Directory Access Protocol version 3 (LDAPv3)–compliant directory stores.

Azure AD Domain Services

Azure AD Domain Services (currently in preview) now gives you the option to create a virtual network in Microsoft Azure, create new virtual machines (VMs) and servers in Microsoft Azure, and connect to a stand-alone managed domain you made available in this virtual network. Users in this network will be able to join this managed domain with their corporate credentials as user accounts; groups and credentials are synchronized to the Azure AD tenant from their on-premises Active Directory. Applications deployed on VMs within the virtual network benefit from Azure AD Domain Services such as domain join, LDAP read, LDAP bind, NTLM and Kerberos authentication, Group Policy, and so on.

www.dbooks.org

It is important to note that only synchronized identities with password synchronization are a mandatory requirement to be able to use Azure AD Domain Services. This is because users' credentials are required in the managed domain provided by Azure AD Domain Services in order to authenticate these users via NTLM or Kerberos authentication methods.

> **More info** To read more about Azure AD Domain Services and the benefits it provides in a hybrid environment, go to https://azure.microsoft.com/documentation/articles/active-directory-ds-overview.

Azure AD Join

Microsoft has made significant investments in developing Windows Server 2016 and Windows 10 to extend hybrid capabilities to an entire range of devices that use the latest Windows operating systems; for example, unlike any other Microsoft operating systems before, you can now choose to join Azure AD when setting up devices running on Windows Server 2016 and Windows 10. With Azure AD Join, users on Windows 10 devices can consume Azure AD resources without having to join your internal Active Directory domain.

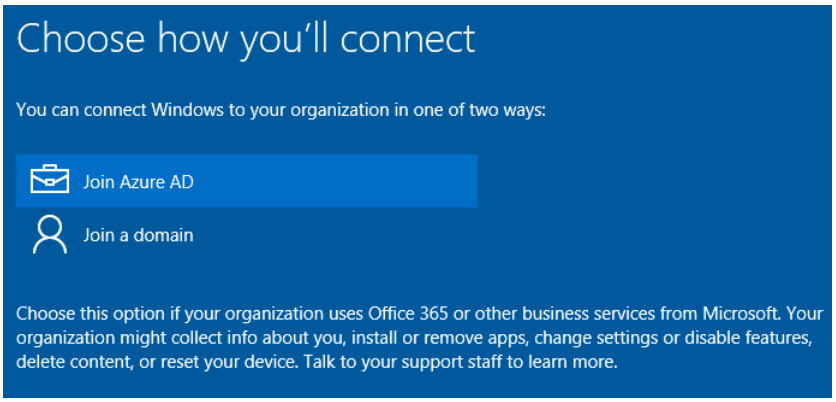


Figure 2-1: You now have the option to join Azure AD instead of an on-premises domain in Windows 10.

Example scenarios of Azure AD Join usage can include not only organizations that are cloud-first/cloud-only that do not have an on-premises Active Directory infrastructure, but also organizations that have devices (such as mobile devices) that are incapable of a traditional domain join. These users can be remote users, temporary, or contract workers that need to collaborate on documents shared in Office 365. Administrators have the control to enforce enrollment policies on these devices if required.

In a SharePoint hybrid scenario, Azure AD Join users can take advantage of single sign-on (SSO) resources in Office 365 and other business applications that rely on Azure AD for authentication. Corporate-owned devices that are joined to Azure AD also enjoy SSO to on-premises resources when the device is on a corporate network, and they can dos so from anywhere when these resources are exposed via the Azure AD Application Proxy.

> **More info** To read more about extending capabilities to Windows 10 devices through Azure AD Join, go to https://azure.microsoft.com/documentation/articles/active-directory-azureadjoin-overview.

Identity models

It is important to understand the three different identity models that are available: cloud identity, synchronized identity, and federated identity. Cloud identity is not truly used in a SharePoint hybrid scenario. Synchronized identity and federated identity are the only two identity models that are used in a SharePoint hybrid environment.

Cloud identity

Although this model is not truly a hybrid model in and of itself, it is important to note that organizations that currently use it may do so as a starting point to integrate with other hybrid models as business requirements and regulatory compliance mandates. In this model, user's identities are managed in the Office 365 Admin Center and stored in Azure AD. There is no synchronization or integration back to an on-premises directory. Users must sign in to Office 365 by typing in their user names and passwords. There are no password synchronization or user-identity relationships, even if an organization has an existing on-premises active directory. Figure 2-2 presents an overview of cloud identities. There is no on-premises directory, SharePoint resources, or any synchronization for user identities. Office 365 and Azure AD is the source of authority as all identities are mastered in the cloud.

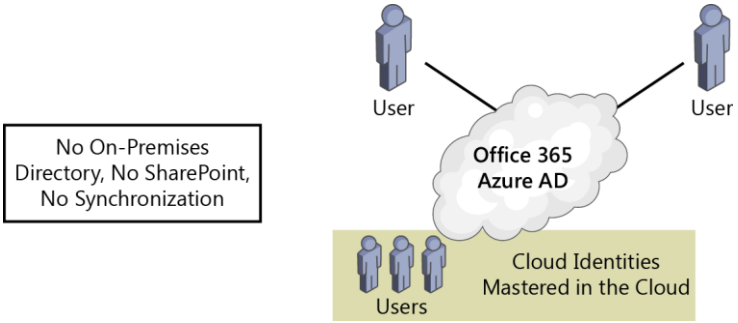


Figure 2-2: An overview of cloud identities.

Following are some cloud identity use cases:

- You are a startup company and require a turnkey IT solution that includes components such as email, user management, Microsoft Office products, SharePoint team sites, chat, and video conferencing.
- Your organization has no on-premises user directory such as Active Directory.
- You simply want to avoid integrating with the cloud because you want to run a pilot trial of Office 365, or your organization's on-premises directory structure is very complex, or your organization is governed by strict regulations.

Synchronized identity

When you integrate with Azure AD, you can synchronize your on-premises Active Directory users with Azure AD. You can also add password synchronization to their on-premises credentials so that password hashes are synchronized with Azure AD. With password write-back, users can change their passwords through a self-service password reset, and the password is written back to their on-premises active directory. Figure 2-3 presents an overview of synchronized identities. An on-premises directory service such as Active Directory exists. Identities are mastered on-premises and are synchronized along with their passwords to the cloud via Azure AD Connect—the directory synchronization tool. On-premises SharePoint and other corporate resources exist on-premises.

www.dbooks.org

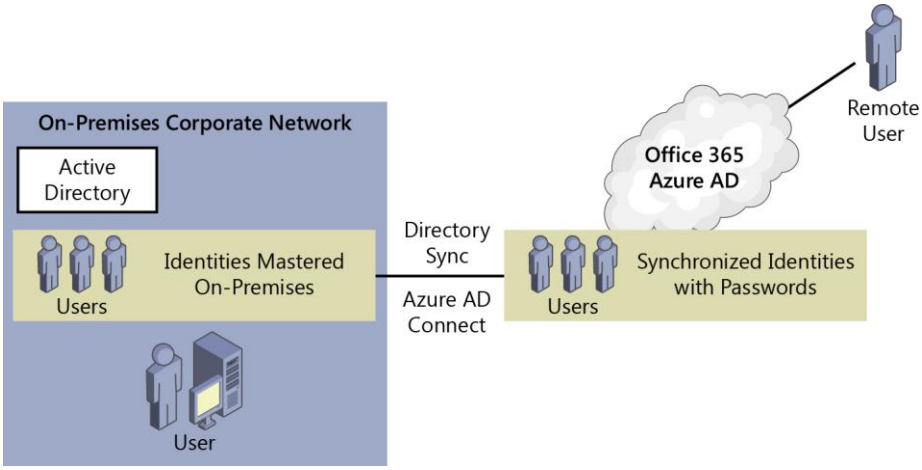


Figure 2-3 An overview of synchronized identities.

Following are some synchronized-identity use cases:

- Your organization has an existing Active Directory domain and wants to maintain its business applications on the internal network.
- Your organization has remote workers who need to securely access resources using their domain credentials while working off site or travelling.
- There are budgetary constraints to operating Active Directory Federation Services (AD FS).
- Your business plans utilize Azure AD Domain Services, for which synchronized identities with password synchronization is a mandatory requirement.

Federated identity: SSO

With federated identities, users from within your organization can seamlessly access Office 365 services without typing passwords, providing a SSO environment. With SSO, Office 365 is configured to trust the on-premises environment for user authentication. You should deploy AD FS infrastructure on premises and publish it to the Internet to support user authentication redirection from the Office 365 sign-in experience. Additionally, you should ensure that this infrastructure is highly available because the business now depends on it for authentication to Office 365–based services. Figure 2-4 presents an overview of federated identities. An on-premises directory service such as Active Directory exists. Identities are mastered on-premises and are synchronized to the cloud via Azure AD Connect—the directory synchronization tool. Passwords aren't synchronized, because users are authenticated via a federation service such as AD FS, also known as Security Token Service (STS). SharePoint and other corporate resources exist on-premises.

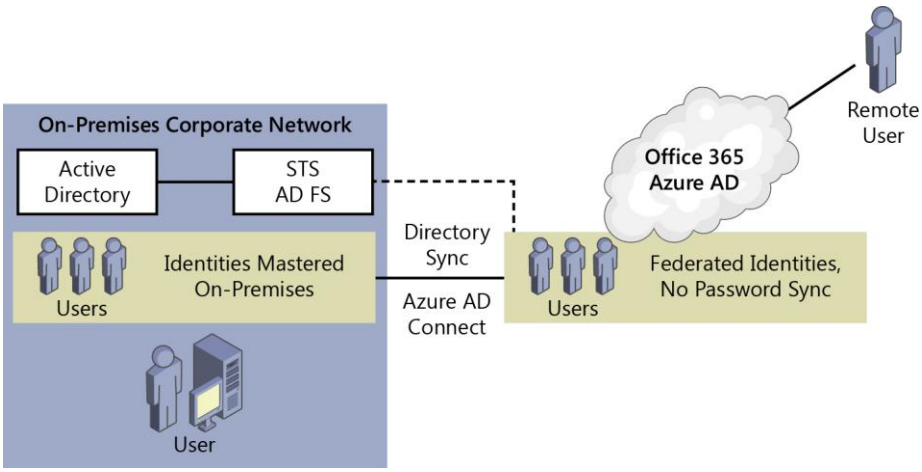


Figure 2-4: An overview of federated identities.

Following are some federated-identity use cases:

- Your organization wants to minimize users having to type user names and passwords, thus providing a seamless hybrid experience.
- You currently run a cloud-identity or synchronized-identity model and plan to implement SSO.
- Your organization has access to IT staff members who are skilled in the management of AD FS or the organization has existing AD FS infrastructure in place.
- You have a requirement to collaborate with partner organizations and increase productivity.
- Your organization plans to gradually transition to the cloud.

How does Office 365 and Azure work?

Microsoft has created a trust between Office 365 and Azure AD. This trust relationship between them is the conduit by which subscribers can utilize any of the SaaS, PaaS, and IaaS offerings. Azure AD is the directory service that Office 365 uses. Just as Active Directory is a store for identities used for authentication for server applications such as SharePoint, Azure AD is a store for identities used for authentication for Office 365 applications such as SharePoint Online and applications in Azure.

Essentially, a hybrid environment is created when on-premises server products are integrated with Office 365 and Azure AD. Administrators can choose which users are synchronized to Office 365 and assign them licenses.

> **Note** It is possible to mix and match Office 365 subscriptions in one tenant. So, it is possible to allocate different types of users to different plans and the corresponding plan features. Users are able to authenticate by using their cloud identities or on-premises credentials, which is the same identity and password.

By using hybrid functionality in SharePoint Server 2016 and SharePoint Online in Office 365, you can integrate and extend to cloud capabilities such as SharePoint Search, Business Connectivity Services, and Duet Enterprise Online.

> **More info** For the Azure subscription and service limits, quotas, and constraints, go to https://azure.microsoft.com/documentation/articles/azure-subscription-service-limits.

www.dbooks.org

There are a variety of ways in which businesses or individuals can get started with Azure. Plans are offered via prepaid subscriptions, Microsoft resellers, and large organizations with Enterprise Agreements. Subscriptions offered through Enterprise Agreements (EAs) offer great benefits such as the following:

- Microsoft's commitment to EA customers continues on to Azure, giving those customers the best prices based on their infrastructure spending, regardless of their upfront Azure commitment.
- The same rates are honored to unplanned growth that EA customers have on Azure. They scale to what they need and pay for what they consume.
- Enterprise portal is a great resource for customers managing multiple accounts or subscriptions.

More info To calculate price of Azure features for your scenarios, go to https://azure.microsoft.com/pricing/calculator. To view the billing usage rate card, go to https://azure.microsoft.com/documentation/articles/billing-usage-rate-card-overview.

Choosing the right Office 365 plan

To be able to synchronize users, the plan you select must have the Active Directory Integration feature available. Office 365 plans for Small Business, Enterprise, Education, Government, and Nonprofit include Active Directory Integration.

Following are some of the popular business and enterprise plans of Office 365:

- Office 365 Business Essentials (300 user limit)
- Office 365 Business Premium (300 user limit)
- Office 365 Enterprise E1 (unlimited users)
- Office 365 Enterprise E3 (unlimited users)
- Office 365 Enterprise E5 (unlimited users)

More info You can access a plan selection tool based on the features that you need at https://products.office.com/business/compare-office-365-for-business-plans.

FastTrack for Office 365

Microsoft's FastTrack engineers can provide your organization with remote and personalized assistance to help you prepare your technical environment and ensure a smooth transition and migration experience. The FastTrack team will work with you to ensure that the core capabilities of Office 365 are ready to use by synchronizing users, assigning user licenses, and moving eligible services.

More info To learn more about FastTrack, go to https://fasttrack.office.com.

Getting started

To become familiar with subscription features and the benefits of Office 365 and Azure, Microsoft offers 30-day free trials. This gives you the ability to test any of the hybrid models with real users, and if you purchase a subscription that covers the number of users, your configuration and user accounts

will remain intact. You won't be able to continue using Office 365 free of charge after your trial subscription ends. Your data will remain for another 30 days, at which point all stored information and your configuration will be permanently deleted. You can cancel subscriptions at any time; however, penalties apply when subscriptions (such as Office 365 Enterprise E5) with annual commitments are canceled mid-contract. You can add multiple Office 365 plans and corresponding licenses to a tenant account. For example, you can purchase a small plan and add other plans as your business and requirements grow.

More info To sign up for a 30-day Office 365 Enterprise E3 trial, go to https://go.microsoft.com/fwlink/p/?LinkID=403802&culture=en-US&country=US.

To sign up for a 30-day Office 365 Enterprise E5 trial, go to https://go.microsoft.com/fwlink/p/?LinkID=698279&culture=en-US&country=US.

To compare the Office 365 plans available, go to https://products.office.com/business/compare-more-office-365-for-business-plans.

To sign up for an Azure AD 30-day trial, go to https://azure.microsoft.com/trial/get-started-active-directory.

For the developer's guide to Azure AD, go to https://azure.microsoft.com/en-us/documentation/articles/active-directory-developers-guide.

Configuring hybrid overview

Depending on the size, internal processes, and governance requirements of your organization, planning and piloting an Office 365 deployment might not be that big of a task. However, factors such as SharePoint hybrid with the added internal governance, change management, and security processes will add to the overall planning and configuring timeframes. The following list provides an overview what is broadly involved in the configuration of SharePoint hybrid:

- Information gathering and business requirements

  Enhance organizational knowledge on Office 365 and the capabilities offered for SharePoint hybrid. If your organization also already uses Office 365 for its Exchange online emails, user identities would already be synchronized to Office 365.

  Gather Business requirements such as business continuity, SSO requirements, and internal Service Level Agreements (SLAs).

  Some organizations might pick and choose the different SharePoint hybrid features and might not require certain features to be rolled out to all users. An example of this is choosing SharePoint online and not choosing OneDrive for Business.

  Identify the pilot users in your organization for hybrid features and determine the roll out schedule to the business. Some hybrid options such as hybrid OneDrive and sites include the ability to direct features to an audience of users. By adding more users to the audience over time a business can phase the rollout to Office 365 on their own terms.

- Plan architecture, topologies, and technical requirements

  Ensure that all SharePoint hybrid infrastructure, network environment, and server requirements are understood and achievable within the agreed timeframes for the business. Check the prerequisites for each of the infrastructure components and ensure that the existing operating systems are at the supported levels.

www.dbooks.org

If you choose federated identity (SSO), ensure that you meet high-availability requirements along with having adequate processes in place to meet the uptime requirements of the SSO STS. If the STS is down, users won't be able to authenticate to Office 365 and Azure, and in turn, SharePoint hybrid services that require authentication will fail.

Gather technical requirements from the business to ensure that you include high-availability strategies for SharePoint and include Azure as an option as either the sole datacenter for a SharePoint farm or a datacenter extension.

- Environment assessment

  Assess your current environment and ensure full compatibility with the cloud before you carry out user synchronization. Tools such as IdFix are purpose-built for these assessments.

  If you're configuring federated identities, ensure that the organization has skilled staff to operate Microsoft federation applications such as AD FS and the Web Application Proxy or non-Microsoft federation applications such as Shibboleth along with other third-party reverse-proxy devices.

  Ensure that the build/version levels of SharePoint Server, your browser, Microsoft Office client applications, and the operating systems are compatible and capable.

- Platform hygiene and remediation

  Perform platform fixes to remediate issues based on the assessment reports and technical requirements. Ensure that servers are ready and prepared for the synchronization tool and/or federation services like AD FS and proxy services such as Web Application Proxy servers.

  Ensure that you have access to modify the DNS host records on your domain name. Ensure firewall rules are in place. Purchase the Secure Sockets Layer (SSL) certificate required for federation identity configuration.

- Turn on core Office 365 synchronization capabilities

  If your organization also already uses Office 365 for its Exchange online emails, users would already be synchronized to Office 365. It's best to ensure that all of the required user attributes are synchronized to the cloud at this stage.

- Turn on SharePoint hybrid features

  Ensure that SharePoint on-premises has the necessary service applications and settings in place; for example, user profile service application is configured and in a good state. Configure server-to-server (S2S) authentication between your SharePoint on-premises farm, SharePoint online, and Azure AD. Configure the chosen SharePoint hybrid features on your farm and where required in Office 365; for example, features such as hybrid extranet are turned on and configured in Office 365. Create audiences, if required, on your SharePoint on-premises farm to roll out to pilot users.

- Optionally, enhance Office 365 integration

  If you initially chose only a synchronized-identity model, this phase would be in anticipation of moving to a federated-identity model to achieve SSO.

  If your organization did not plan for high availability, this would be a good opportunity to visit and present to business the cost and benefits of high availability.

  This phase would also be good to revisit disaster recovery plans and ensure that your documentation is updated to include the architecture, services, configuration endpoints, and permissions in your SharePoint hybrid environment.



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

Microsoft

www.dbooks.org

CHAPTER 3

Architecture, authentication, and authorization

This chapter touches on a wide variety of topics and assists in planning the topology options organizations are faced with when it comes to the infrastructure and server planning. Authentication and authorization topics are discussed to provide an understanding of the behind-the-scenes services and server components required. We look at server-to-server (S2S) authentication and how you can use it in a SharePoint hybrid environment. We explain how user authentication works with federated identities. We also cover some basic permission planning around SharePoint Online.

Architecture topologies

When designing a SharePoint hybrid environment, you need to consider your existing environment's topology. This would include the topology for network, servers, and your SharePoint farm. The domain controller placement, the partner organizations you want to collaborate with, and the devices with which users access data are all important considerations when designing a SharePoint hybrid topology.

A good practice is to have all of the different roles on dedicated servers to avoid issues with administration down the road. Combining roles might be possible but this is subject to some constraints. These are described in detail in Chapter 4 as we walk through each of the servers that are required for the planning.

In this chapter, we will take a look at the different ways you can plan for your architecture.

Figure 3-1 depicts a simplistic SharePoint hybrid environment, using a minimum of servers and with no redundancy should a failure occur. There is no single sign-on (SSO) configured in this example and synchronized identities with password synchronization—no Active Directory Federated Services (AD FS)—is utilized for simplicity. Small businesses might consider this arrangement. Microsoft Azure Active Directory (Azure AD) Connect is installed on the domain controller and the synchronization runs on that server. For such environments, there might be no high availability (HA) requirements and limited server resources. A SharePoint Server 2016 single-server farm with its own SQL server is also provisioned in this environment. When provisioning SharePoint Server 2016, you would need to select the single-server farm role to have an all-in-one SharePoint 2016 installation. I recommended that you keep SQL on its own dedicated server, separate from SharePoint, as illustrated in Figure 3-1.

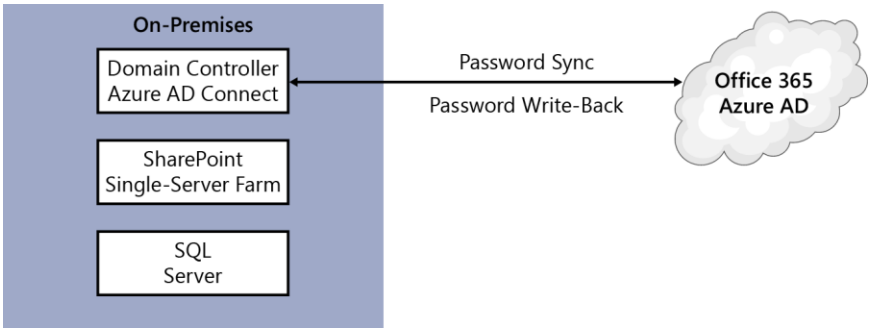


Figure 3-1: A simplified SharePoint hybrid topology environment with no redundancy

Hybrid HA planning

The other side of topology planning takes us to a fully scaled-out environment with SSO, AD FS proxy servers, and HA at every tier. Figure 3-2 shows an on-premises corporate network with a perimeter network for the Web Application Proxy servers for AD FS proxy functionality.

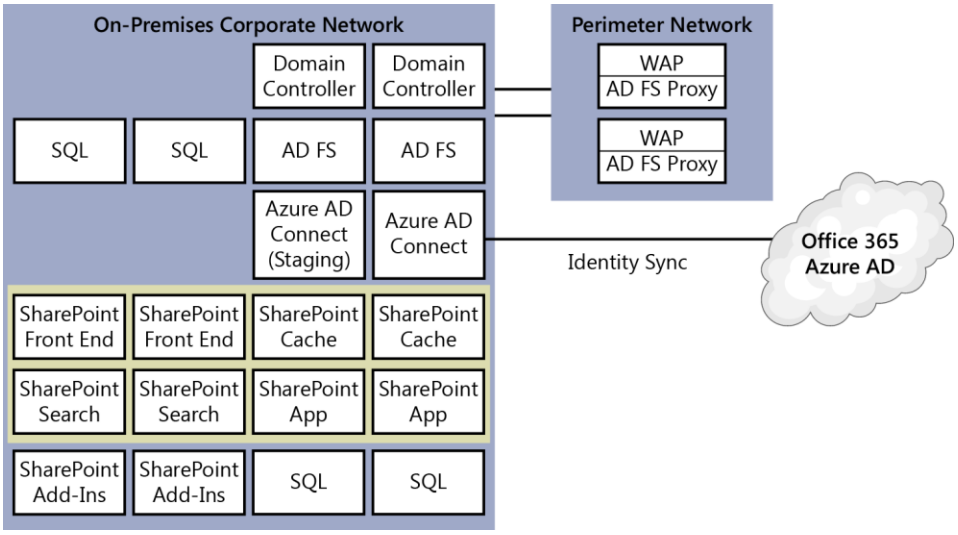


Figure 3-2: A SharePoint hybrid topology environment with redundancy.

www.dbooks.org

There are a minimum of two of each server types with the exception of the Azure AD Connect synchronization server, for which there is only one active server possible at any point in time. To achieve HA with Azure AD Connect, you would need to consider a staging server as described later in this chapter.

The following is a list of the server components that you need to consider in your HA planning:

- **Domain Controller** Two directory servers in your organization to provide redundancy
- **Azure AD Connect synchronization server** No true HA or automatic failover is possible. An Azure AD Connect synchronization staging server is possible, but it requires a manual step to commission it to active service.
- **Active Directory Federation Services (AD FS)** A two-server farm for redundancy behind a load-balanced virtual IP (VIP).
- **SQL Server** A redundant SQL server for AD FS. Two server nodes at a minimum.
- **Web Application Proxy servers with AD FS Proxy capability** Two Web Application Proxy servers to provide redundancy. They need to reside behind a load-balanced VIP address.
- **Network equipment** These devices comprise a redundant pair of reverse proxies, load balancers, proxy servers, firewalls, and network switches.
- **SharePoint Server 2016 on-premises servers** Fully scaled-out SharePoint Server 2016 farm with all the premastered roles such as front end, cache, search, and application. Two of each server is required for redundancy and two additional "Add-in" servers illustrated here to host provider-hosted add-ins for SharePoint. These servers aren't SharePoint servers and can be .NET- or PHP-enabled servers. Additionally, SharePoint will consume its own redundant SQL tier.

Azure AD Connect HA

When you plan for Azure AD Connect HA, it is not possible to have two Azure AD Connect synchronization servers running and synchronizing together; you would need to configure a secondary server as a "staging server." Synchronizing a single Azure AD (Office 365) tenant with multiple Azure AD Connect synchronization servers connected to the same Azure AD directory, even if they are configured to synchronize a mutually exclusive set of objects (with the exception of a staging server), is unsupported.

This staging server will be configured and will have all of the configurations ready for synchronization. In the event of a disaster to the primary Azure AD Connect synchronization server, you will need to use the Azure AD Connect Wizard and perform a manual failover on the staging server. I advise that you place the staging server in an alternative datacenter for fault tolerance.

More info To read more on topologies for Azure AD Connect, go to https://azure.microsoft.com/documentation/articles/active-directory-aadconnect-topologies.

SSO considerations

To configure SSO, you need to consider hosting your own federation service on-premises; for example, sts.contoso.com. Service Level Agreements (SLAs) should match or exceed the SLAs of Office 365 and Azure AD to be able to provide a quality service with minimal disruption to users. You should be aiming for an SLA of 99.9% for your own federation service. This translates to 43 minutes of potential downtime/unavailability per month.

To plan uptime for SSO, you need to consider the entire range of devices and equipment that will be subject to the SLA. These are the network reverse-proxy devices used, load balancer, AD FS proxy servers, AD FS servers, SQL servers, internal network equipment, domain controllers, and all underlying storage and datacenter resources.

ExpressRoute planning

With ExpressRoute, you can connect your organization to connect to Azure over a private connection, not over a VPN tunnel via the public Internet. The advantage of ExpressRoute is faster link speeds—lower latency, more reliability, higher security, and cost benefits for larger consumers.

Using ExpressRoute connections, you can access the following services:

- Microsoft Azure services
- Microsoft Office 365 services
- Microsoft CRM Online services

With ExpressRoute, you can consider Azure as an extended datacenter, with your own direct connection from your on-premises network. For this reason, you can plan to host your AD FS and a pair of domain controllers in Azure (see Figure 3-3).

ExpressRoute has an SLA of 99.9%, which it achieves via geographic separation and discrete hardware components to eliminate single points of failure for each "fault domain."

Other usage scenarios for ExpressRoute are data replication and large data transfers to your geographically separated datacenter (Microsoft Azure), business continuity scenarios, and HA topology requirements. In Azure, you should always configure availability sets when creating two or more virtual machines running the same role. Availability sets guarantees that these virtual machines are hosted on different racks in Azure data centers for HA.

More info For a technical overview on ExpressRoute, go to https://azure.microsoft.com/documentation/articles/expressroute-introduction.

For ExpressRoute pricing, go to https://azure.microsoft.com/pricing/details/expressroute.

For ExpressRoute locations and network connectivity providers, go to https://azure.microsoft.com/documentation/articles/expressroute-locations.

www.dbooks.org

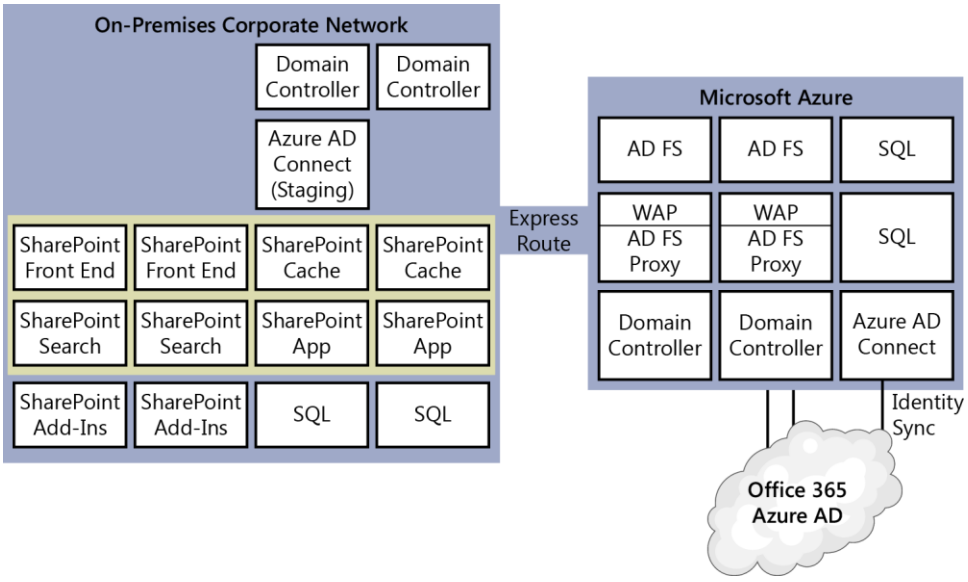


Figure 3-3: A SharePoint hybrid topology environment with redundancy and utilizing availability sets in Microsoft Azure Infrastructure as a Service as an extended datacenter.

Scenarios for SharePoint on-premises and Azure with ExpressRoute

As I mentioned earlier, when you use ExpressRoute, you can consider Azure as your own extended datacenter. For SharePoint hybrid scenarios, you can consider Azure Site Recovery (ASR) and standby farms in Azure. Additionally, Azure can also host your development and test environments. This book is not focused on SharePoint server on-premises but it is useful to cover some of these concepts at a high level for architecture planning purposes.

Azure Site Recovery

With Azure Site Recovery (ASR), you can have the capability to automate the recovery of your virtual machines (VMs) to Azure based on policies you set and control. ASR helps orchestrate replication, failover, and recovery of workloads and applications such as SharePoint on-premises so that they will be available in Azure if your primary datacenter suffers an outage. ASR handles data management, and data replicates directly to your Azure storage account. Replicated Azure VMs are automatically started when failover to Azure occurs. ASR supports encrypted replication of Hyper-V, VMware, and physical servers. Your data is stored in your own Azure storage account and is encrypted at rest. You are able to encrypt the at-rest data and maintain the encryption key.

Health monitoring with ASR is available to continuously monitor your protected resources in Azure. ASR has native support for SQL Server AlwaysOn to manage the failover of availability groups.

For Hyper-V based environments, you will need the following:

- System Center 2012 R2 Virtual Machine Manager (VMM).
- A Hyper-V host with a minimum of Windows Server 2012 with Hyper-V role.
- An Azure subscription.
- An Azure storage account.

- Azure Site Recovery Provider on VMM servers. The Provider communicates with Azure Site Recovery.
- Azure Recovery Services agent on Hyper-V host servers. The agent handles data replication between source and target Hyper-V servers. Nothing is installed on VMs.

More info To read more about ASR, go to https://azure.microsoft.com/documentation/articles/site-recovery-overview.

Standby farms

For business continuity planning, you might want to consider a standby SharePoint farm in which you have VMs prepared and ready for failover when a disaster occurs. It really depends on the SLAs you have to meet for your organization. You can consider planning for a disaster-ready environment in Azure where your standby farm VMs reside in Azure. Your recovery time objective (RTO) will significantly decrease if Azure is already configured to be your organization's backup environment, where backups are already replicated to the Azure datacenter.

The following points describe the different standby farm definitions based on availability.

- **Cold standby** A secondary datacenter that can provide availability within hours or days. The farm is fully built, but the VMs are not running.
- **Warm standby** A secondary datacenter that can provide availability within minutes or hours. The farm is built and VMs are running and updated. Recovery includes attaching content databases, provisioning service applications, and crawling content. The farm can be a smaller version of the production farm and then scaled-out to serve the full user base.
- **Hot standby** A secondary datacenter that can provide availability within seconds or minutes. A fully sized farm is provisioned, updated, and running on standby.

More info To read more about SharePoint disaster recovery in Microsoft Azure, go to https://technet.microsoft.com/library/dn635313.aspx.

To read more about creating a hybrid disaster-recovery environment with Microsoft Azure for your on-premises SharePoint farm, go to https://technet.microsoft.com/library/mt607084.aspx.

To read more about choosing a disaster recovery strategy for SharePoint, go to https://technet.microsoft.com/library/ff628971(v=office.15).aspx.

Planning for multiforest directory scenarios

If your environment has multiple Active Directory forests, you will need to ensure that they are all reachable by the single Azure AD Connect synchronization server. You can do this by opening the appropriate network ports between the Azure AD Connect synchronization server and the Domain controller of the different forests you have. The Azure AD Connect server does not have to be a domain server itself; it can be a workgroup server placed in a common network location such as a perimeter network.

The Azure AD Connect Wizard has capabilities to consolidate users across different forests even if the same user is represented multiple times in those forests. Using the wizard, you can configure so that the user is represented only once in Azure AD. You do this is done on the Uniquely Identifying Your Users page in the wizard. As of this writing, the consolidation capability is scoped for users and not groups. Groups are not consolidated with the default configuration.

www.dbooks.org

More info For more information on Azure AD Connect topologies, go to https://azure.microsoft.com/documentation/articles/active-directory-aadconnect-topologies.

Hybrid network ports and protocols overview

When planning for a hybrid environment, you would need to consider all the network ports and protocols that are required to be open for communication between the on-premises environment, Office 365, and Azure AD. The main ports are HTTPS on TCP 443, because most communications occur with Secure Sockets Layer (SSL) endpoints on both ends.

You need to open other ports initially for directory remediation work and fixing potential identity synchronization issues.

More info To learn more about network ports and protocols used, go to the section "Network Requirements" in Chapter 4.

Identity models in SharePoint hybrid (user authentication)

With SharePoint hybrid, our concern is the management of identities both on-premises and in the cloud, and the authorization of these identities in both environments. We are presented with two SharePoint hybrid identity deployment models: *synchronized identities* and *federated identities*. Both of these models require that our on-premises identities are replicated to Office 365. You do this by means of a directory synchronization tool that runs on your on-premises environment, reads from your directory store (Active Directory), replicates, and synchronizes identities into Office 365. The authentication part of these models are different and have their own set of requirements. Following are descriptions of each model:

- **Synchronized identities** Passwords can be replicated to Office 365 (Azure AD) and authentication is performed by Office 365 (Azure AD) in a forms-based authentication mechanism, regardless of the user's location (whether on-premises or externally).
- **Federated identities** Passwords are not replicated to Office 365 and authentication is performed by a federated Security Token Service (STS) outside of Office 365 (Azure AD). This STS in most scenarios can be on-premises or reside with another Infrastructure as a Service (IaaS) provider like Azure.

The federation authentication process

If you select to configure federated identities, it is important to understand how the federation authentication process works from a user authentication perspective. Throughout the examples used in this book, we will be using AD FS as our federation service provider. Figure 3-4 illustrates the authentication process.

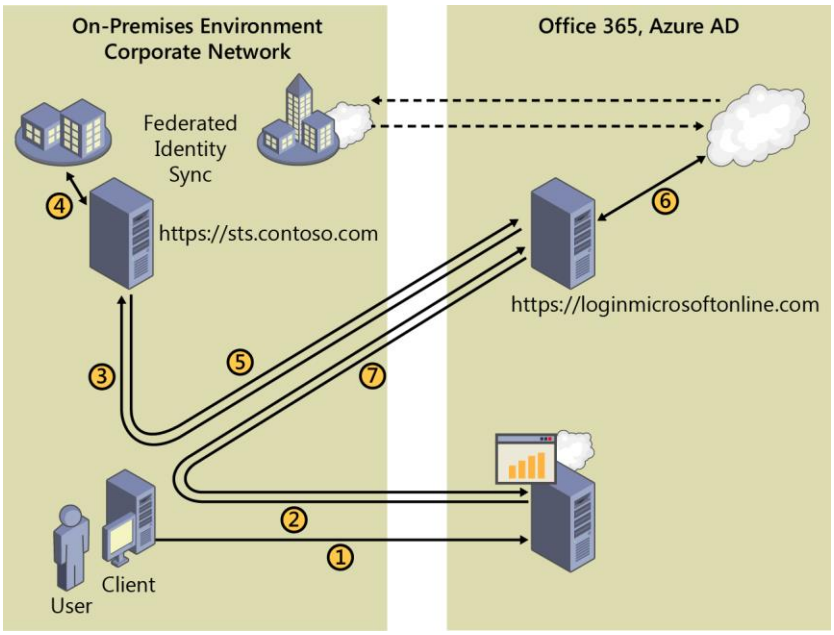


Figure 3-4: The federation authorization process for user authentication.

Following is a description of each step of the process presented in Figure 3-4:

1. The client initiates a connection to Office 365. An internal user attempts to visit SharePoint Online and, in the browser, types https://contoso.sharepoint.com.
2. SharePoint Online (AD FS-aware) requires an authentication token. Because the client in our example here does not have a token, the user is redirected (HTTP 302) to the Office 365 sign-in page at http://login.microsoftonline.com.
3. The user types in her email address, which initiates a script and performs a realm discovery to determine the user's domain name and whether that name is federated. All of this is based on the user principal name (UPN), which in most cases is the same as the email address typed in by the user. Because the realm discovery determined that the domain name is a federated domain, it looks up the authentication URL, which is the federation service; for example, https://sts.contoso.com/.
4. The browser then authenticates against the local federation service (sts.contoso.com) because the client is in the corporate network.
5. AD FS Federation service uses the Office 365 federation trust, the token-signing certificate, and Active Directory and the client request information to generate a Security Assertion Markup Language (SAML) Claim (with the user's on-premises identity) and returns it to the client in an HTTP response. The client is then redirected (HTTP 302) back to the identity platform (login.microsoftonline.com) with the SAML claim.
6. Office 365 identity platform validates the SAML claim by the customer's local AD FS service token-signing certificate. Office 365 Identity resolves the user's on-premises identity to the equivalent identity in Azure AD, and generates a SAML Access Token.
7. The client is redirected (HTTP 302) to SharePoint Online https://contoso.sharepoint.com with the SAML access token.
8. The user is authenticated with SharePoint Online and sees content.

www.dbooks.org

Note SharePoint Online has a feature called auto-acceleration by which the sign-in prompts are reduced and the user is "accelerated" through the Azure AD home real discovery sign-in page. This is achieved by appending the home realm parameter to the sign-in request and is applicable to internal users only.

To read more about auto-acceleration for SharePoint Online, go to https://support.office.com/article/Enable-auto-acceleration-for-your-SharePoint-Online-tenancy-74985ebf-39e1-4c59-a74a-dcdfd678ef83.

To turn on the auto-acceleration feature, in the SharePoint Online Management Shell, run the Set-SPOTenant -SignInAccelerationDomain Windows PowerShell cmdlet:

```
Connect-SPOService -Url https://contoso-admin.sharepoint.com -credential
admin@contoso.com

Set-SPOTenant –SignInAccelerationDomain "contoso.com"
```

To download the SharePoint Online Management Shell, go to http://go.microsoft.com/fwlink/p/?LinkId=255251.

Open Authorization and server-to-server authentication

Open Authorization (OAuth) 2.0 is an open standard for authorization and is a way for users to gain limited access to a resource; for example, a website, by using their Microsoft, Google, Facebook, or Twitter accounts without sharing their password with the website provider (resource owner).

Because user credentials are not passed from one computer to another, authentication and authorization is based on the exchange of security tokens. These tokens grant limited access to a specific set of resources for a specific amount of time.

OAuth essentially allows access tokens to be issued to third-party clients by an authorization server, with the approval of the "resource owner." The third party then uses an access token to access the protected resources hosted by the resource server.

Server-to-server (S2S) authentication uses the OAuth protocol with its token exchange system. In SharePoint, S2S authentication allows for servers that are S2S capable to access and request resources from one another on behalf of users.

Note The S2S authentication protocol used for SharePoint hybrid capabilities is separate from user authentication. You should not confuse it as a user sign-in authentication protocol by SharePoint users.

Cross-server resource-sharing capabilities are possible through software applications that understand server-to-server authentication. These applications include SharePoint 2016 and 2013, Exchange Server 2016 and 2013, Skype for Business Server 2015, Lync Server 2013, Azure Workflow service, SharePoint Online, and Azure Access Control Services (ACS).

Although server-to-server authentication facilitates functionality that was introduced in SharePoint Server 2013—such as eDiscovery, Exchange task management, site mailboxes, workflow manager and Duet—in SharePoint hybrid, it is required for the cloud search service application, hybrid sites features, hybrid Business Connectivity Services, and hybrid Duet Enterprise Online.

Azure ACS

Azure ACS provides an easy way of authenticating (identity) and authorizing users (access control) to gain access to applications and services using popular web-based identity providers such as Microsoft account (formerly known as Windows Live ID), Facebook, Yahoo!, Google, and WS-Federation identity providers. ACS eliminates the need for custom authorization code to be written to the application per social identity provider. ACS provides an authorization store that can be accessed programmatically as well as via a management portal.

Microsoft has outlined its plans to eventually replace Azure ACS with Azure AD. I recommend that you read the current documentation provided by Microsoft on the roadmap of ACS.

Azure AD not only provides directory services for SharePoint Online, but with ACS it is used as a trust broker for both the on-premises SharePoint Server farm and SharePoint Online in a hybrid SharePoint environment.

ACS is compatible with a wide variety of programming and runtime environments, and it supports many protocols including OAuth, OpenID, WS-Federation, and WS-Trust. ACS is compatible with virtually any modern web platform, including .NET, PHP, Python, Java, and Ruby.

ACS integrates with Windows Identity Foundation (WIF). In addition, it supports AD FS 2.0; OAuth 2.0 (draft 10); WS-Trust; WS-Federation protocols; SAML 1.1; SAML 2.0; Simple Web Token (SWT) and Json Web Token (JWT) token formats; Integrated and customizable Home Realm Discovery that allows users to choose their identity provider; and Open Data Protocol (OData)-based management service that provides programmatic access to the ACS configuration.

More info To read more on federated identity with Azure ACS, go to https://msdn.microsoft.com/library/hh446535.aspx.

S2S authentication trust between SharePoint and SharePoint Online

When you set up an S2S trust for hybrid environments, you need to create an S2S trust relationship between your on-premises SharePoint farm, your SharePoint Online tenant, and Azure AD. Essentially you are creating a high-trust authorization system that is created between SharePoint on-premises and SharePoint Online that accommodates interserver communication. SharePoint Online uses Azure AD as a trusted token signing service. You can configure the S2S authentication configuration through Windows PowerShell on an on-premises SharePoint server. However, there are a few other steps that you need to do, which I'll describe later.

S2S authentication trust is an important prerequisite for SharePoint hybrid functionality, such as hybrid search, that requires communication between the SharePoint on-premises servers and SharePoint Online. When it is implemented, a person from SharePoint on-premises can query the SharePoint Online index. The incoming search request is sent to SharePoint online along with the on-premises user's UPN. The UPN is then used to look up the identity of the user in the SharePoint Online user profile store. If a match is found, the user identity is regenerated in the cloud and used to perform security trimming for the search results.

Another important prerequisite for inbound connections, such as hybrid search queries that are performed from Office 365 to search the on-premises farm, is that the User Profile Service Application on-premises must be configured and synchronized with all the users that are synchronized to Azure

www.dbooks.org

AD. It must also have all the user attributes correctly synchronized for the user profiles so that SharePoint can look up the user's UPN and then match and successfully regenerate the user's identity.

Here are the main user properties that you need to validate:

- User principal name (UPN)
- Simple Mail Transfer Protocol (SMTP) address
- Name identifier—such as Windows Security Identifier (SID)
- Session Initiation Protocol (SIP) address

Each SharePoint on-premises farm has its own STS with self-signed certificates by default to validate incoming tokens. In a hybrid environment, Azure AD acts as a trusted token signing service for SharePoint on-premises and uses the SharePoint on-premises STS certificate as the signing certificate.

> **Note** As the S2S STS is not intended for user authentication, you won't see the S2S STS listed on the user sign-in page, in the Authentication Provider section in Central Administration, or in the People Picker in SharePoint on-premises.

Through Windows PowerShell, you can configure Azure AD to trust your STS certificate. Essentially, your STS certificate on each SharePoint on-premises farm should be a Base 64 encoded X.509 certificate with a minimum length of 2,048 bits. You can use a self-signed certificate. I recommend against reusing a certificate from elsewhere. Create a separate certificate for this signing certificate.

Previously, the steps to create an S2S trust between SharePoint on-premises and SharePoint Online were manual, but you now have a few options to easily create an S2S trust. The following options are available to configure the S2S trust:

Method	On-premises version	Considerations
Cloud-driven hybrid picker	SharePoint Server 2016	Available to "first release" Office 365 subscribers. Configures OneDrive for Business or hybrid Site integration features.
Onboard-CloudHybridSearch.ps1	SharePoint Server 2016, SharePoint Server 2013	Configures the Cloud Search Service Application
Manually configure with Windows PowerShell	SharePoint Server 2016, SharePoint Server 2013	Create own STS certificate. Full control on the configuration.

Following are some more details about each method:

- **Cloud-driven hybrid picker** You can use the hybrid picker to create the S2S trust, but it also configures either the OneDrive for Business to Office 365 redirect or hybrid site integration features between Office 365 and your on-premises SharePoint environment. To read more about the hybrid picker prerequisites and functionality, go to http://go.microsoft.com/fwlink/?LinkId=620229.
- **Onboard-CloudHybridSearch.ps1** With the introduction of the Cloud Search Service Application, there is now a Windows PowerShell script available to from TechNet to assist you in creating the S2S trust. The Onboard-CloudHybridSearch.ps1 Windows PowerShell script configures the cloud search service application to interact with the Office 365 tenant and also sets up server-to-server authentication. You can download the Onboard-CloudHybridSearch.ps1 script at http://go.microsoft.com/fwlink/?LinkId=717902.

- **Manually configure with Windows PowerShell** The steps are documented with the SharePoint Server 2013 in TechNet. To read the documentation on how to configure server-to-server authentication from SharePoint Server 2013 to SharePoint Online, go to https://technet.microsoft.com/library/dn197169.aspx.

Configuring S2S trust manually involves the following steps:

- Create a new self-signed or public CA issued X.509 certificate as the new STS token signing certificate. You can use the default farm STS certificate, but provisioning a new certificate is the most common practice.
- Replace the STS token signing certificates on all SharePoint on-premises servers
- On a SharePoint on-premises server, install the following:
  - The Microsoft Online Services Sign-In assistant
  - The Azure Active Directory Module for Windows PowerShell
  - The SharePoint Online Management Shell
- Establish trust between the on-premises SharePoint farm and SharePoint Online
- Upload the newly created STS certificate to SharePoint Online
- Add service principal name (SPN) to Azure for the on-premises domain

  For example, 00000003-0000-0ff1-ce00-000000000000"/*.contsoso.com. The SharePoint Online application principal ID is always 00000003-0000-0ff1-ce00-000000000000.
- Register the SharePoint Online application principal object ID as a trusted provider in SP on-premises
- Configure a common authentication realm between your on-premises SharePoint Server farm and SharePoint Online
- Configure an Azure ACS Application Proxy on-premises

After you establish the S2S trust relationship, both SharePoint on-premises and SharePoint Online trust the security tokens issued by Azure AD. Furthermore, SharePoint Online will be registered as a high-trust application in SharePoint on-premises as part of the S2S trust setup process. It is here that your users (either synchronized identities or federated identities) are granted access to SharePoint resources based on the security tokens that are used by the authentication services in both SharePoint on-premises and SharePoint Online. The STS service in SharePoint on-premises is enabled and utilized for S2S authentication as SharePoint Online is registered as a high-trust application in SharePoint on-premises.

What is identity management?

An identity is an object such as a user, groups of users, or network services that possess a distinctive characteristic or multiple characteristics that determines who that user or group of users are.

Identity management (IdM) is about the processes and controls in place when identifying and controlling a user's access to the resources in a system or application.

Two of the main pillars of IdM that we will focus in this chapter are authentication and authorization:

- Authentication is the process by which you verify what an identity claims itself to be.

www.dbooks.org

- Authorization is about determining what level of access or what actions an authenticated identity is allowed to perform on the network.

Microsoft has released Microsoft Identity Management 2016 which has replaced Forefront Identity Manager 2010 R2. With Microsoft Identity Manager 2016, you are able to synchronize identities between directories, databases and applications, self-service password management with Azure multifactor authentication (MFA), group, and certificate management. A new feature of MIM 2016 is the privileged access management.

With MIM 2016, you can create identity management activity reports of events that are both on-premises and in the cloud. These reports can be then viewed in the Azure portal.

> **More info** Chapter 4 explains more about planning identity attributes for directory synchronization.

Planning source of authority

Your organization user identity management might be complex and might require some IdM planning around especially the *source of authority*. Source of authority refers to the location where identities, such as users and groups, are mastered (the original source). If configured, user write-back makes it possible for Office 365 administrators to create users from within Office 365 or Azure AD. Azure AD Connect then writes back the identity to Active Directory. In such instances, you would need to plan the identity lifecycle of that object—how it is created, managed, and eventually deactivated for deletion.

Another aspect of planning for source of authority is that in many organizations the user attributes themselves have different sources of authority where they are mastered at an attribute level; for example, telephone-related information might be mastered in an organization's phone system, human resources information might be mastered in the HR system, and user photos might be mastered in the SharePoint farm on-premises (Thumbnail attribute export). In this example, all of these would need to be aggregated and written to Active Directory so that the identity contains the rich set of attributes, ready to be synchronized to Azure AD or consumed in other systems such as SharePoint on-premises.

Azure AD requires a single source of authority for every object because it is unable to aggregate all these attributes from their mastered systems. This is where an application like Microsoft Identity Manager 2016 would populate Active Directory from all the sources of authorities, and, in turn, Azure AD Connect will synchronize this to the cloud. Microsoft Identity Manager 2016 has its own synchronization engine that you can use against a wide range of directory stores. Chapter 4 covers this in greater detail.

Authorization: planning access

When planning authorization for SharePoint hybrid, we need to plan for not only SharePoint on-premises but also for SharePoint Online. We also need to understand what the other Office 365 features for SharePoint hybrid offer in terms of security access planning. This section is primarily focused on explaining SharePoint Online access.

> **Note** You should never use on-premises built-in domain groups and users in any SharePoint on-premises permissions. These built-in groups and users are never synchronized to the cloud because they are flagged as "IsCriticalDomainObject" and are blocked from synchronization.

Plan SharePoint Online access

You can enforce user access by the following security control features of SharePoint Online:

- SharePoint groups

  There are three default SharePoint groups that are created when the site collection is created. Each of these precreated default SharePoint groups has its own preconfigured permission settings. The groups with their permission settings are as follows:

  - Members, Edit permission level
  - Owners, Full Control permission level
  - Visitors, Read permission level

  All users placed in each respective group are granted the same level of access as the other users that are part of the same group of which they are members. A site collection administrator typically adds user, multiple users, or a group of users to the SharePoint group. For the initial set of site collections created in every tenant, the initial site collection administrator is the global administrator of the Office 365, with the exception of the "my" site collection.

  Site collection administrators also have the choice to add synchronized groups of users that were synchronized from the on-premises directory through the Azure AD Connect synchronization engine.

- Permission levels

  Permission levels are applied to SharePoint groups and users. There are currently eight precreated permission levels in SharePoint Online:

Permission level	
Full Control	Has full control
Design	Can view, add, update, delete, approve, and customize.
Edit	Can add, edit and delete lists; can view, add, update and delete list items and documents.
Contribute	Can view, add, update, and delete list items and documents.
Read	Can view pages and list items and download documents.
Limited Access	Can view specific lists, document libraries, list items, folders, or documents when given permissions.
Create New Subsites	Can create new subsites.
View Only	Can view pages, list items, and documents. Document types with server-side file handlers can be viewed in the browser but not downloaded.

  You can create new permission levels for specific permission in SharePoint, such as the following:

  - List permissions
  - Site permissions
  - Personal permissions

  It is recommended that you not modify the default permissions levels, because it can cause access issues and hinder Microsoft support in assisting. However, you can edit your own custom

www.dbooks.org

permission levels, created by your organization. My advice is to create your own SharePoint groups with custom permission levels and edit as you require.

- Permissions inheritance

  Just like SharePoint on-premises permissions, the permissions apply to all sites and all site content in the site collection.

  You can further customize permission settings to reflect the requirements of the organization, the business division, or as directed by an endorsed information architecture plan. Site collection administrators can stop the inheritance of permissions at a specific site and can create new groups with their own custom permissions. These changes can be made at the level of the site collection hierarchy by the site collection administrator. Other site owners have the privileges to break inheritance on the sites that they own.

- Preconfigured objects

  There are a few preconfigured objects in SharePoint Online that you would need to consider in your authorization planning.

  - Company Administrator

    Claims encoding example: c:0-.f|rolemanager|{SID}

    By default, all Office 365 global administrators are members of the Company Administrators role and are site collection administrators of the primary root site collection in SharePoint Online. I recommend against modifying membership of Company Administrators because it can lead to unexpected consequences.

  - Everyone except external users

    Claims encoding example: c:0-.f|rolemanager|spo-grid-all-users/{GUID}

    By default, all users, when synchronized to Office 365, are automatically members of the Everyone Except External Users group. By default, the Everyone Except External Users group is added to the Members group on the SharePoint Team Site that has the contribute permission level. By default, all licensed users added to Office 365 are able to view, add, update, and delete items from lists and libraries. If you want to change the permission levels for this group, you can remove it from the Members group and then add it to a group that uses different permissions. For example, you might add the Everyone Except External Users to the SharePoint Visitors group (read permissions).

  - Everyone

    Claims encoding example: c:0(.s|true

    This is the All Authenticated Users group that is preset in SharePoint Online. I recommend against altering this in any way because it can cause unexpected results.

Note Every SharePoint site your users work on is within or under a site collection. Every site exists in a site collection, which itself is a group of sites under a single top-level site called the *root site* of the site collection.

To manage site collections, manage owners and sharing properties, go to the SharePoint admin center in Office 365; for example, https://contoso-admin.sharepoint.com, as illustrated in Figure 3-5.

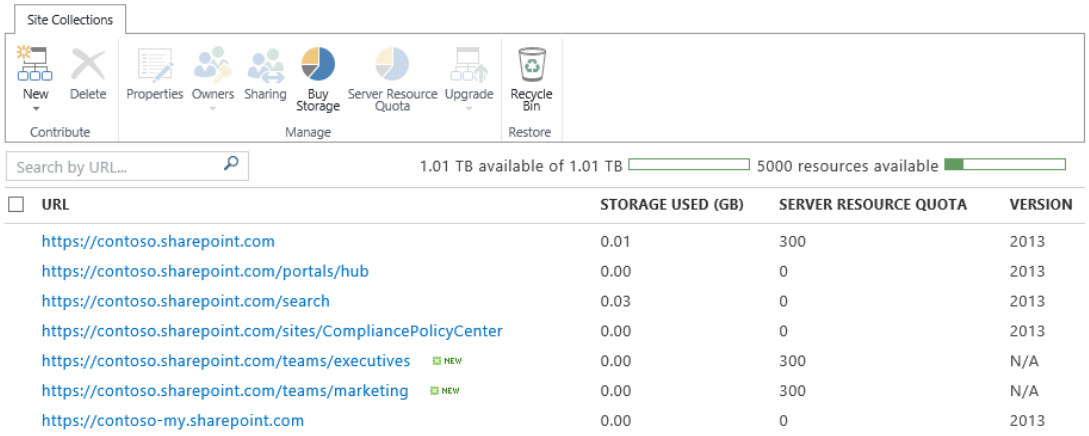


Figure 3-5: SharePoint Online site collections are managed through the SharePoint Admin Center in Office 365.

The company administrator for your Office 365 subscription is the first site collection administrator. The site collection administrator can grant permission for other users to become site collection administrators as needed.

More info To learn more about planning sites and managing users, go to https://support.office.com/article/Plan-sites-and-manage-users-95f9eb7a-4ac8-4dd5-a883-17686cbf8fff.

Plan for users outside the organization to access resources

If you want to plan sharing documents and collaborating other business partner organizations, with vendors, clients, or customers, you would consider the external sharing features of SharePoint Online. You are able to share content with people outside your organization, and they are not required to have licenses for your Office 365 subscription.

There are three options available for sharing with external users (see Figure 3-6):

- Don't allow sharing outside your organization

  Prevent all users on all sites from sharing sites or sharing content on sites with external users.

- Allow external users who accept sharing invitations and sign in as authenticated users

  Require external users who have received invitations to view sites or content to sign in with a Microsoft account before they can access the content.

- Allow sharing with all external users and by using anonymous access links

  Allow site users to share sites with people who sign in as authenticated users, but you also want to allow site users to share documents through the use of anonymous guest links, which do not require invited recipients to sign in.

www.dbooks.org

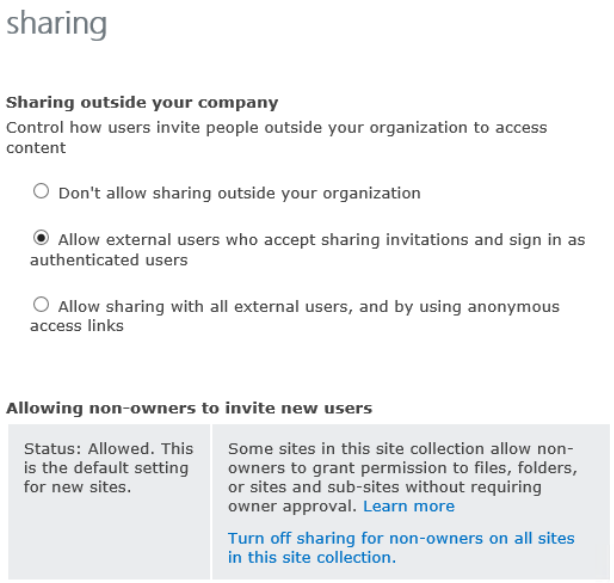


Figure 3-6: The SharePoint Online site collection sharing settings.

More info To read more on how to manage external sharing for your SharePoint Online environment, go to https://support.office.com/article/Manage-external-sharing-for-your-SharePoint-Online-environment-c8a462eb-0723-4b0b-8d0a-70feafe4be85.

Plan for administrators

I recommend that you plan to set aside a dedicated Global Administrator account for technical administration purposes such as configuring directory synchronization and federation services for SharePoint hybrid.

I would further recommend that this account's use the .com domain address. The contoso.onmicrosoft.com domain is considered the default domain.

For example, administrator@contoso.onmicrosoft.com.

More info To learn more, go to https://support.office.com/article/SharePoint-Online-Planning-Guide-for-Office-365-for-business-d5089cdf-3fd2-4230-acbd-20ecda2f9bb8.

CHAPTER 4

Platform hygiene preparation

This chapter goes through the preparation steps required for an on-premises environment to integrate with the cloud, especially for a Microsoft SharePoint hybrid topology. This includes prerequisite planning, scanning, and fixing potential issues with user-identity attributes.

Organizations that have an existing Microsoft Office 365 subscription might have performed most platform preparation tasks already. To make an informed decision, organizations are recommended to invest in the knowledge of what's available in terms of SharePoint hybrid deployment topologies and their requirements. In fact, there is no one-size-fits-all approach; every organization has its own requirements, roadmaps, user attributes, varying platforms, and operating system versions. Adequate, informed planning is important and should not be overlooked.

Planning requirements and functionality

The requirements for configuring a SharePoint hybrid environment are varied. This is not surprising, given how many different products and services that are integrated together to form this environment. Each of these products and services require various skill levels to install, operate, and manage. This section is all about planning the minimum requirements to get your organization started with cloud capabilities.

The following list provides a synopsis of what you need to do to configure a SharePoint hybrid environment:

- Purchase or trial an appropriate Office 365 subscription
- Utilize an existing or acquire a new domain name
- Configure and verify domain name
- Perform Office 365 readiness checks

www.dbooks.org

- Identify and prepare on-premises server and network infrastructure
- Prepare the on-premises directory for synchronization
- Configure user synchronization via Azure Active Directory Connect (Azure AD Connect)
- Optionally, configure Active Directory Federation Services (AD FS) for single sign-on (SSO) authentication
- Activate Office 365 licenses for users
- Prepare SharePoint on-premises farm
- Configure SharePoint hybrid capabilities

Note This chapter focuses on the on-premises platform preparation as prerequisite to synchronizing users in the cloud (directory synchronization).

Environment preparation

Before organizations plan for integrating into Office 365, careful planning is required to ensure that the on-premises platform, network, servers, and user directory with its attributes are in a clean state, ready to be synchronized with the cloud.

More info For additional reading on Office 365 integration with on-premises environments, go to https://support.office.com/article/Office-365-integration-with-on-premises-environments-263faf8d-aa21-428b-aed3-2021837a4b65.

For more information on Azure AD Connect prerequisites, go to https://azure.microsoft.com/documentation/articles/active-directory-aadconnect-prerequisites.

Office 365 readiness checks

The Office 365 health, readiness, and connectivity checks is a tool that gathers configuration requirements for the services that you want to set up. It performs readiness checks against your on-premises environment to ensure that basic requirements are met. You can run it as the first step when analyzing your environment or after you have made configuration changes. Running these checks is a good start to ensuring that the foundational blocks are in place for your SharePoint hybrid environment.

The tool checks for the following:

- **Domains** This looks at your Office 365 verified domain and domain name system (DNS) settings to ensure that they are complete and accurate. Errors might be reported for settings you haven't made yet. You can always rerun the Office 365 Readiness check tool again to verify settings after they have been made.
- **Users and Groups** Determines whether Active Directory is present and evaluates settings and establishes whether the environment is ready to deploy directory synchronization and/or SSO.
- **Office setup** This performs several checks, including Microsoft Office settings and your desktop's Outlook configuration. Incompatible add-ins are checked.
- **Computer update status** Looks to see if the desktop Windows update is outdated as well as determining your Internet browser versions, and other configuration settings.

To run the Readiness checks, perform the following steps:

1. Ensure that you're using a computer running Windows 7 or greater (64-bit only with .NET 3.5).
2. Go to https://portal.office.com/Admin/Default.aspx#ToolsPage, sign in using your onmicrosoft.com account (with Global Administrator rights), and then select Check Your Configuration With Office 365 Health, Readiness, And Connectivity Checks.
3. Select either the Quick or Advanced check box (see Figure 4-1), click Next, and then, on the page that opens, click Run Checks.
4. Install any prerequisite software (when prompted). You need to download a small app for the checks to run.
5. Review the results of the checks.

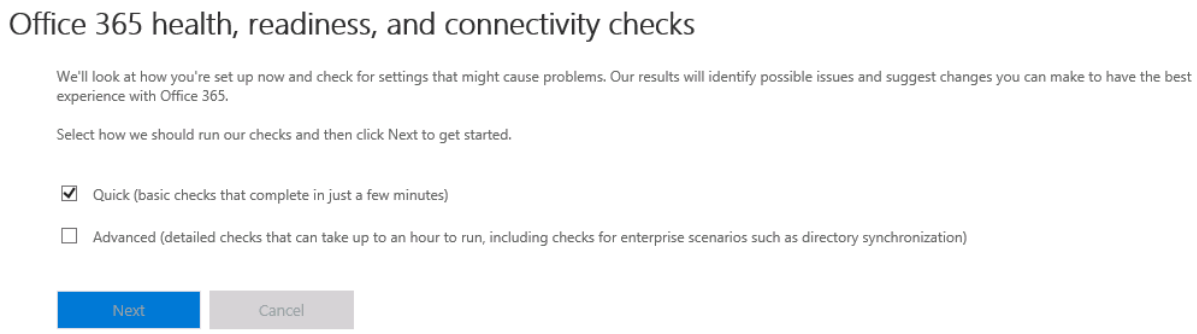


Figure 4-1: The Office 365 Health, Readiness, And Connectivity Checks Wizard.

More info To learn more about the readiness checks, go to https://community.office365.com/w/deploy/office-365-readiness-checks.

User identities and directory preparation

To be able to synchronize your users to the cloud, you would need to achieve compliance in your directories. For example, you must scan and clean Active Directory to be able to synchronize users to the cloud without issues. The synchronization tool is an important element of SharePoint hybrid. Chapter 5 covers the configuration of the directory synchronization tool (Azure AD Connect) in detail. From the perspective of platform hygiene preparation, we need to ensure that the cloud's requirements are satisfied, regardless of the chosen identity model (synchronized identity or federated identity). Microsoft has developed easy-to-use tools to make the journey to the cloud easier. For example, you will need to prepare your on-premises directory for synchronization. To do this, you should use the IdFix tool developed by Microsoft to scan and report on problems with your on-premises Active Directory. Currently, IdFix tool works with Active Directory and Lightweight Directory Access Protocol (LDAP) directories.

Note We'll look at the IdFix tool in greater detail toward the end of this chapter.

If your organization has an identity management system or another automated process to create users, you need to implement careful planning and pay attention to ensure that process finishes successfully and be alert for problems that might occur. For example, attributes that are fixed by the IdFix tool might revert back to the original state that was initially flagged as an error by the tool.

www.dbooks.org

You should review your current identity management system or user creation process to ensure that the user attribute settings are not constantly generating incompatible attribute values that will display as errors in the IdFix tool. You can optionally update the following user attributes via the IdFix tool:

- mail
- mailNickName
- proxyAddresses
- sAMAccountName
- targetAddress
- userPrincipalName

Generally, discovery and remediation activities for your on-premises directory should include the following tasks:

- Identify users who need to be synchronized to the cloud. Assign them as members of an Active Directory group or place them in an Active Directory Organization Unit (OU) for synchronization.
- Check and remove duplicate proxyAddress and userPrincipalName attributes.
- Update blank and invalid userPrincipalName attributes such as nonroutable domain names.
- Check for attribute values that exceed specified character lengths.
- Remove invalid and questionable characters in the following attributes: mail, mailNickName, sAMAccountName (only if no user principal name [UPN] value), targetAddress, and userPrincipalName.

Active Directory schema

The on-premises Active Directory forest functional level must be Windows Server 2003 or later. There is no specific version for the domain functional level required as long as the forest level requirements are met.

> **More info** To learn more, go to https://azure.microsoft.com/documentation/articles/active-directory-aadconnect-prerequisites.

External domain name

If the chosen identity deployment model is federated identities, you must configure AD FS for the SSO experience. An externally accessible domain name is required. To make the process simple, Microsoft has tied up with GoDaddy to easily configure domains purchased through that service. If the purchased or existing external domain name does not match the on-premises Active Directory domain name, you need to add the external domain as an alternate UPN suffix to the existing active directory domain. To add an alternative UPN suffix, you need to open the Active Directory Domain and Trusts Administrative tool by right-clicking Active Directory Domains And Trusts and then selecting Properties. The matching UPN suffix must be added to the internal domain (see Figure 4-2), and all users who are planned for synchronization to Azure AD must have the alternative UPN specified; for example, the domain name contoso.com.

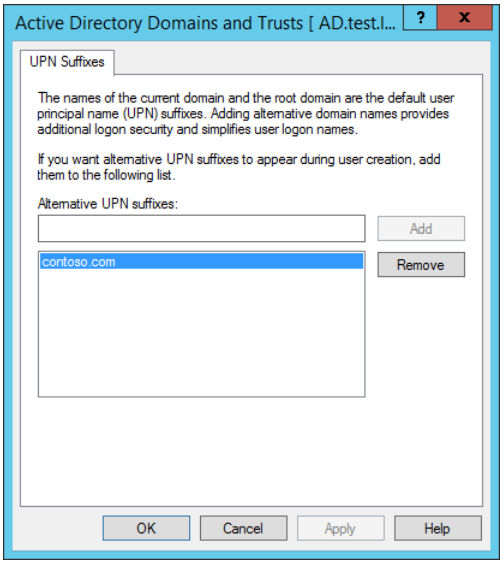


Figure 4-2: contoso.com is added as an alternative UPN suffix for the Active Directory domain.

A single Office 365 tenant (account) can host multiple domains. For example, one Office 365 account can host contoso.com, fabrikam.com, and northwindtraders.com. You can add up to 900 domains to your Office 365 subscription, under most circumstances.

You cannot share or spread an individual domain across multiple Office 365 tenant accounts. For example, contoso.com can belong only to one tenant account in Office 365.

If an organization utilizes subdomains as part of its Active Directory domain and forest hierarchy, the parent domain must be registered in the Office 365 Admin Center first. For example, the parent contoso.com must be registered first before you can register subdomains such as corp.contoso.com, asia.contoso.com, and europe.contoso.com.

More info For more information about custom subdomains, go to http://go.microsoft.com/fwlink/?LinkId=321220.

When you sign up for an Office 365 account, you are allocated a subdomain name of the onmicrosoft.com initial domain; for example, contoso.onmicrosoft.com. You cannot change contoso.onmicrosoft.com to another subdomain name such as fabrikam.onmicrosoft.com in the same Office 365 account. You can use Office 365 features such as email and other collaborative capabilities, but it won't be under your businesses domain name. Emails will be received and sent from user@contoso.onmicrosoft.com. You would need to select a domain name that you want to use for Office 365 features. Furthermore, a SharePoint hybrid environment is not possible with just the initial domain name (onmicrosoft.com), because you don't have access to manage the onmicrosoft.com domain name to configure AD FS essentials such as adding an A record or Secure Sockets Layer (SSL) certificate verification. For these reasons it is necessary for you to use either an existing domain name or purchase a new domain name that represents your business, school, organization, or, alternatively, an easy to remember domain name for your users if you aren't planning to use Exchange online.

After the domain name you plan to use has been selected and added in Office 365, you need to verify the domain. For example, if you plan to use contoso.com for your users, verify that this domain is configured as the default domain for your users. However, as a global administrator, it is best to safely store the onmicrosoft.com administrator's credentials because you will need it when configuring synchronization with the Azure AD Connect tool. A good practice is the administrator should designate a synchronized account as an additional global administrator.

www.dbooks.org

Internal domain name

Office 365 requires a routable Internet domain name (.com, .gov, .org, .com.au, etc.) that it can verify for Azure AD for its synchronization of Active Directory objects. Because nonroutable domain names such as .local or .internal cannot be verified, the user will be synchronized to the .onmicrosoft.com domain in Office 365. For example, if the UPN of a user is akelly@contoso.local, the user's synchronized account in Office 365 will be created as akelly@contoso.onmicrosoft.com.

Renaming the internal domain to the domain (Internet routable) you verified in Office 365, but that is not recommended due to the risks breaking your on-premises applications.

> **Note** If your domain NetBIOS name is different than the fully qualified doman names (FQDN) of the domain, SharePoint on-premises user profile synchronization service might not start or function properly without granting Replicate Directory Changes permission on the cn=configuration container and also setting the NetBiosDomainNamesEnabled property for the User Profile Synchronization connection. For more information, go to https://technet.microsoft.com/library/hh296982.aspx and https://technet.microsoft.com/library/ee721049.aspx.

The recommended approach is to add the UPN suffix (the same as you verified in Office 365) as an additional domain and change the users UPN with the newly added UPN suffix, as demonstrated in Figure 4-3.

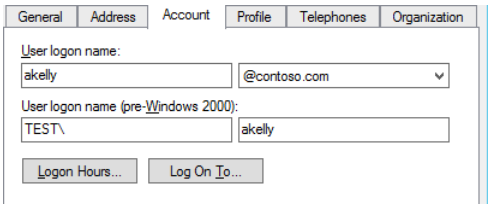


Figure 4-3: The UPN of a user set to an Internet-routable domain contoso.com, whereas the internal domain is TEST.local

> **More info** For a step by step guide to adding a new UPN suffix, go to https://support.office.com/article/How-to-prepare-a-non-routable-domain-such-as-local-domain-for-directory-synchronization-e7968303-c234-46c4-b8b0-b5c93c6d57a7?ui=en-US&rs=en-US&ad=US.

If you have a lot of users to update, it is easier to use Windows PowerShell. The following example uses the cmdlets Get-ADUser and Set-ADUser to change all contoso.local suffixes to contoso.com:

```
$LocalUsers = Get-ADUser -Filter {UserPrincipalName -like *contoso.local'} -Properties userPrincipalName -
ResultSize $null

 $LocalUsers | foreach {$newUpn = $_.UserPrincipalName.Replace("contoso.local","contoso.com") $_ | Set-ADUser
-UserPrincipalName $newUpn}
```

See Active Directory Windows PowerShell module http://go.microsoft.com/fwlink/p/?LinkId=624314 to learn more about using Windows PowerShell in Active Directory.

> **Note** For rollback purposes, it is important to verify that you have the appropriate backups in place before running any of the commands in this book. Carefully go through the commands and update them before running them. It is recommended that you run the preceding code in a test environment first.

Some Active Directory objects might not have UPNs assigned to them due to various factors such users that existed from legacy domain environments. You can use the following Windows PowerShell script to find all users without a UPN configured:

```
(Get-ADUser  -Filter {-not (UserPrincipalName -like '*')} -SearchBase
'OU=LegacyUsers,DC=test,DC=local').Count
```

Here's a Windows PowerShell script to set the UPNs to the users from a certain OU that do not have a UPN assigned to their account:

```
Get-ADUser  -Filter {-not (UserPrincipalName -like '*')} -SearchBase 'OU=LegacyUsers,DC=test,DC=local' | %
{$UPN = $_.SamAccountName + "@contoso.com" ; Set-ADUser -Identity $_.DistinguishedName -UserPrincipalName
$UPN}
```

> **Note** You cannot synchronize objects in Active Directory that have the property `IsCriticalDomainObject = true` due to security restrictions; for example, the Administrator built-in account and Domain Users built-in group will not be synchronized.

Multiforest environments

Organizations that have multiple Active Directory forests can synchronize them to a single Office 365 tenant account. The main consideration here is to ensure that no duplicate UPNs or email addresses exist across the forests. For example, a user with the same UPN or email address should not overlap between the forests.

Currently, only Azure AD Connect and Microsoft Identity Manager 2016 support multiforest synchronization operations.

> **Note** Microsoft Identity Manager Server software rights are granted with Windows Server licenses (any edition). Because Microsoft Identity Manager runs on Windows Server OS, as long as the server is running a valid, licensed copy of Windows Server, you can install and use Microsoft Identity Manager on that server. No other separate license is required for Microsoft Identity Manager server.
>
> For more information, go to https://azure.microsoft.com/documentation/articles/active-directory-editions.

Some organizations might have non-Microsoft directory services to manage identities. As long as that service is LDAPv3-compliant, Azure AD Connect can synchronize with it. Contact Microsoft Support or specialist partners for more information or assistance.

Name resolution (DNS)

There are a few DNS records that need to be configured for the domain verification for Office 365. If the domain is hosted on GoDaddy, Microsoft can automatically configure your domain and add the necessary DNS records for you, as illustrated in Figure 4-4. You would need the user name and password to your GoDaddy account. It is very useful for businesses with simple requirements or pilot/test usage scenarios.

www.dbooks.org



View the DNS records we'll add

MX records

Priority	Host name	Points to address or value	TTL
0	@	contoso-com.mail.protection.outlook.com	3600

CNAME records

Host name	Points to address or value	TTL
autodiscover	autodiscover.outlook.com	3600
sip	sipdir.online.lync.com	3600
lyncdiscover	webdir.online.lync.com	3600
msoid	clientconfig.microsoftonline-p.net	3600
enterpriseregistration	enterpriseregistration.windows.net	3600
enterpriseenrollment	enterpriseenrollment.manage.microsoft.com	3600

TXT records

TXT name	TXT value	TTL
@	v=spf1 include:spf.protection.outlook.com -all	3600

SRV records

Service	Protocol	Port	Weight	Priority	Name	Target	TTL
_sip	_tls	443	1	100	@	sipdir.online.lync.com	3600
_sipfederationtls	_tcp	5061	1	100	@	sipfed.online.lync.com	3600

Figure 4-4: Office 365 automatically configured the domain contoso.com that was registered through GoDaddy.

Alternatively, if your domain is hosted by another hosting company or if you choose to modify DNS records yourself, you would need to configure the DNS records, as indicated in the Office 365 page at http://go.microsoft.com/fwlink/?LinkId=321222.

If you are planning to send emails from SharePoint Online to external recipients, you want to ensure that emails are successfully delivered. You can do this by using Sender Policy Framework (SPF), a simple email-validation system. You must add the following .txt record (containing the SPF) so that email is delivered from sharepoint.com and sharepointonline.com:

```
v=spf1 include:spf.protection.outlook.com include:*.sharepoint.com include:*.sharepointonline.com -all
```

> **Note** To read more about SPF and SharePoint online, go to https://community.office365.com/f/158/t/263103.

For AD FS SSO, you must create a DNS A record that points to the load-balanced virtual IP (VIP) of the federation service, which is essentially the Security Token Service (STS) endpoint exposed to the Internet via an SSL certificate. Ideally the endpoint would be exposed by two AD FS proxy servers for high availability and would be placed in a perimeter network for security reasons.

For internal users, you must create an internal DNS A record that points to the federation service VIP on the on-premises environment.

For example, in Figure 4-5, sts.contoso.com points to your AD FS Web Application Proxy load balancer VIP address.

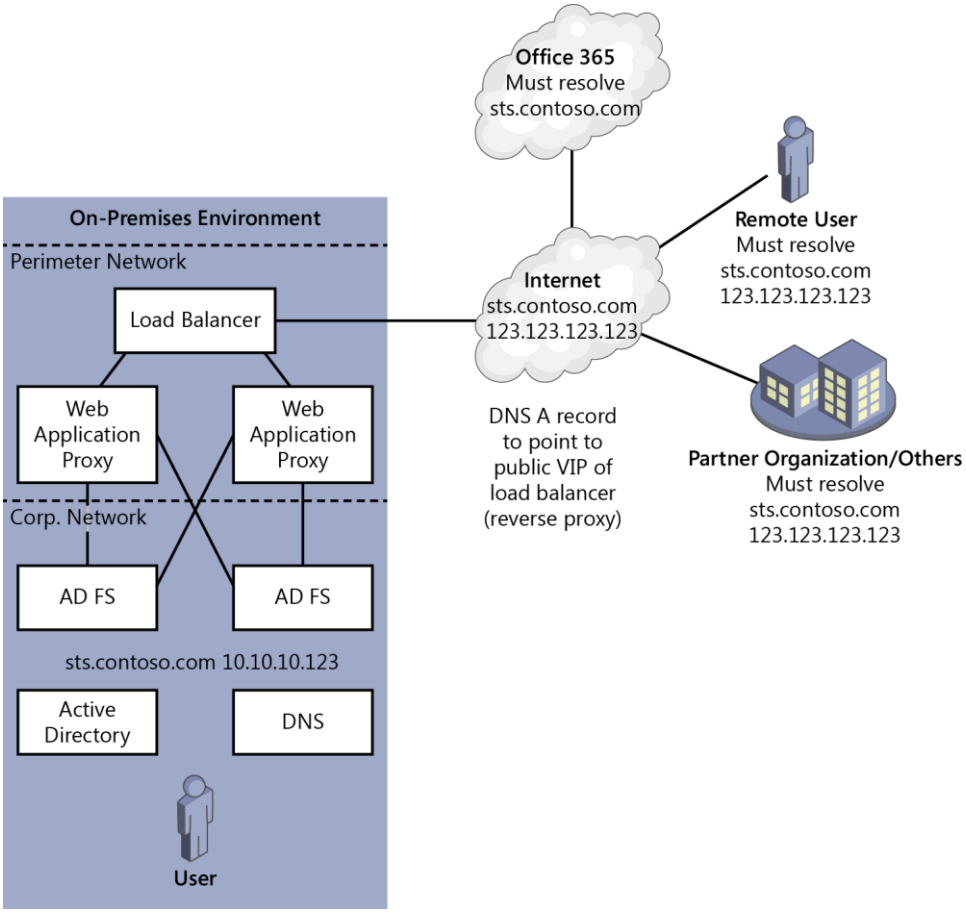


Figure 4-5: The AD FS STS must be available internally and externally. It must be resolvable from Office 365, remote users, and partner organizations.

More info To read more about the DNS records required for Office 365, go to https://support.office.com/article/External-Domain-Name-System-records-for-Office-365-c0531a6f-9e25-4f2d-ad0e-a70bfef09ac0.

SSL certificates

If you are considering AD FS for SSO, you will need an SSL certificate. AD FS makes extensive use of SSL certificates. You must use an X.509 certificate, and the same certificate must be applied across all AD FS and Web Application Proxy server nodes.

For SharePoint hybrid deployments, the AD FS service exposed to the public Internet requires a public SSL certificate issued by a trusted Certification Authority (CA) such as GeoTrust, Symantec, or Thawte. It is important that the subject name or subject alternative name (SAN) dnsName property of the SSL certificate matches what was configured for the AD FS service name; for example, sts.contoso.com or a wildcard *.contoso.com to include subdomains. Chapter 6 contains information on configuring federated identities and AD FS prerequisites.

If you're planning on using the Workplace Join feature, you will need an additional SAN with the value enterpriseregistration, followed by the UPN suffix of your organization; for example, enterpriseregistration.contoso.com.

www.dbooks.org

Note Although this book is focused on SharePoint hybrid, it is worth noting that multiple services such as Microsoft Exchange federation services, autodiscover, and transport each require certificates. It is recommended that you contact the other Systems Administrators in your organization to coordinate the planning around consuming other Office 365 services such as Exchange hybrid and Workplace Join. For additional information, go to https://technet.microsoft.com/library/hh563848(v=exchg.150).aspx.

Server requirements

The following subsections describe the server roles and their requirements.

Note You can configure one server to have more than one role, depending on your current environment and planned future state.

Domain controllers

The domain controllers of all domains and forests must be available while running the IdFix tool. (The IdFix tool is be covered in more detail later in this chapter). Furthermore, these domain controllers will be queried when the synchronization process runs (every 30 minutes).

Domain controllers must run a minimum of 32-bit or 64-bit Windows Server 2003 Standard Edition or Enterprise Edition with Service Pack 1 (SP1). Because Windows Server 2003 is out of support, the next operating system version is 32-bit or 64-bit edition of the Windows Server 2008 Standard or Enterprise. All later Windows Server versions are supported.

Password write-back prerequisite

If you plan to use the password write-back feature, the domain controllers must be running Windows Server 2008 (with the latest service pack) or a later Windows Server operating system. Furthermore, if your domain controllers are pre-Windows 2008 R2, you must apply hotfix KB2386717 (http://support.microsoft.com/kb/2386717) to those domain controllers.

Note For users to be able to reset, unlock, and change their passwords with on-premises write-back, you must have an Azure AD Premium subscription.

Azure AD Connect server

You can install Azure AD Connect only on a 64-bit Windows Server 2008 (with SP4 and latest Windows updates) or later server version. If you plan to synchronize passwords, Azure AD Connect must be installed on Windows Server 2008 R2 SP1 or later. It cannot be installed on Windows Server Essentials or Small Business Server because they are unsupported operating systems for an installation of Azure AD Connect. The server level must be Windows Server standard or higher.

If you're using express settings, this server can be on a domain controller or a member server (joined to the same domain). However, there is no requirement for the server to be joined to a domain if you selected the Customize option for a custom setup.

Note To be able to query Active Directory, you need to ensure that certain ports are open for communication. For more information, see the section "Firewall" later in this chapter.

The Azure AD Connect server must have .NET Framework 4.5.1 or later and Microsoft PowerShell 3.0 or later installed. If the necessary prerequisites aren't already installed, Azure AD Connect will install them during its installation. The following are the software packages that are installed with Azure AD Connect:

- Windows Azure Active Directory Module for Windows PowerShell
- Microsoft Online Services Sign-In Assistant (no dependency on it)
- Microsoft SQL Server 2012 Command Line Utilities
- Microsoft Visual C++ 2013 x64 Redistribution package
- Azure AD Connect synchronization services
- Azure AD Connect Health agent for sync
- Microsoft SQL Server 2012 Native Client
- Microsoft SQL Server 2012 Express LocalDB (optional)

Organizations with a large number of AD objects (users, mail-enabled contacts, and groups) of 100,000 or more must install Azure AD Connect (customize settings) on its own SQL Server and it does not need to be on the same server as Azure AD Connect. For directories with lesser AD objects, this is optional because SQL Server installs its own SQL Express LocalDB.

The minimum hardware requirements are as follows:

Objects in AD	CPU	Minimum memory	Minimum hard drive size
Fewer than 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
For 100,000 or more objects the full version of SQL Server is required			
100,000–300,000	1.6 GHz	32 GB	300 GB

Note The preceding table was sourced from the *Hardware requirements for Azure AD Connect*. To read more about hardware requirements for Azure AD Connect, go to https://azure.microsoft.com/documentation/articles/active-directory-aadconnect-prerequisites.

If you plan to use multi-factor authentication, the URL https://secure.aadcdn.microsoftonline-p.com must be in the trusted sites list in the Azure AD Connect server's Internet properties, through group policy or manually, by adding it to the trusted sites in Internet Explorer 11.

AD FS Server

If you decide to configure a federated identity model for SSO, you must deploy AD FS. For AD FS, Windows Server 2012 R2 or later will be required. Older servers have older versions such as AD FS 2.0. Azure AD Connect has a built-in capability to configure AD FS remotely on a designated Windows 2012 R2+ server. You must turn on Windows Remote Management on the AD FS servers for remote installation. Because AD FS is a critical piece of infrastructure, consider deploying two AD FS servers (an AD FS farm) for high availability.

Earlier versions of AD FS ran on Internet Information Services (IIS) and required additional server resources. AD FS now runs on the kernel-based web service "HTTP.sys" and thus no longer requires IIS and additional resources. Smaller environments might choose to install AD FS on domain controllers. However, it is not possible to use Windows Network Load Balancing with domain controllers, so an

www.dbooks.org

external load balancer is required. For larger environments, the recommendation has not changed to install AD FS on dedicated services with high availability.

Alternately, you can host AD FS servers and Web Application Proxy servers in Microsoft Azure. It is easier to configure high availability in Microsoft Azure with availability set options for deployment. The minimum recommended Azure virtual machine (VM) for AD FS and Web Application Proxy servers are A2 configuration or higher.

Following are the minimum requirements for computers running AD FS:

- CPU: Dual core 1.6 GHz or higher
- Memory: 2 GB or higher

More info To view pricing on Azure VMs, go to https://azure.microsoft.com/pricing/details/virtual-machines

AD FS proxy server

The AD FS proxy is a service feature of the Web Application Proxy server role that is installed as part of the Remote Access server role in Windows Server 2012 R2 onward. In Windows Server 2008 R2 and Windows Server 2012, it was known as Federation Service Proxy and was installed as an AD FS role service.

An AD FS proxy or Federation Service Proxy functionality gives you the ability to publish the internal AD FS service to the outside world and should typically reside in your organization's perimeter network. The server you install the AD FS proxy does not need to be joined to the domain. It is not a requirement to install an AD FS proxy, but it is a good practice to include AD FS proxy servers when you are exposing your federation service to the Internet. It reduces the attack surface area and you can set up in a high availability configuration.

AD FS proxy via the Web Application Proxy server role is available with Windows Server 2012 R2 or later and can be any of the following server editions: Essentials, Standard, or Datacenter. You must install the Remote Access server role and then select the Web Application Proxy role service to turn on the AD FS proxy capability. AD FS is required to provide authentication and authorization services to AD FS proxy in the Web Application Proxy server role.

Typically, the AD FS proxy server has two network adapters configured. One adapter is configured to connect to the internal corporate network via a firewall or reverse proxy device. The second network adapter needs to be connected to an externally facing network.

Ideally, the external network adapter will be exposed to the Internet (to send and receive traffic). Optionally, the Web Application Proxy server could be placed behind a reverse proxy device for high availability and load-balancing purposes when there are two or more AD FS proxy (Web Application Proxy) servers.

The perimeter network should be behind an edge firewall for additional security.

Note HTTPS traffic (TCP port 443) must be allowed for outgoing and incoming traffic to the Web Application Proxy servers. The SSL Certificate used here would be called something along the lines of sts.contoso.com. ("sts" here being the acronym for Security Token Service.) You will need to create a public DNS A record to point to the reverse proxy publishing the Web Application Proxy. Port 443 is also required for device registration using Workplace Join. If you're planning to use the Workplace Join feature, an additional SAN is required with the value enterpriseregistration. followed by the UPN suffix of your organization, for example, enterpriseregistration.contoso.com.

The Web Application Proxy itself needs to be able to communicate back to the AD FS server(s) on the internal corporate network on TCP port 443.

Microsoft Identity Manager 2016 server

The older version of Microsoft Identity Manager 2016 was known as Forefront Identity Manager. Some tools and documentation might still refer to Forefront Identity Manager, such as *Forefront Identity Manager Connector for Windows Azure Active Directory*.

Large organizations with complex multiforest scenarios will need to consider planning with a full deployment of Microsoft Identity Manager 2016. Microsoft Identity Manager 2016 can be useful in non-AD environment user stores such as SAP HR, Oracle eBusiness, and PeopleSoft and can connect to custom systems such as SQL, Oracle, and MySQL.

Microsoft Identity Manager 2016 has a new and improved set of features for identity management, privileged access management, and synchronization, but we can't engage in a discussion about them here because it is beyond the scope of this eBook.

> **More info** For more information about the Forefront Identity Manager Connector for Windows Azure Active Directory, go to https://msdn.microsoft.com/library/dn511001(v=ws.10).aspx.
>
> To read about a feature comparison of the different directory integration tools, go to https://azure.microsoft.com/documentation/articles/active-directory-hybrid-identity-design-considerations-tools-comparison.

Network requirements

It is important to note that IP addresses within the Office 365 network are subject to change without prior notice. If your on-premises proxies or firewalls rules are configured using IP addresses, rather than domain names, outages will definitely occur if the Office 365 IP addresses change. Although this is extremely rare, Microsoft does provide notification of changes to prevent such issues.

For this reason, it is best to configure firewalls and proxies with domain names instead of IP addresses/IP network entries. You should try to work with routable domain names such as *.sharepoint.com, *.sharepointonline.com, *.microsoftonline.com, *.outlook.com, and *.lync.com.

> **Note** Some firewalls and reverse proxies do not recommend wildcard FQDN due to a DNS lookup limitation. It is recommended that you check with the vendors' documentation on the suggested configuration.

Reverse proxy

Reverse proxy devices are required for the on-premises SharePoint farm to achieve high availability and traffic load balancing. With load balancing, administrators have the ability to distribute traffic across two or more servers to equally balance traffic. It allows web servers to scale out by adding additional web servers to the load-balanced pool as workloads increase.

Additional functionality includes traffic management, SSL acceleration, and compression, depending on the brand of reverse proxy you select.

A hardware or software reverse proxy providing load-balancer capability is required to achieve high availability with the AD FS SSO servers and Web Application Proxy servers. You also must have reverse proxies if you plan to publish and load-balance in SharePoint hybrid scenarios such as SharePoint on-premises and optionally the Office Online Server (successor to Office Web Applications).

Windows Network Load Balancing has been available as a feature in Windows Server operating systems since Windows NT 4. NLB is available in Windows Server 2016. You should contact your

www.dbooks.org

network administrators to find out what load-balancing solutions your organization currently has in place. It is advisable to consider compatibility and other implications of implementing Network Load Balancing in your environment.

The key definition of a proxy that can be used to support a SharePoint hybrid topology is compliance with RFC2716. Other popular reverse proxy brands are:

- F5 BIG-IP
- NGINX
- Blue Coat ProxySG
- Cisco ACE

WAN accelerators

If your organization has a branch office and uses wide-area network (WAN) acceleration proxy appliances, users might encounter issues when they attempt to access the Office 365 services. You might need to optimize your network device or devices to ensure that your users have a consistent experience when accessing Office 365. For example, Office 365 services encrypt some Office 365 content and the TCP header. Your device might not be able to handle this kind of traffic. You should contact the appliance vendor for optimization solutions.

Firewall

There are a number of firewall rules that need to be planned carefully to ensure a fully functional SharePoint hybrid experience.

There are different groups of firewall rules specified on the Office support site. The Office 365 documentation is clear about the required and optional rules. Thus, firewall rules contained in the Office 365 documentation are not duplicated here. However, we will discuss additional firewall configuration rules and considerations. The following firewall rule groups are specified in the documentation:

- Office 365 portal and shared

  Contains rules to access essential Office 365 and Azure resources, including Content Delivery Networks (CDNs) locations.
- Office 365 authentication and identity

  Contains rules for Azure AD Connect, AD FS (optional), and AD FS Web Application Proxy (optional).
- SharePoint Online

  Contains rules to access SharePoint online and CDNs.
- Other rule groups such as Exchange and Skype for Business

More info To read more about the Office 365 URLs and ports for your firewall configuration, go to https://support.office.com/article/Office-365-URLs-and-IP-address-ranges-8548a211-3fe7-47cb-abb1-355ea5aa88a2.

The following ports must be opened to the domain controller or LDAP directory from the server/desktop running the IdFix tool:

Protocol	Port	Traffic type
TCP	3268	LDAP global catalog
TCP and UDP	389	LDAP
TCP	636	LDAP SSL

Additionally, ensure that the server that runs Azure AD Connect is allowed outbound connections over TCP port 443 and outbound connections to https://ssprsbprodncu-sb.accesscontrol.windows.net.

For proxy or general connectivity issues, allow outbound connections over TCP ports 9350 to 9354.

More info To learn more, read the Azure AD Connect reference, available at https://azure.microsoft.com/documentation/articles/active-directory-aadconnect-ports.

IPv6 considerations

Not all Office 365 features have full IPv6 support. ExpressRoute for Office 365 currently does not support IPv6; however, this is subject to change in the future. Turning off IPv6 is also not recommended. This means that you must use both IPv4 and IPv6 to connect to Office 365. Work is underway at Microsoft to make Azure fully IPv6 capable. As of this writing, there is no date confirmed when full IPv6 support will be generally available. (To learn more, go to https://azure.microsoft.com/pricing/faq.)

More info This test plan is recommended for all Enterprise and Government SKUs. To learn more about IPv6 connectivity to Office 365 testing, go to https://www.microsoft.com/download/details.aspx?id=37135.

For information about IPv6 support in Microsoft products and services, go to https://technet.microsoft.com/network/hh994905.aspx.

For additional information about IPv6 for Microsoft Windows and FAQs, go to http://go.microsoft.com/fwlink/p/?LinkId=325418.

Client application preparation

Microsoft's supported browser for Office 365 is Microsoft Edge and Internet Explorer 11. Microsoft Edge browser updates are available through the Windows servicing branches. To get the best experience out of Office 365, it is recommended that you work with the latest branch of the Edge browser.

More info For a list of known issues when connecting to SharePoint Online and OneDrive for Business from the Edge browser, go to http://go.microsoft.com/fwlink/p/?LinkID=627569.

For non-Microsoft web browsers, Microsoft generally supports only the current versions of Safari, Chrome, and Firefox. Microsoft will not support browsers that are not supported by the vendors themselves.

More info For software requirements for Office 365 plans for business, education, and government, go to https://products.office.com/office-system-requirements.

www.dbooks.org

The following websites must be in your Internet Properties Trusted Sites zone:

- https://*.sharepoint.com
- https://<tenant>.sharepoint.com
- https://<tenant>-files.sharepoint.com
- https://<tenant>-my.sharepoint.com
- https://<tenant>-myfiles.sharepoint.com

To add these sites on a single desktop, go to Control Panel, and then, in the Search Control Panel, type **internet**. In the Internet Options section, click Change Security Settings, click Trusted Sites, and then click Sites, as shown in Figure 4-6.

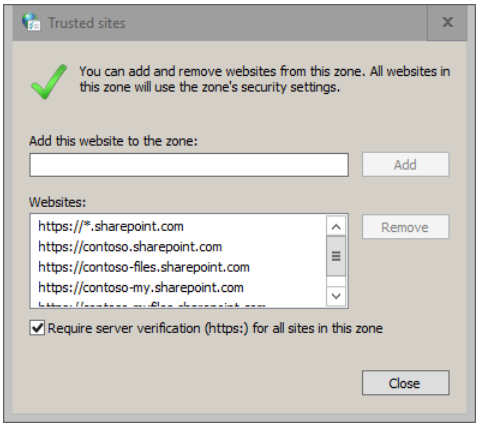


Figure 4-6: Trusted sites to be added in Internet properties.

SharePoint on-premises requirements

If you are looking at implementing the cloud search service application, the following versions of SharePoint are the minimum requirements:

- SharePoint Server 2016 RTM, build version 16.0.4351.1000
- SharePoint Server 2013 September 2015 public update (PU), build version 15.0.4753.1001

It is recommended to test with the latest cumulative update (CU) without known regressions.

> **More info** For the hardware and software requirements of SharePoint Server 2016, go to https://technet.microsoft.com/library/cc262485(v=office.16).aspx.

IdFix DirSync Error Remediation Tool

You use IdFix to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for synchronizing identities to Azure AD. The purpose of IdFix is to identify and optionally remediate Active Directory object issues that will fail the Azure AD Connect synchronization. It produces results in a data grid in which administrators are able to sort and edit entries directly within the tool. IdFix keeps a log of its changes, so it has an undo/rollback functionality.

IdFix reduces the time involved in remediating synchronization errors reported by Azure AD Connect. It supports both multitenant and dedicated rule sets. Most Office 365 customers are multitenants and this is the default option preselected when you first run the IdFix tool.

Note To download IdFix, go to http://go.microsoft.com/fwlink/?LinkId=321122. You can also download the tool from within the directory synchronization management page in the tenant admin site.

Supported operating system

To run IdFix, you need to meet certain hardware and system requirements.

Hardware requirements

You can run the IdFix tool on a domain controller or a member server or desktop that is part of a domain. Because it runs under the signed-in user's identity, it is necessary for the user to have access to view all objects in the Active Directory OU that is being planned for synchronization.

The server should meet the following specifications at a minimum:

- 4 GB RAM (minimum)
- 10 GB of drive space (minimum)

System requirements

- **Operating System** Windows Server 2008 R2 + and Windows 7 for x64-bit versions.
- **Active Directory** Queries are via native LDAP and have been tested with Windows Server 2008 R2, but all versions should be expected to work.
- **Exchange Server** The messaging attributes retrieved are version-independent and should work with Exchange 2003 or later.
- **.Net 4.0** Must be installed on the workstation/server running the application.
- **Permissions** By default, the application runs in the context of the authenticated user, which means that it can query another forest, provided that you supply the correct credentials to the application that it has rights to read the directory of the other disparate forest. If you want to apply changes to the directory, the authenticated user needs write permission to the desired objects. With IdFix, you can change the credentials to perform these operations.

Note This information was sourced from the IdFix download page, *System Requirements* section, which you can find at https://www.microsoft.com/download/details.aspx?id=36832&e6b34bbe-475b-1abd-2c51-b5034bcdd6d2=True.

IdFix collects data from your corporate network and can optionally store data that might contain personal information in a Comma-Separated Value (.csv) or LDAP Data Interchange Format (.ldf) file located on the computer on which the program was run, as depicted in Figure 4-7. Microsoft recommends that you remove this file when you have completed your use of the program.

www.dbooks.org

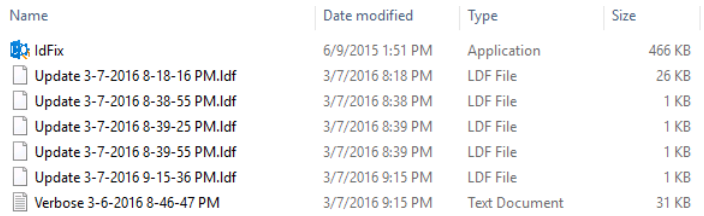


Figure 4-7: LDAP Data Interchange Format (.ldf) files created in the same folder from which IdFix was run.

Operating the IdFix tool

After you download the IdFix tool, copy it to a supported server/desktop, start it, and then, in the upper-right corner of the window, click the settings button (the small gear icon). This opens the Settings dialog box (see Figure 4-8), in which you can review the the tool's setup. You can specify multiple domains in a forest or even multiple forests here.

Because the Azure AD Connect tool can selectively synchronize specific OUs, you can specify the OU that contains the users who you plan to synchronize with Office 365.

Other LDAP directories can be searched, and the credentials will be in the format those directories understand. The default port is 389 because it is used for write-back purposes.

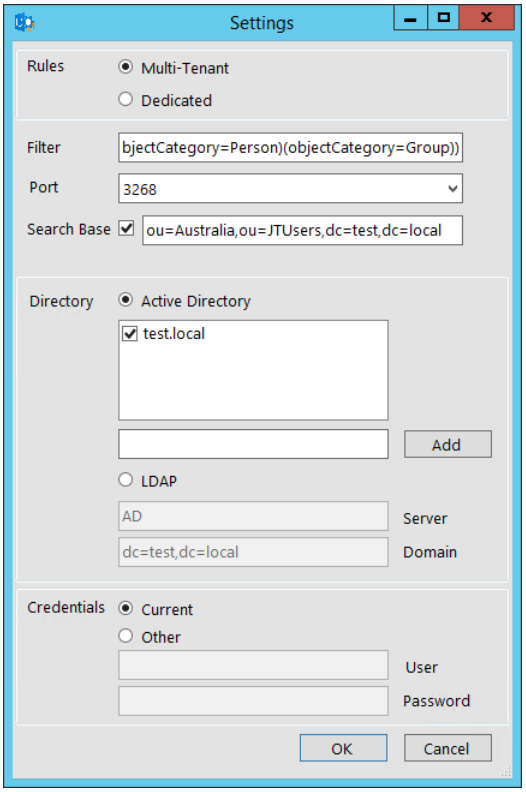


Figure 4-8: The IdFix tool settings with Search Base selected and specifically looking at users from the Australia OU.

Click OK to open the IdFix error report dialog box, and then, on the menu bar, click Query to start the discovery process, establish an LDAP connection, and generate a report on objects that contain errors. If you open the tool without identifying a specific OU, it will query the entire directory.

Figure 4-9 shows that the tool reported five objects with errors.

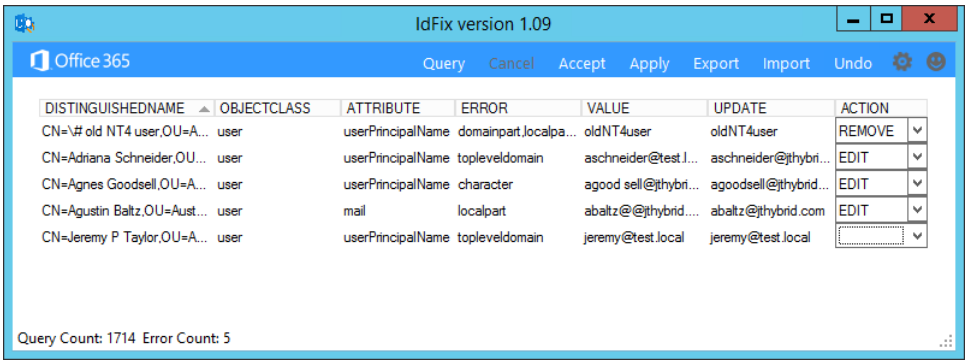


Figure 4-9: IdFix reported five objects with errors

You can act on the errors by selecting any of the following:

- **Accept** Accept all suggested updates (in the Update column).
- **Apply** Apply selected actions.
- **Export** Export the output of the IDFix tool to a CSV file. You can use this to correct the error objects in Windows PowerShell. For example: Get-Content - Set-ADUser.
- **Import** Import if you want to continue from where you left off without querying the domain or if you prefer to modify anything and get the tool to update.
- **Undo** Load update file to Undo.

In the Update column, you can type a change directly into the field and then select Edit as the action, then click Apply to update it.

More info For more information on running the IdFix tool, go to https://support.office.com/article/Prepare-directory-attributes-for-synchronization-with-Office-365-by-using-the-IdFix-tool-497593cf-24c6-491c-940b-7c86dcde9de0.

Note There is a detailed IdFix Guide included with the IdFix tool download. To download the Guide and IdFix tool, go to https://www.microsoft.com/download/details.aspx?id=36832.

You can send bug reports and desired feature request to IdFixSupport@Microsoft.com.

Directory auditing

With a hybrid environment, organizations might want to log and review the events that are associated with directory synchronization. Auditing can be turned on on-premises, and administrators can evaluate events such as user creation, password reset, adding users to groups, and so on, as demonstrated in Figure 4-10. Auditing captures directory services logs from the Active Directory domain controllers. It is recommended to discuss auditing and reporting solutions currently in place in your organization.

More info To learn more about turning auditing for an on-premises Active Directory, go to https://technet.microsoft.com/library/cc731607(v=ws.10).aspx.

To learn more about viewing reports in Azure AD, go to https://azure.microsoft.com/documentation/articles/active-directory-view-access-usage-reports.

www.dbooks.org

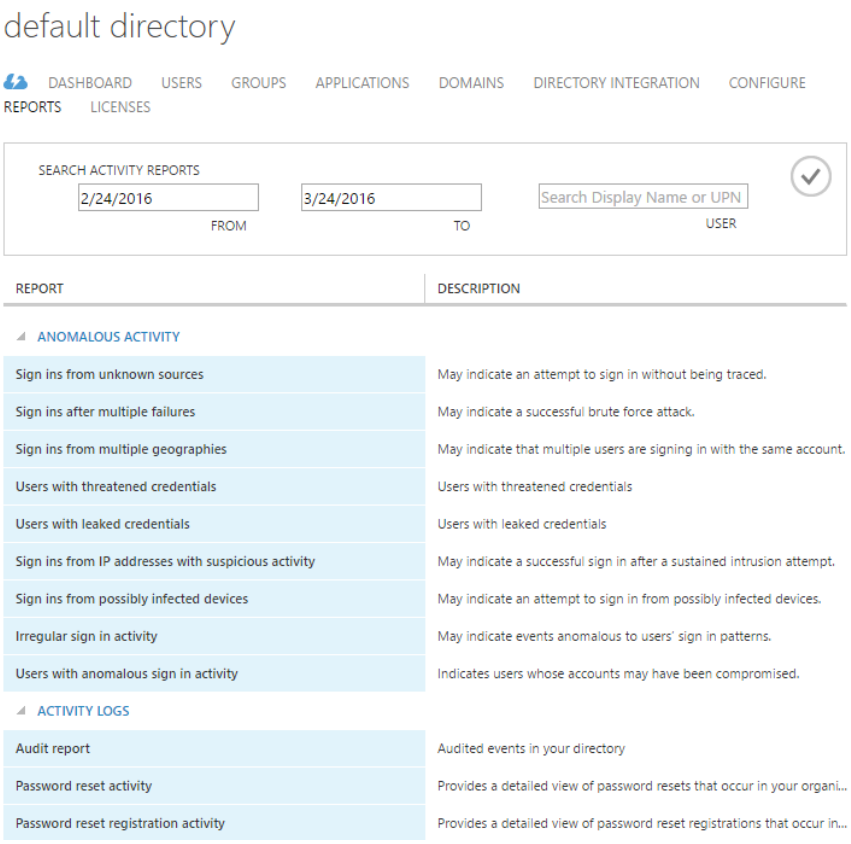


Figure 4-10: Azure AD reports for auditing.

Capacity planning

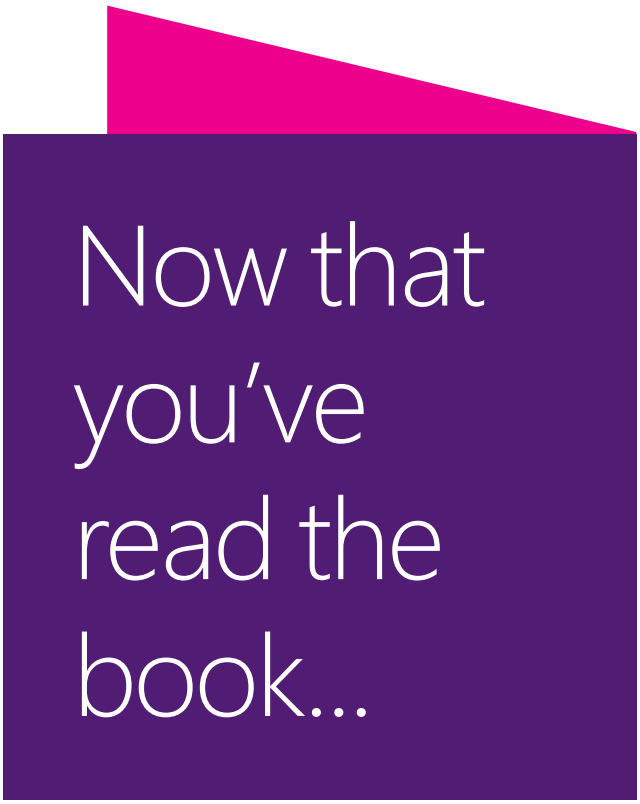
There are many considerations when planning for scale. Large organizations are advised to know the service limits of Microsoft Azure, Office 365, on-premises applications and the tools needed to support them.

Azure AD Connect requires a full instance of Microsoft SQL Server (Standard edition, SQL Server 2008 onward) installation for forests of more than 50,000 objects. For smaller businesses, the Windows Internal Database is sufficient and is installed by default.

Azure AD will by default accommodate 50,000 objects without a verified domain name but that limit is increased to 500,000 objects after a domain name is verified. If you need more objects synchronized in Azure AD, you need to open a support case with Microsoft to have that limit increased.

The Free edition of Azure AD accommodates a maximum of 500,000 objects.

> **More info** For more information on Azure service limits and quotas, go to https://azure.microsoft.com/documentation/articles/azure-subscription-service-limits/#active-directory-limits.



Tell us what you think!

Was it useful?
Did it teach you what you wanted to learn?
Was 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

www.dbooks.org

CHAPTER 5

Synchronizing users to the cloud

This chapter helps you to plan for directory synchronization to Microsoft Azure Active Directory (Azure AD), which Microsoft Office 365 uses for authentication and identity management. Chapter 4 covered the infrastructure requirements of Azure AD Connect for Active Directory identity cleansing. This chapter focuses on the configuration of Azure AD Connect specific to synchronized identities with password synchronization and the options you have when setting up the tool. Users will be able to sign in to the cloud using the same password as their on-premises account. This chapter discusses the configuration of directory synchronization with Azure AD Connect which is used as a prerequisite for Chapter 6 (federated identities, single sign-on), which builds on the knowledge that you will gain from this chapter.

Directory synchronization

The term *directory* refers to the shared information resource for creating, managing, and organizing network resources such as users, groups, devices, and so on. The term *on-premises directory* refers to Active Directory, a familiar name to most IT professionals. The term *Azure AD* refers to the cloud-based directory that contains users, groups, devices, and so forth that Office 365 uses for its own authentication and authorization requirements. A synchronization tool is required to replicate on-premises Active Directory users with Azure AD. Azure AD itself is a partitioned directory service for Office 365, wherein each Office 365 tenant has access to its own Azure AD group and user identities. In June 2015, Microsoft released Azure AD Connect which was a newer release of Azure AD Sync with many additional capabilities such as the ability to configure Active Directory Federation Services (AD FS) and AD FS proxies.

Azure Active Directory Sync

Azure Active Directory Sync—widely known as "DirSync"—was the first tool publically released to synchronize on-premises identities to Azure Active Directory. DirSync installed and relied on Forefront Identity Manager (FIM) as its synchronization engine. However, DirSync had limitations such as no multiforest synchronization, no attribute filtering, no AD FS configuration, and so on. DirSync is now deprecated and there are no future releases planned. If your organization is running DirSync, you should be able to upgrade to Azure AD Connect in-place if the synchronized directory objects (users, contacts, and groups) is less than 50,000., If you're installing Azure AD Connect on the same server as DirSync, Azure AD Connect has functionality to read an existing DirSync configuration and perform an in-place upgrade.

Azure AD Sync

Azure AD Sync (now discontinued) was released after DirSync because it had some enhanced features such as multiforest identity synchronization. It was retired in June 2015 when Azure AD Connect was released.

You can upgrade Azure AD Sync to Azure AD Connect if you install Azure AD Connect on the same server (in-place upgrade). Azure AD Connect has the ability to read the Azure AD Sync configuration and perform an in-place upgrade.

Azure AD Connect

Azure AD Connect is a feature-rich software tool compared to its predecessors. Its hybrid deployment capabilities include a robust directory synchronization engine and configuration of AD FS in a single wizard. It has the ability to perform in-place upgrades from older tools and password hash synchronization for synchronized identities. It can optionally configure AD FS and AD FS Web Application Proxy servers, depending on the sign-on option (identity model) that you choose.

For synchronization, Azure AD Connect uses Microsoft Azure AD Connect synchronization services, which is Microsoft Identity Manager (MIM) 2016 behind the scenes, as illustrated in Figure 5-1. If you're a SharePoint administrator, you might be familiar with troubleshooting on-premises SharePoint user profile synchronization errors with the help of a client application (miisclient.exe) to view FIM synchronization. The miisclient.exe tool still exists in MIM 2016 and still helps troubleshoot those synchronization issues.

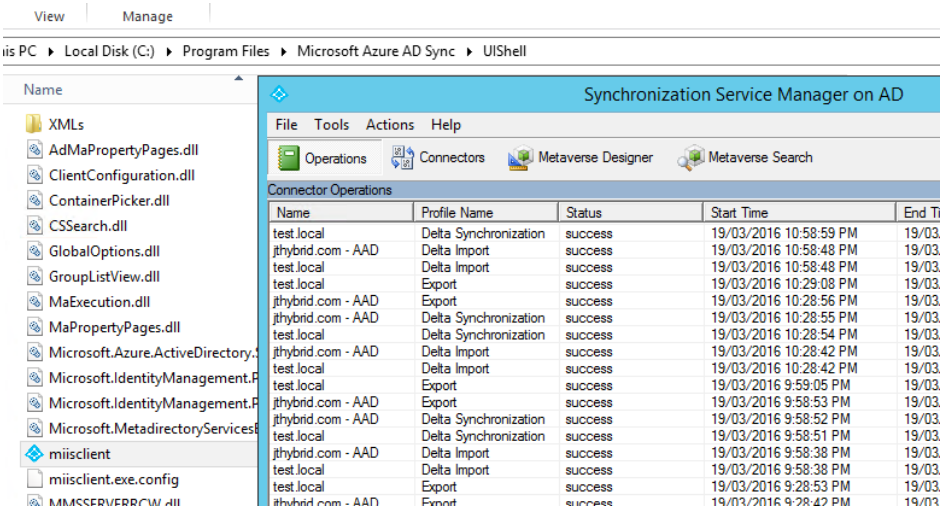


Figure 5-1: Microsoft Identity Manager is the synchronization engine for Azure AD connect.

www.dbooks.org

Note In this book, we focus on Azure AD Connect. MIM 2016 is beyond the scope of this discussion.

MIM 2016

MIM 2016 makes it possible for organizations with more complex and custom requirements to synchronize users to the cloud, typically in a federated identity model because MIM does not accommodate password synchronization. With MIM, you can synchronize multiple on-premises Active Directory, non-Microsoft directories, Lightweight Directory Access Protocol (LDAP), and custom repositories.

More info To read a comparison of hybrid identity directory integration tools, go to https://azure.microsoft.com/documentation/articles/active-directory-hybrid-identity-design-considerations-tools-comparison.

Azure AD Connect preparation

To install and configure Azure AD Connect, you need to do the following for a synchronized identity setup (federated identity model is discussed in detail in Chapter 6):

- Fix all issues by using IdFix
- Determine the immutableID
- Plan Active Directory attributes to be synchronized
- Verify domain name with Office 365

You also need to have the following installed and/or set up:

- Azure AD Connect server (High Availability options, discussed in Chapter 6)
- Enterprise Admin account
- Domain Admin account
- Azure AD Connect service account
- Microsoft SQL Server for installations over 100,000 directory objects (users, groups and contacts)
- Office 365 subscription (or trial). It includes Azure AD basic
- Azure AD tenant (optional) to manage Azure resources and consume Azure Cloud Services through the portal
- Global Administrator credentials for Office 365 or Azure AD with the initial domain name, onmicrosoft.com; for example, jtaylor@contoso.onmicrosoft.com

Domain verification

Ensure that your domain is added and verified in Office 365 using the DNS configuration information provided in the Office 365 Admin Center.

Figure 5-2 shows a domain selected (contoso.com). To see the required DNS configuration, in the pane on the right, click Domain Settings. You also can click Find And Fix issues to assist you in verifying your domain's DNS configuration.

Note Chapter 4 discusses the DNS setup and provides a link to the step-by-step instructions for popular DNS hosting providers.

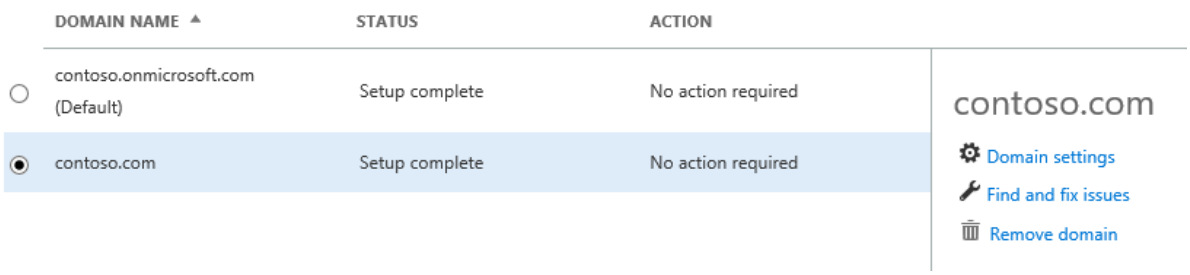


Figure 5-2: Find and fix issues regarding your domain name.

Cloud user ID verification

Before you commence any synchronization activities, it is best to verify whether there are any user identities already created in your Office 365 or Azure AD tenant. If there are cloud identities created, switching on directory synchronization will not affect them unless there is a Simple Mail Transfer Protocol (SMTP) match, where the primary SMTP address is used to match the on-premises user account to the Office 365 user account. Directory synchronization will be blocked for users with an SMTP and UPN clash.

Note Refer to Chapter 3 for information on planning the source of authority for identity mastering.

IdFix cleanup

You would need to ensure that that IdFix does not report on any duplicate objects. You can choose to fix issues manually or through Windows PowerShell. After you have set up and verified your domain and fixed issues with IdFix, you need to look at getting into the core of user synchronization configuration. For an overview on cleaning up identities reported by IdFix, refer to Chapter 4.

Activate Directory synchronization

You will need to activate the Active Directory synchronization capability in your Office 365 subscription by performing the following steps:

1. Sign in to the Office 365 Admin Center as a Global Administrator.
2. In the pane on the left, in the Users section, click Active Users.
3. In the pane on the right, adjacent to Active Directory Synchronization, click Manage, as illustrated in Figure 5-3.

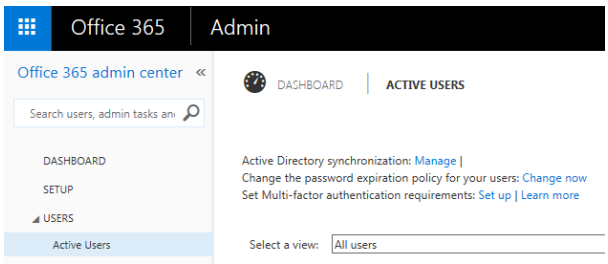


Figure 5-3: Click Manage to activate your subscription for directory synchronization.

www.dbooks.org

This takes you to the Directory Synchronization page, where you can see the current state of the directory synchronization set up and the tools with which you can synchronize users to Office 365.

4. Click Activate.

Figure 5-4 shows that the Directory Sync Status has been activated but Last Directory Sync is blank, indicating that synchronization hasn't yet taken place.

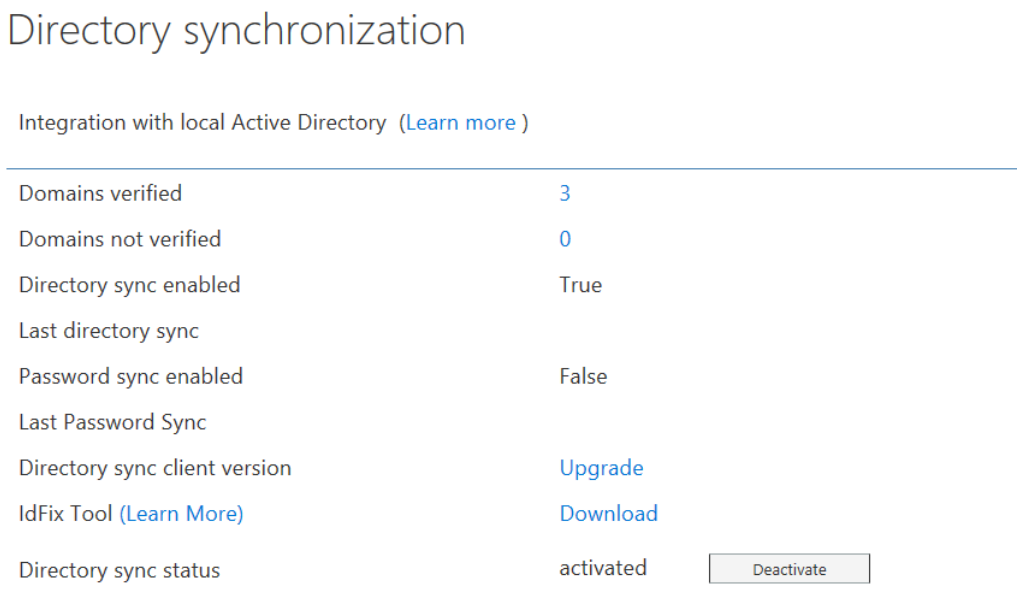


Figure 5-4: Last Directory Sync and Last Password Sync do not contain any information yet. Directory Sync Status has been activated.

It is on this page that you can activate or deactivate Directory Sync and download the IdFix tool and the "Directory sync" client: Azure Active Directory Connect. Deactivating directory sync can take up to 72 hours to complete, hence I do not recommend that you do this unless it's absolutely necessary. An example of the need to do so would be a business migrating to a cloud-only identity model. The other scenarios are when mergers and acquisitions take place where multiple tenants merge together or splits occur by the exiting entity.

You also can activate and deactivate directory synchronization from Azure AD:

1. In the Office 365 Admin Center, in the Admin section, click Azure AD.
2. Select the Default Directory.
3. Click Directory Integration.

The Integration With Local Active Directory page opens, on which you can turn on or turn off Directory Sync, as depicted in Figure 5-5.

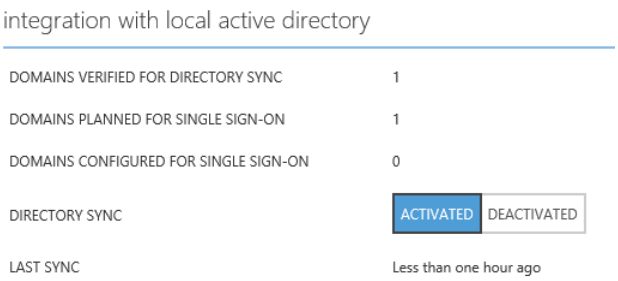


Figure 5-5: You can activate or deactivate from the Azure AD management page.

Password write-back

You can use the password write-back feature to reset your password in the cloud, and the updated password is written back to the on-premises directory. To take advantage of this feature, you must have an Azure AD premium subscription and the license must be assigned to the users requiring password write-back. A 30-day trial of Azure AD premium is also available.

> **More info** To learn more about password write-back, go to https://azure.microsoft.com/en-us/documentation/articles/active-directory-passwords-learn-more/#what-data-is-used-by-password-reset.

Users need to register an alternate email address or mobile phone to be able to reset their password. Alternatively, administrators can prepopulate this information via Windows PowerShell. To register for password reset, go to https://account.activedirectory.windowsazure.com/profile.

> **Note** You can configure alternate email and phone settings easily by using Azure PowerShell. To do so, you will need to download and install the Azure PowerShell Module at https://msdn.microsoft.com/library/azure/jj151815.aspx#bkmk_installmodule

Active Directory permissions required

To obtain the permissions required for password write-back, perform the following steps:

1. Using an account that has the appropriate domain administration permissions, open Active Directory Users And Computers.
2. In the View Menu option, ensure that Advanced Features is turned on.
3. In the left pane, right-click the object that represents the root of the domain.
4. Click Properties, click the Security tab, and then click Advanced.
5. On the Permissions tab, click Add.
6. Click Select A Principal. Lookup the account to which you want to give permissions (this is the same account that was specified while setting up Azure AD Connect; for example, TEST\AADConnect).
7. On the drop down menu at the top, select Descendent User Objects.

www.dbooks.org

8. In the Permission Entry dialog box that opens (see Figure 5-6), select the check boxes for the following:

    a. Change Password

    b. Reset Password

    c. Write lockoutTime

    d. Write pwdLastSet.

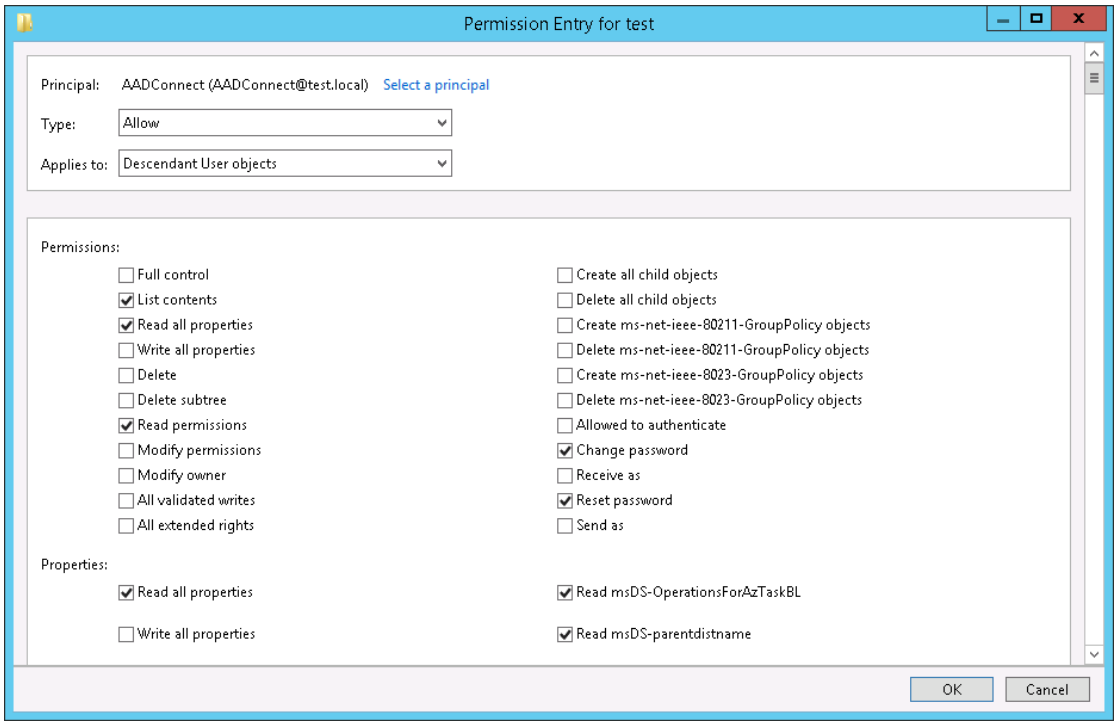


Figure 5-6: Selecting the required permissions for the AADConnect service account to turn on password write-back to on-premises Active Directory.

9. Click Apply/Ok through all of the open dialog boxes.

10. Close the Active Directory Users And Computers MMC Snap-in.

More info To read more detail about configuring users to reset their passwords, including password write-back, go to https://azure.microsoft.com/documentation/articles/active-directory-passwords-getting-started/#enable-users-to-reset-their-azure-ad-passwords.

Azure AD Connect configuration

Before configuring Azure AD Connect, ensure that you have read Chapter 4, which covers the server requirements for Azure AD Connect and Active Directory attribute cleansing with the help of IdFix. You must fulfil these requirements before you can continue on here.

To download Azure AD Connect, go to https://www.microsoft.com/download/details.aspx?id=47594.

When you run the Azure AD Connect executable file, it will install its prerequisites. When this is done, the Azure Active Directory Connect Wizard opens to guide you through the entire configuration process. Figure 5-7 shows the Welcome page. Note that this wizard will dynamically change depending on your selections. The synchronization process will not begin until you have gone through each of the wizard's pages (and if staging has not been selected).

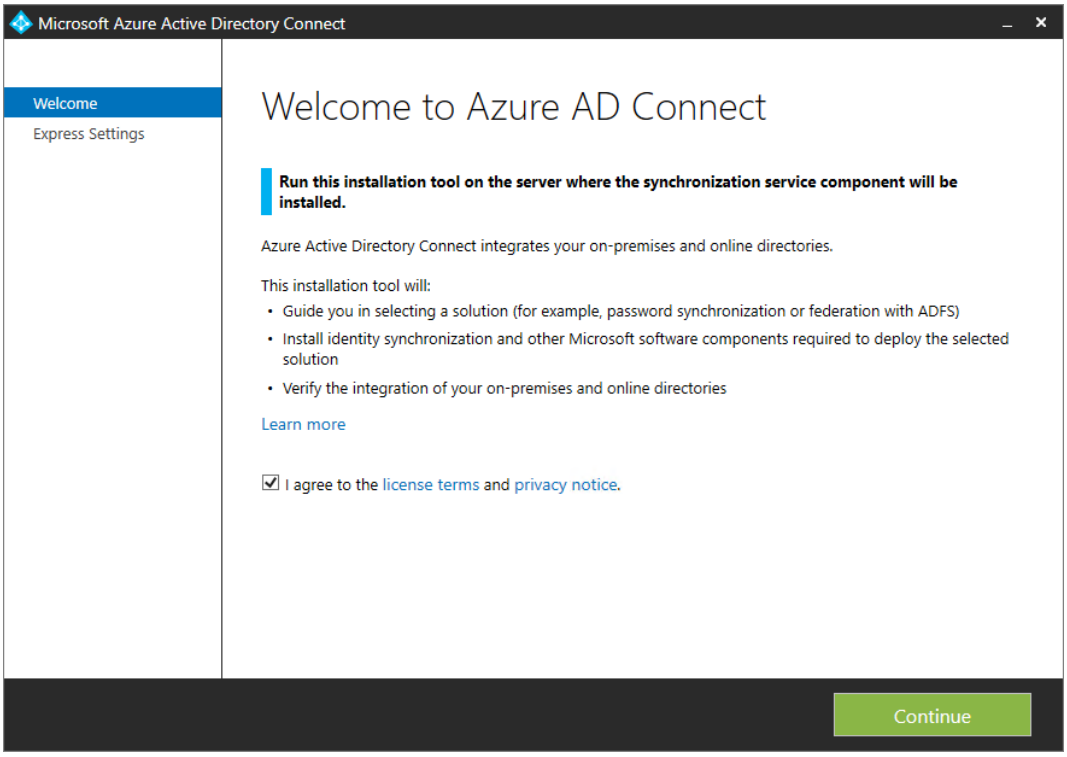


Figure 5-7: The Azure AD Connect installation tool welcome screen.

If you are synchronizing a small directory, a test/trial, or proof of concept environment, you can choose Express Settings. As Figure 5-8 depicts, this synchronizes all Active Directory attributes from one Active Directory forest, installs its own SQL Express LocalDB on the server, but does not allow you to configure an AD FS federated identity model. Express Settings also configures the synchronized identities with password hash synchronization, and it turns on automatic updates to Azure AD Connect by default (you can turn it off by using Windows PowerShell, which I explain later in this chapter).

www.dbooks.org

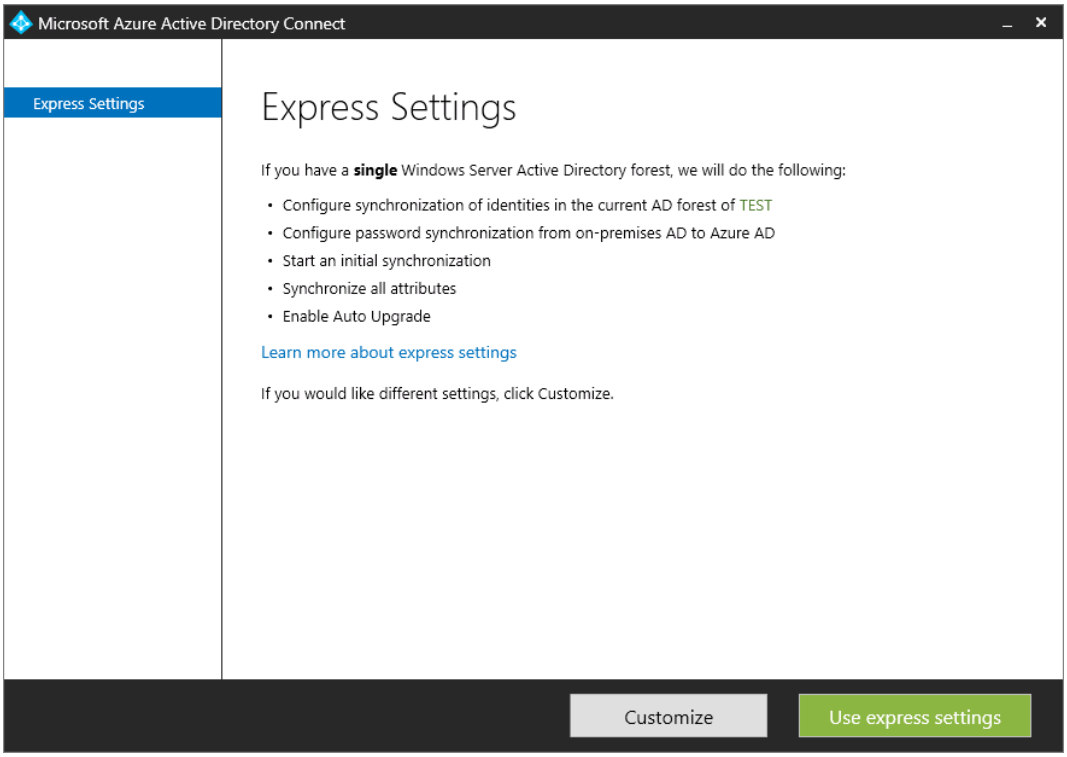


Figure 5-8: Azure AD Connect Express Settings.

> **More info** To read more about Azure AD Connect using express settings, go to http://go.microsoft.com/fwlink/?LinkID=391993.

If Azure AD Connect does not find an existing synchronization service, it presents four optional configuration choices, as demonstrated in Figure 5-9.

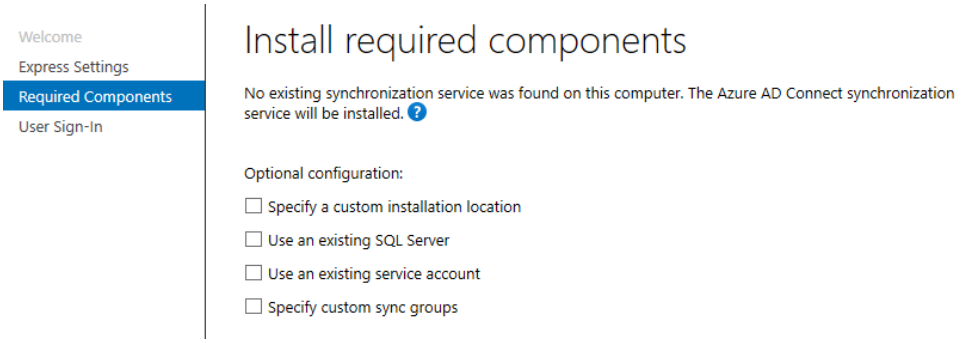


Figure 5-9: The required components for an Azure AD Connect installation with optional configuration choices.

The optional configurations are as follows:

- **Specify A Custom Installation Location** Use this to specify an installation location other than the default. By default, Azure AD Connect installs to C:\Program Files\Microsoft Azure AD Sync.
- **Use An Existing SQL Server** This is recommended for database management and required for directories with more than 100,000 objects (users, groups, and contacts).

- **Use An Existing Service Account** Use this to specify a dedicated service account, such as Contoso\AADConnect. This service account will run the synchronization service and will be configured with Replicate Directory Changes permissions in Active Directory.
- **Specify Custom Sync Groups** These groups are local to the Azure AD Connect server but not Active Directory domain groups, unless you install Azure AD Connect on a domain controller. You can choose to precreate these groups if you want and configure this option to use them. If you don't select this option, Azure AD Connect will automatically create four local groups on the server on which you are running Azure AD Connect installation:
  - **Administrators Group** ADSyncAdmins

    Azure AD Connect creates a Directory synchronization service account, a local user named something similar to AAD_762ec736ff66, and then adds this user to the ADSyncAdmins local group.
  - **Operators Group** ADSyncOperators
  - **Browse Group** ADSyncBrowse
  - **Password Reset Group** ADSyncPasswordSet

On the next wizard page, you need to choose the user sign-in method. Your options are Password Protection, Federation With AD FS, and Do Not Configure. This chapter is specific to password synchronization (synchronized identities), so select Password Synchronization, as illustrated in Figure 5-10. If you are planning to integrate with an existing AD FS farm and Web Application Proxy servers or a third-party federation solution like Shibboleth, you should choose Do Not Configure.

Note Selecting Federation With AD FS will proceed to configure federated identities. Chapter 6 continues from selecting this option. Federated identities are covered in detail in Chapter 6.

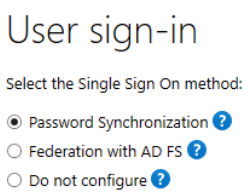


Figure 5-10: Select Password Synchronization for synchronized identities.

The next step connects to your Azure AD tenant. You receive Azure AD free as part of your Office 365 subscription. You will need to sign in as a global administrator account of the Office 365 subscription. This must be an account with the onmicrosoft.com domain; for example, jtaylor@contoso.microsoft.com.

On the Connect Your Directories page, you link Azure AD Connect to your on-premises directories or forests. The credentials supplied here will be used as the AD management agent account that reads and optionally writes to the directory in that forest (depending on the optional write-back features you require). The default domain user permission is sufficient for read-only purposes, but I recommend planning to use a dedicated service account for this because our goal is to achieve synchronized identities with password synchronization.

Password synchronization requires that this service account has the following permissions:

- Replicate Directory Changes
- Replicate Directory Changes All

www.dbooks.org

The following are the optional features that require write-back permissions:

- Exchange hybrid deployment
- Password write-back
- Device write-back
- Group write-back

> **More info** To learn more about the permissions required for these features, go to https://azure.microsoft.com/documentation/articles/active-directory-aadconnect-accounts-permissions/#create-the-ad-ds-account.

To connect to additional forests, you must provide the fully qualified domain name (FQDN) of the forest and the full FQDN of the internal domain name. For example, for the forest fabrikam.com, the internal FQDN name is FABRIKAM.local. You will need to provide user name, which will be similar to FABRIKAM.local\<sAMAccountName>.

> **Note** When you install Azure AD Connect, the account you specify on the Connect Your Directories page must be present in Active Directory and have the required permissions granted. The installation wizard will not verify the permissions, and any issues will be found only during synchronization.

Next, you need to configure domain and Organizational Unit (OU) filtering. You can change this at any time in the future. You can select all domains and OUs or only certain among them, as shown in Figure 5-11.

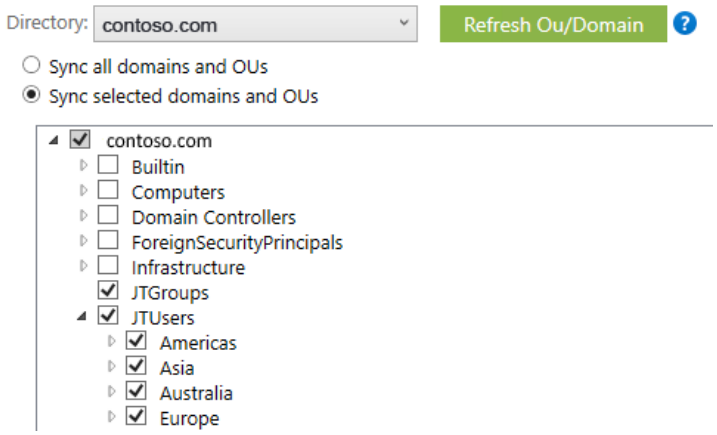


Figure 5-11: Domain and OU filtering.

On the next wizard page (see Figure 5-12), you configure how your users will be identified across your organization's on-premises directories.

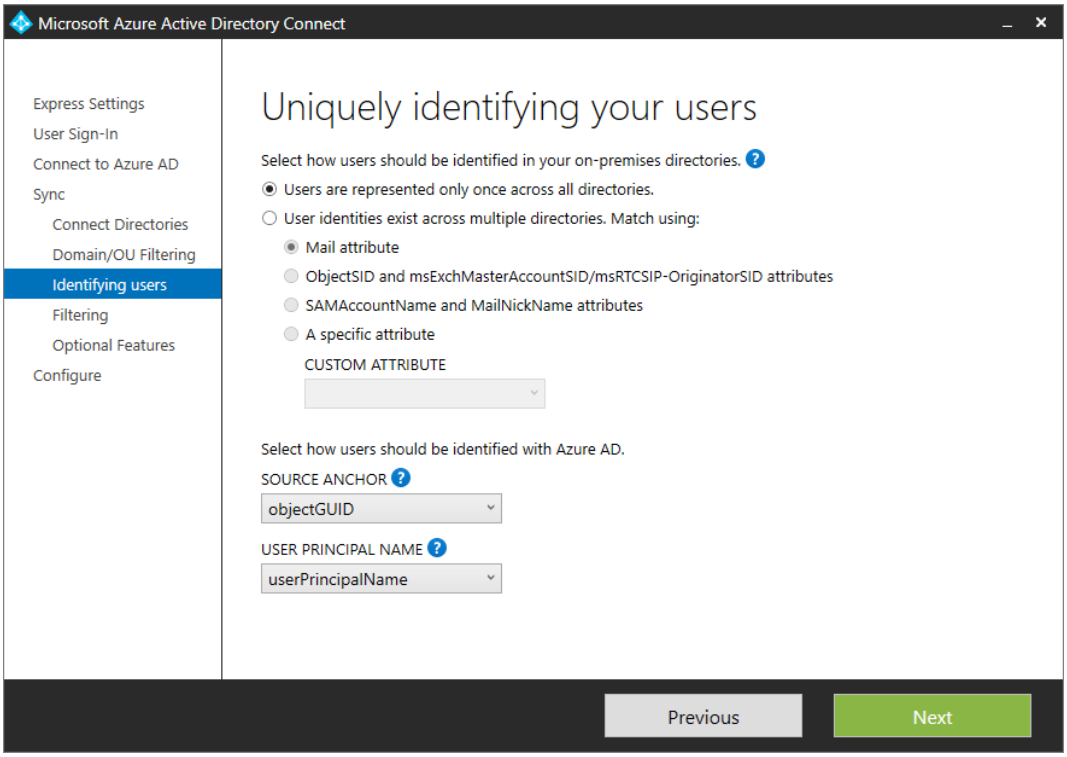


Figure 5-12: Uniquely identifying your users in your own on-premises directory and Azure AD.

The default setting, Users Are Represented Only Once Across All Directories, assumes that there are no duplicate representations of users in your environment (single or multiforest). If you have multiple directories or forests, there exists a possibility that an object might exist in multiple directories or forests. For example, a user in one forest might be a contact in another forest. If this is the case in your organization, select User Identities Exist Across Multiple Directories. You would then need to match (join) the objects with a certain attribute across these directories or forests to synchronize into Azure AD. You have four options here: Mail, ObjectSID, SAMAccountName, or you can specify a custom attribute. In most cases, the Mail option applies.

Further down on this page, you select how your users should be identified in Azure SD. Here are the options:

- **Source Anchor** The attribute sourceAnchor is one that does not change during the lifetime of a user or object. It is also known as immutableID because you are unable to change it in the future. It is considered to be the primary key linking an on-premises user to the synchronized user in Azure AD. Planning the selection of a good sourceAnchor is discussed in Chapter 3.
- **UserPrincipalName** Use this attribute for authentication in a hybrid cloud environment. The domain used (UPN-suffix) must be the verified domain in Azure AD. I strongly recommend that you keep the default attribute userPrincipalName. If you are planning to use an alternative attribute to user principal name, refer to Chapter 3 for additional information and guidance.

On the Filtering page, you can choose to filter users and devices based on an on-premises AD Group membership. This is initially best suited for a pilot hybrid cloud proof-of-concept for a small group of users. The default Synchronize All Users And Devices synchronizes everything subject to the OUs selected earlier in the wizard.

Figure 5-13 shows a specified "pilot group" called JTHybrid-PilotUsers. Ensure that the OU in which this AD Group object resides has been selected as part of the synchronization.

www.dbooks.org

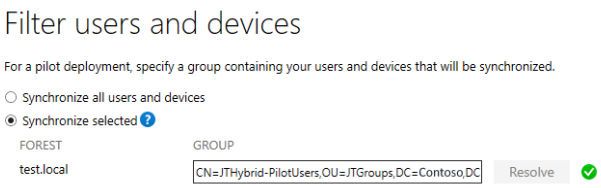


Figure 5-13: Filter users and devices based on an on-premises AD group for pilot deployments.

On the Optional Features page of the Azure Active Directory Connect Wizard for synchronized identity configuration you can select optional features such as the following:

- Exchange hybrid deployment
- Azure AD app and attribute filtering

  To ensure that you have Microsoft SharePoint Online covered from a hybrid perspective, it is advisable to select this feature and select SharePoint Online at a minimum, depending on your broader organizational requirements. This ensures that the minimum required SharePoint Online attributes (currently 89 attributes) are selected for synchronization.
- Password hash synchronization (this should be selected and dimmed)
- Password write-back
- Group write-back
- Device write-back
- Directory extension attribute sync

Selecting any of these features might dynamically add an extra step or two in the wizard. Each of them has their own requirements, planning, and permissions.

More info To learn more about these optional features, go to http://go.microsoft.com/fwlink/?LinkId=532861.

More info For a list of AD attributes that are synchronized with Azure AD Connect (Synchronization tool), go to https://azure.microsoft.com/documentation/articles/active-directory-aadconnectsync-attributes-synchronized/#sharepoint-online.

When this is done, you are ready to configure. You have the choice to start the synchronization process as soon as the configuration completes. If you're an administrator, you might choose to clear this option to give you control as to when the first synchronization will commence. Clearing this option turns off synchronization. You can turn on and start synchronziation by using Windows PowerShell. This is covered in the section "Managing directory synchronization" later in this chapter.

Note You can turn on staging mode for a secondary Azure AD Connect server to achieve a standby synchronization server in case the active server fails. When in staging mode, the new synchronization server will perform its import but not export to Azure AD. Password synchronization and password write-back are not turned on for this server while in staging mode. The metaverse (an intermediate database) is fully populated and ready to export data back to Azure AD when staging mode is turned off. Configuration changes made in the active Azure AD Connect server are not automatically replicated to the staging server, requiring additional manual configuration to this server.

This concludes the configuration of synchronized identities with Azure AD Connect. You can exit Azure AD Connect now.

> **More info** To read more documentation on the custom installation of Azure AD Connect, go to https://azure.microsoft.com/documentation/articles/active-directory-aadconnect-get-started-custom.

Verification

Use the following checklist for your verification steps:

- Ensure that directory synchronization has been activated in Office 365 or Azure AD.
- Verify that Azure AD Connect creates a directory synchronization service account, a local user with a name similar to AAD_762ec736ff66, and adds this user to the ADSyncAdmins local group.
- Ensure a new service, Microsoft Azure AD Sync, is in a running state and runs with the directory synchronization service account.
- In Windows PowerShell, run Get-ADSyncScheduler to verify the sync schedule settings.
- Synchronization occurs every 30 minutes by default. When you are ready to turn on the synchronization schedule, ensure that SyncCycleEnabled is set to True by running Set-ADSyncScheduler -SyncCycleEnabled $true in Windows PowerShell.
- Ensure that all outbound connections over port 443 TCP are allowed from the Azure AD Connect server, especially https://ssprsbprodncu-sb.accesscontrol.windows.net.
- In the Office 365 Admin Center, in the Users section, click Active Users and then Manage Active Directory synchronization. Verify that Directory Sync Enabled and Password Sync Enabled. The section also reports when the last synchronization occurred. For example, as illustrated in Figure 5-14, the Last Directory Sync and Last Password Sync reports Last Synced Less Than An Hour Ago. Verify the Directory Sync Service Account is displaying an account. This account is automatically created by Azure AD Connect and the string of characters after Sync_AD will change in your environment.

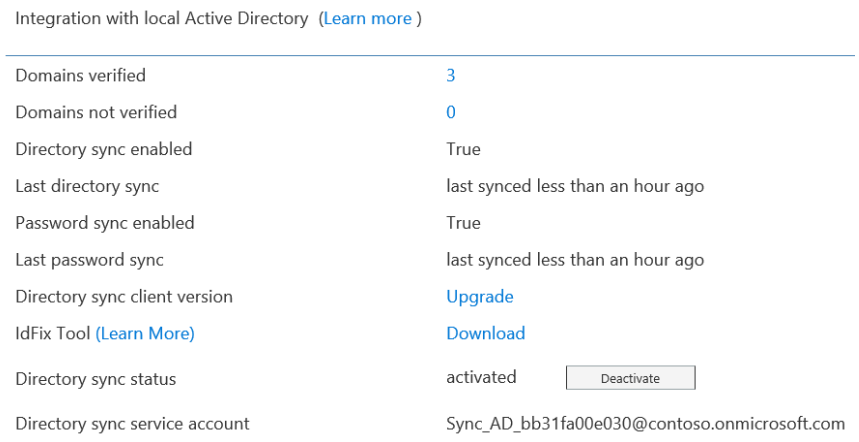


Figure 5-14: Verify the status reported for Last Directory Sync and Last Password Sync. Note the newly populated Directory Sync Service Account.

- Verify your current AzureAD Connect configuration by reopening Azure AD Connect and selecting Review Your Solution, as shown in Figure 5-15.

www.dbooks.org

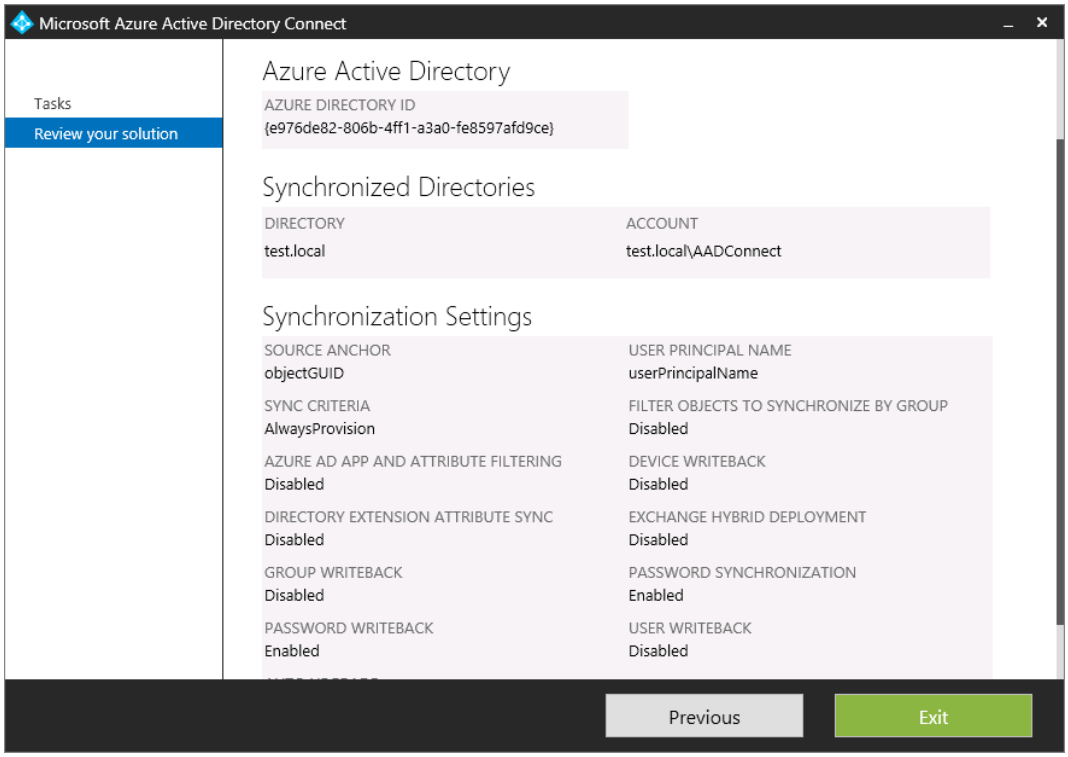


Figure 5-15: The Review Your Solution wizard page, where you can see your synchronization settings and any active features.

- Verify that all ports in the firewall and proxy are configured as documented by Microsoft.
- To verify that password write-back is successfully working, you need to see if there are any events logged in the Application Event Viewer, such as Event 656 - Password Change Request, as depicted in Figure 5-16. Passwords changed from the cloud adhere to password complexity policies set in the on-premises active directory.

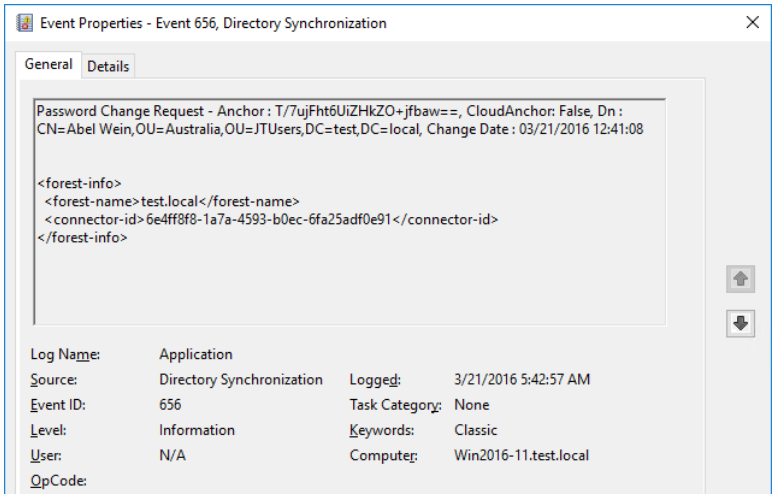


Figure 5-16: Event ID 656: Password Change Request made from a user in the cloud.

When a password has successfully changed from the cloud, the password hash is written back to the on-premises directory. This is a synchronous operation and events such as Event 657 - Password Change Result will be written to the Azure AD Connect server instantaneously, as depicted in Figure 5-17.

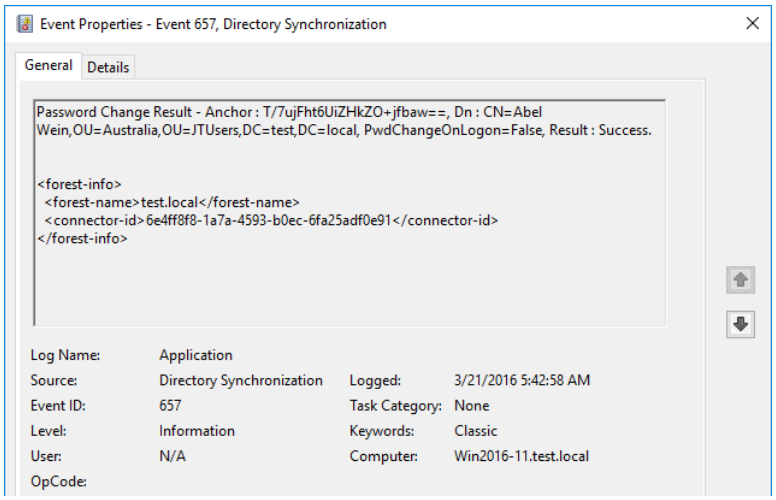


Figure 5-17: Event ID 657 – An event after a password has been successfully changed and written to an on-premises directory.

More info To read more on troubleshooting password synchronization, go to https://support.microsoft.com/kb/2855271.

To learn more about how password write-back works, go to https://azure.microsoft.com/documentation/articles/active-directory-passwords-learn-more/#how-password-writeback-works.

Troubleshooting synchronization issues

When you consider the number of infrastructure components in a hybrid deployment, you can imagine that it's highly possible that one of these components might fail to operate. Luckily, the components in Office 365 are managed by Microsoft support, but your IT operations staff still needs to support the on-premises components.

Although Chapter 6 covers troubleshooting single sign-on (SSO) issues, we'll nonetheless take a moment in this section to focus on customers that choose password synchronized identities. The main and obvious symptom of a malfunctioning synchronization deployment is when new users and passwords are not synchronized to the Azure AD. The following are not scoped for SharePoint hybrid, but are scoped to cover only the underlying directory synchronization:

- Azure AD Connect trace logs

  Review Azure AD Connect trace logs for any warnings ([WARN]) or errors ([ERROR]) that occurred during the installation of Azure AD Connect. These warnings and errors are the first signs of the potential issues related to configuration options chosen and permissions.

  You can find the trace log files in C:\Users\%username%\AppData\Local\AADConnect\trace-*yyyymmdd-xxxxx*.log, where *yyyymmdd-xxxxx*.log is the name of the file.

- Noncomplying directory objects

  Recheck any directory object (users, groups, and contacts) errors by running IdFix in a new folder to get a fresh report on potential errors. Implement fixes and then rerun the IdFix tool to ensure that your directory is cleansed from all errors reported by the IdFix tool.

- Windows event logs

www.dbooks.org

On the Azure AD Connect server, check the Windows event log for any events (normally displayed as informational events) in the Application event log. These can indicate whether passwords are being synchronized successfully or if there are any failures in the synchronization process.

The same goes for the other servers, such as the domain controllers, to capture errors and security failure events that are logged to help in your troubleshooting.

- Synchronization Service Manager (see Figure 5-18)

  The default path to the miisclient is C:\Program Files\Microsoft Azure AD Sync\UIShell\miisclient.exe.

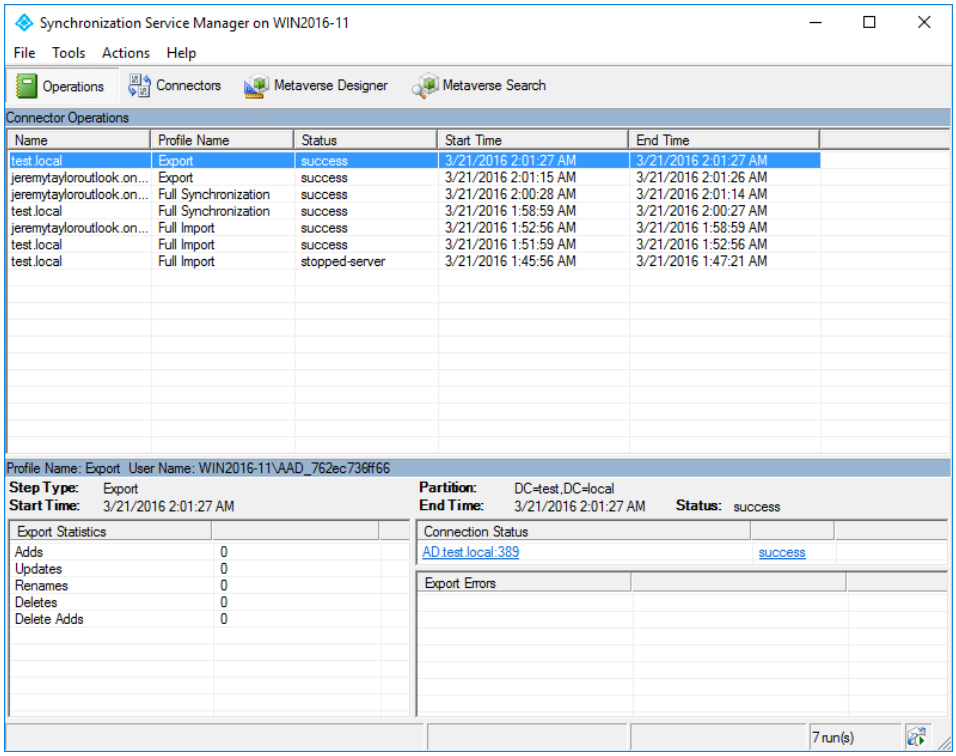


Figure 5-18: The Synchronization Service Manager.

- Troubleshooting tools

  There are a couple of tools that can help you to troubleshoot any obvious issues with the on-premises environment and connectivity to Office 365. To access these tools, go to the Office 365 Admin Center, and then, on the menu bar, click Tools.

- Check your Office 365 configuration with Office 365 health, readiness, and connectivity checks. This tool runs checks to determine the status of your on-premises or cloud configuration. For convenience, users are able to run this tool without the involvement of an administrator, provided the software requirements are met, such as Microsoft .NET 3.5. The Office 365 health, readiness, and connectivity checks tool is available at http://aka.ms/checkmypc.

- Check your Office or Office 365 connectivity by using the Microsoft Connectivity Analyzer.

- Directory Synchronization Troubleshooter

  The directory synchronization troubleshooter is an online tool that is available to use 24 hours after a last successful synchronization has occurred. After 24 hours has passed, it is displayed on https://portal.office.com/admin/default.aspx#ActiveUsersPage.

The tool is directly available at http://aka.ms/dsup.

The troubleshooting tool looks for possible issues and provides guidance on changes that can help fix your synchronization issues. You are able to perform a quick scan of your event logs and Office 365 settings. A full scan includes the checks done in a quick scan and additionally scans your Active Directory objects for issues.

More info To learn more about the tools available to troubleshoot directory synchronization issues, go to https://community.office365.com/b/news_hub/archive/2015/04/13/use-the-directory-synchronization-troubleshooter-to-solve-problems-with-dirsync.

- New service request

  Office 365 has a service request facility where you can issue a service request for the specific problem you are experiencing after conducting your initial troubleshooting. To raise a new service request in Office 365, go to the Office 365 Admin Center. In the pane on the left, expand support and click Service Requests. Click the + (plus) sign to create a new service request. For directory synchronization issues, select Identity Management, as depicted in Figure 5-19.

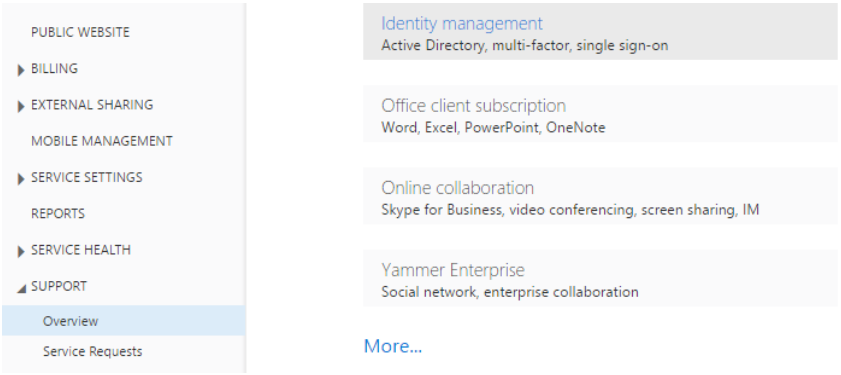


Figure 5-19: Opening a support ticket through the Office 365 Admin Center.

- Office 365 Community

  Try searching for solutions from the forums, wikis, and troubleshooting section. You also can post a question and receive community support for your issue, moderated by Microsoft.

Managing directory synchronization

You will be required to manage and maintain the components installed with Azure AD Connect. After you have set up directory synchronization, you can add additional administrators to manage the installed synchronization engine. To add additional administrators to access and manage the engine, add their user names to the group named ADSyncAdmins on the local Azure AD Connect server.

To change review and change the Azure AD Connect configuration, such as customizing synchronization options or migrating to SSO, you need to open Azure AD Connect and select the Additional Task that you want to perform.

www.dbooks.org

Starting and stopping synchronization

When configuring Azure AD Connect, you might have chosen to not start synchronization. At some point, you will want to start it and turn on the schedule.

To force-start a synchronization, on the Azure AD Connect server, run the following Windows PowerShell command:

```
Start-ADSyncSyncCycle
```

To force-stop a synchronization, run this:

```
Stop-ADSyncSyncCycle
```

To pause the Active Directory Sync Scheduler, run the following in Windows PowerShell on the Azure AD Connect server:

```
Set-ADSyncScheduler -SyncCycleEnabled $false
```

To turn on the synchronization engine to begin its default 30 minute schedule, run the following in Windows PowerShell on the Azure AD Connect server:

```
Set-ADSyncScheduler -SyncCycleEnabled $true
```

To verify if the synchronization engine is scheduled to run every 30 minutes, run the following in Windows PowerShell on the Azure AD Connect server (see Figure 5-20):

```
Get-ADSyncScheduler
```

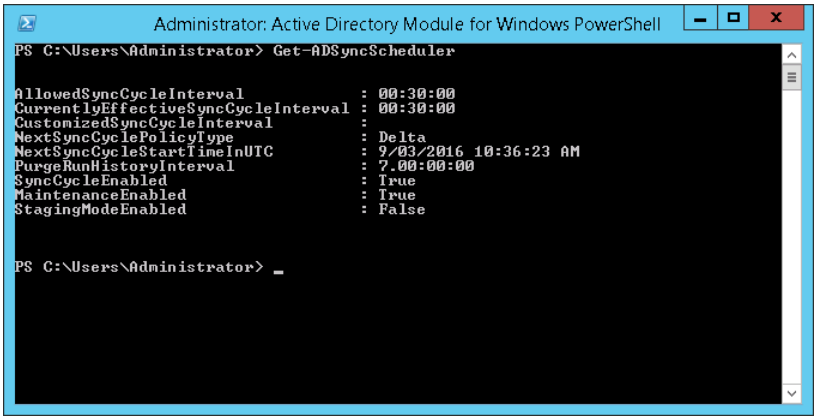


Figure 5-20: Get-ADSyncScheduler displays the synchronization schedule settings and current state.

To view other ADSync Windows PowerShell commands, run the following:

```
Get-Command *adsync*
```

Managing Azure AD by using Windows PowerShell

To begin managing Azure AD via Windows PowerShell, you need to install the Microsoft Online Services Sign-In Assistant for IT Professionals RTW from the Microsoft Download Center: https://www.microsoft.com/download/details.aspx?id=41950.

Next, install the Azure Active Directory Module for Windows PowerShell (64-bit version), and then click Run to run the installer package. To download the module, go to http://go.microsoft.com/fwlink/p/?linkid=236297.

To connect to your Azure AD tenant through Windows PowerShell use the following:

```
$msolcred = get-credential

connect-msolservice -credential $msolcred
```

To view all of your licensed users, run the following:

```
Get-MsolUser -all | Where-Object {$_.isLicensed -eq "true"}
```

More info To learn more on managing Azure AD through PowerShell, go to https://msdn.microsoft.com/library/jj151815.aspx.

www.dbooks.org

CHAPTER 6

SharePoint hybrid single sign-on

This chapter is meant for organizations that plan to implement federated identities using Active Directory Federation Service (AD FS) for single sign-on (SSO). SSO saves users from having to type their credentials each time they access any Microsoft SharePoint Online or Microsoft Office 365 resource. It is considered an important foundation for a SharePoint hybrid environment. Chapter 5 covers synchronized identities with password synchronization. With federated identities, only the identities are synchronized to Office 365. Passwords are not synchronized to Office 365, because authentication occurs at a Secure Token Service (STS), which is typically in an on-premises environment or optionally hosted in Microsoft Azure.

SSO

SSO is a mechanism by which users sign in once to access sites and multiple applications and do not need to do so again when accessing other services within the same tenancy. This reduces the need for users to manage and type multiple passwords. In a SharePoint hybrid environment, this means users do not need to manage multiple credentials for the SharePoint hybrid–related cloud services with Office 365 and SharePoint on-premises. Users need to manage just one set of credentials: their on-premises passwords. With AD FS, authentication is completed by the on-premises AD FS STS; for example, sts.contoso.com. You can choose to expose the STS to the public Internet for remote users to be able to authenticate while outside the corporate network boundaries. Figure 6-1 shows broadly how this works.

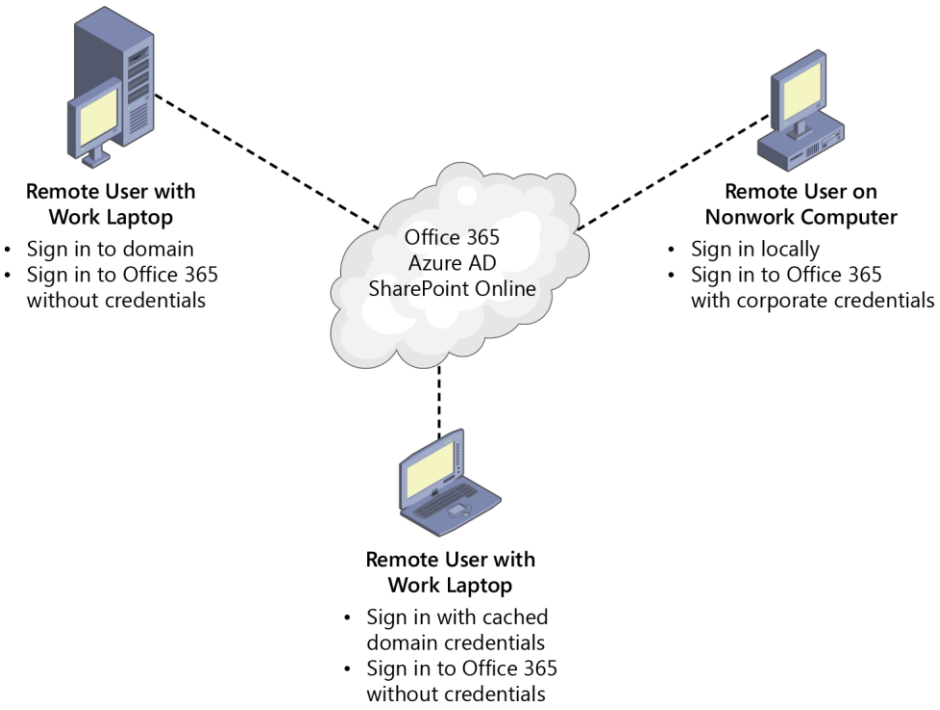


Figure 6-1: Single sign-on overview.

AD FS

AD FS is a service that facilitates the secure, seamless sharing of information between trusted partner organizations, known as federation partners. A federation "trust" is different from a domain trust. With AD FS, all communication occurs via the requesting user (client) over HTTPS (TCP 443). Unlike a domain trust, there are no special requirements such as deep integration or special ports to be opened between the organizations. Some of the key benefits of AD FS are SSO, no duplication of credentials or user accounts across partner organizations, and the elimination of cross-partner organization account management because each organization manages its own users. The first version of AD FS was introduced with Windows Server 2003 R2.

AD FS version	Proxy	Operating system	Availability
AD FS 1.0	Federation Service Proxy	Windows Server 2003 R2	Active Directory Services Windows component
AD FS 1.1	Federation Service Proxy	Windows Server 2008 and 2008 R2	Active Directory Services Windows component
AD FS 2.0	Federation Service Proxy	Windows Server 2008 and 2008 R2	Separate download AdfsSetup.exe
AD FS 2.1	Federation Service Proxy	Windows Server 2012	Windows Server role
AD FS	AD FS Proxy – Web Application Proxy	Windows Server 2012 R2	Windows Server role. WAP – remote Access role.
AD FS	AD FS Proxy – Web Application Proxy	Windows Server 2012 R2	Windows Server role. WAP – remote Access role.

www.dbooks.org

Note From Windows 2012 R2 onward, AD FS, is known as just that: AD FS. It is no longer referred to along with the version number; for example, AD FS 3.0.

AD FS is an STS that is mainly used to compile statements about user's identities. These statements are known as *claims*, and they identify the user's title, user name, UPN, email, and so on. These claims are then used by the web application to ascertain the level of access that should be given to the requesting user.

More info For more information on AD FS and claims, go to https://msdn.microsoft.com/library/bb897402.aspx.

AD FS requires a user directory such as Active Directory or Active Directory Application Mode (ADAM). Other non-Microsoft directories are not compatible with AD FS. You can use third-party identity providers to implement SSO with Azure Active Directory (Azure AD).

More info To learn more about third-party identity providers that you can use to implement SSO with Azure AD, go to https://msdn.microsoft.com/library/azure/jj679342.aspx.

Web Application Proxy

Web Application Proxy is a remote access service in Windows Server by which external clients can securely access internal web applications with their devices outside an organization's corporate network. Web Application Proxy provides its own AD FS proxy functionality and replaces the AD FS proxy that was available with Windows Server 2012 and prior operating system versions. You can use Web Application Proxy servers for publishing internal applications for external access, not just for AD FS proxy scenarios. The AD FS proxy is a critical piece of infrastructure for external clients for SSO. Organizations have the ability to manage risk associated with Web Application Proxy endpoints by controlling authentication and authorization policies from the internal AD FS system.

Configuration steps of AD FS

There are a number of steps required to configure AD FS. (Some of these steps are covered in Chapter 5 as part of the synchronized identities configuration.) The following points are intended to give you a high-level understanding of what is involved:

- Verify your domain to Office 365
- Request a certificate from a third-party Certification Authority (CA) for the federation service name
- Create a DNS record for on-premises STS endpoints (federation service name)
- Install and configure AD FS.
- Optionally, install and configure AD FS proxy functionality provided by the Web Application Proxy role service.
- Add the domain to Office 365 and validate ownership of the domain
- Convert the domain to federated to establish trust between AD FS and Office 365
- Configure AD FS—Add Office 365 as a new relying party trust
- Synchronize Active Directory user accounts to Office 365 (Azure AD)

- Activate users by assigning Office 365/Azure AD licenses
- Configure users authentication phone or email for password reset
- Download Office 365 client tools
- Configure the client computer for SSO

Working with subdomains

If your environment has multiple subdomains, it is important to note that after a root domain has been converted to a federated domain, any new subdomains added to your Office 365 tenant will inherit the parent domain (RootDomain) and its associated authentication state.

A requirement might exist that certain users are to only have synchronized identities and the rest of the users are to be federated identities; for example, Australian users at au.contoso.com are managed separate to the rest of the world at contoso.com. In this scenario, you would add au.contoso.com before you add the root contoso.com. After you convert contoso.com to a federated domain, au.contoso.com will still be a "managed" domain and will not subsequently convert to a federated domain. Adding any new subdomains such as corp.contoso.com will automatically inherit the root domain's state regardless of you convert it to a federated state or reverse it.

> **Note** If you want to have the ability to control the authentication modes for individual subdomains in the future, you would need to add them first before adding the root domain name because new subdomains will automatically inherit the root domain's authentication state.
>
> You also can convert subdomains that you add before the root domain to a federated domain while leaving the top level domain to be in a non-federated state.

You can add new top level domains by using the -SupportMultipleDomain switch in Windows PowerShell. You can use the following commands to create a new relying party trust with support for multiple top-level domains:

```
New-MsolFederatedDomain -DomainName <domainname> -SupportMultiDomain
Update-MsolFederatedDomain -DomainName <domainname> -SupportMultipleDomain
Convert-MsolDomainToFederated -DomainName <domainname> -SupportMultipleDomain
```

If you are planning to add new subdomains under additional top-level domains to the initial federated domain, you will need to manually modify the claims rules for the Microsoft Office 365 Identity Platform in AD FS to avoid authentication issues.

> **More info** To understand claim rule language in AD FS 2.0 and higher, go to http://social.technet.microsoft.com/wiki/contents/articles/4792.understanding-claim-rule-language-in-ad-fs-2-0-higher.aspx.

Secure Sockets Layer Certificates

There are the three certificates that you need to plan for in an AD FS deployment: service communication certificate, token signing certificate, and token decrypting certificate. Each is described in more detail in the following sections.

Service communication certificate

Office 365 requires that a valid service communication certificate is installed and utilized for the on-premises AD FS infrastructure. Because it is not possible for Office 365 to trust an internal CA or a self-signed service communication certificate, you are required to purchase a certificate from a public CA.

www.dbooks.org

The table that follows should help you to plan for the creation of a Subject Alternative Name (SAN) certificate for your Web Application Proxy servers. A SAN certificate allows for different host names to be alternative DNS names in the same Secure Sockets Layer (SSL) certificate. You might have need for additional SAN requirements based on the Office 365 features you select or internal applications you choose to publish through your Web Application Proxy servers.

SAN	Purpose	Example
DNS Name=sts.contoso.com	The STS endpoint where clients authenticate	sts.contoso.com
DNS Name=enterpriseregistration.contoso.com	Workplace join and device registration service	enterpriseregistration.contoso.com
DNS Name= certauth.sts.contoso.com	Used for smart card authentication.	certauth.sts.contoso.com

More info To learn more about alternative SSL hostname binding enhancements in Windows Server 2016, go to https://technet.microsoft.com/library/mt622002.aspx.

Alternatively, you can create a Wildcard SSL certificate that includes the aforementioned hostnames. Wildcard SSL certificates can include other SANs and might cost more than other types of certificates depending on the public CA product offerings.

Wildcard SSL certificate	Purpose	Example
DNS Name=*.contoso.com	A wildcard certificate to allow for the aforementioned subdomains.	sts.contoso.com enterpriseregistration.contoso.com otherapp.contoso.com

Note You need to use the same SSL certificate for all AD FS servers including the Web Application Proxy servers. Ensure that the private key for the chosen certificate is accessible to the service account for this federation service on each server in the farm. The service communicate certificate will need to be in the PFX format for the Azure AD Connect tool.

Token signing certificate

The token signing certificate is used to securely sign all tokens that the federation server issues. By default, the token signing certificate is a self-signed certificate and is generated by AD FS during installation. The token signing certificate is a standard X.509 certificate.

Token decryption certificate

Token decryption certificates are standard X.509 certificates that are used to decrypt any incoming tokens. By default, the token decryption certificate is a self-signed certificate and is generated by AD FS during installation.

Information about both the token signing and token decryption certificates are published on the STS federation metadata; for example, https://sts.contoso.com/federationmetadata/2007-06/federationmetadata.xml. Office 365 uses the certificate information published in the public federation metadata endpoint to alert administrators on expiring certificates (see Figure 6-2). By default, the token signing and token decryption certificate is automatically renewed by AD FS.

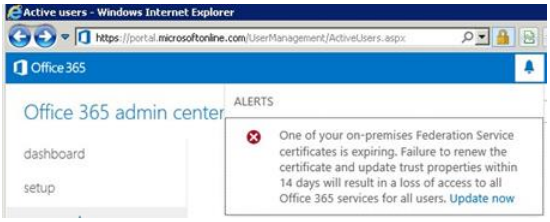


Figure 6-2: An SSL certificate expiry alert on the Office 365 admin center.

DNS settings

For users to be able to authenticate with their federated identities, they must be able to resolve the federation service name, such as sts.contoso.com from within the organization and from the Internet for remote access scenarios. From within the organization, sts.contoso.com would normally resolve to the internal AD FS server or AD FS farm's load-balanced virtual IP (VIP) address. From outside the organization, sts.contoso.com would normally resolve to a public IP address of the Web Application Proxy server or the load-balanced reverse proxy VIP.

A DNS "A" or "AAAA" host record is a requirement for the federation service name. CNAME records are not recommended for the federation service name.

The Web Application Proxy servers must be able to resolve the internal federation service name. Because Web Application Proxy servers might be in a perimeter network (also known as a DMZ, demilitarized zone, and screened subnet) and not joined to a domain that has no DNS server configured, a modified HOSTS file might be required to resolve the internal federation service name; for example, you might need to add a line something similar to the following in the Web Application Proxy server's HOSTS file (C:\Windows\System32\drivers\etc\hosts):

```
10.1.1.10 sts.contoso.com
```

I recommend that you create the DNS host records before you commence the configuration of AD FS and Web Application Proxy servers with Azure AD Connect because there is a final step in the Azure AD Connect wizard that verifies DNS settings.

It is important to ensure that you add the federation service name, such as https://sts.contoso.com to your organization's browser's intranet zone. This is to turn on automatic sending of windows credentials for Windows integrated authentication.

Configuring AD FS

There are three methods by which you can configure AD FS and Web Application Proxy servers. The first is through the Azure AD Connect tool, the second method is through the AD FS configuration wizard, and the third method is via Windows PowerShell. After you have set up AD FS and the Web Application proxies, you will need to run the Azure Active Directory Connect Wizard to complete the Office 365 SSO set up. To download and open the wizard, go to https://www.microsoft.com/download/details.aspx?id=47594.

www.dbooks.org

You cannot use the Azure Active Directory Connect Wizard to configure AD FS to use its own SQL server; instead, it configures AD FS to use the Windows Internal Database (WID). The advantage of manually configuring AD FS is to give administrators the option to install AD FS on a SQL server.

Azure AD Connect

The Azure Active Directory Connect Wizard installs the AD FS role and configures AD FS for you. Similarly, it installs the remote access role and configures Web Application Proxy with AD FS proxy capabilities. For environments that have synchronized identities already set up, you would need to reconfigure the sign-in model using the Azure Active Directory Connect Wizard.

It is important to note that the Azure AD synchronization function is still required and is set up by the Azure Active Directory Connect Wizard in the steps prior to the AD FS configuration steps. When it comes to Azure AD Connect, the main difference between synchronized identities and federated identities is that password synchronization is not configured in the federated identity sign-in model. Refer to Chapter 5 for the initial steps for configuring Azure AD Connect.

If you already have synchronized identities configured, on the Tasks page of the wizard, you need to select Change User Sign-In, as shown in Figure 6-3.

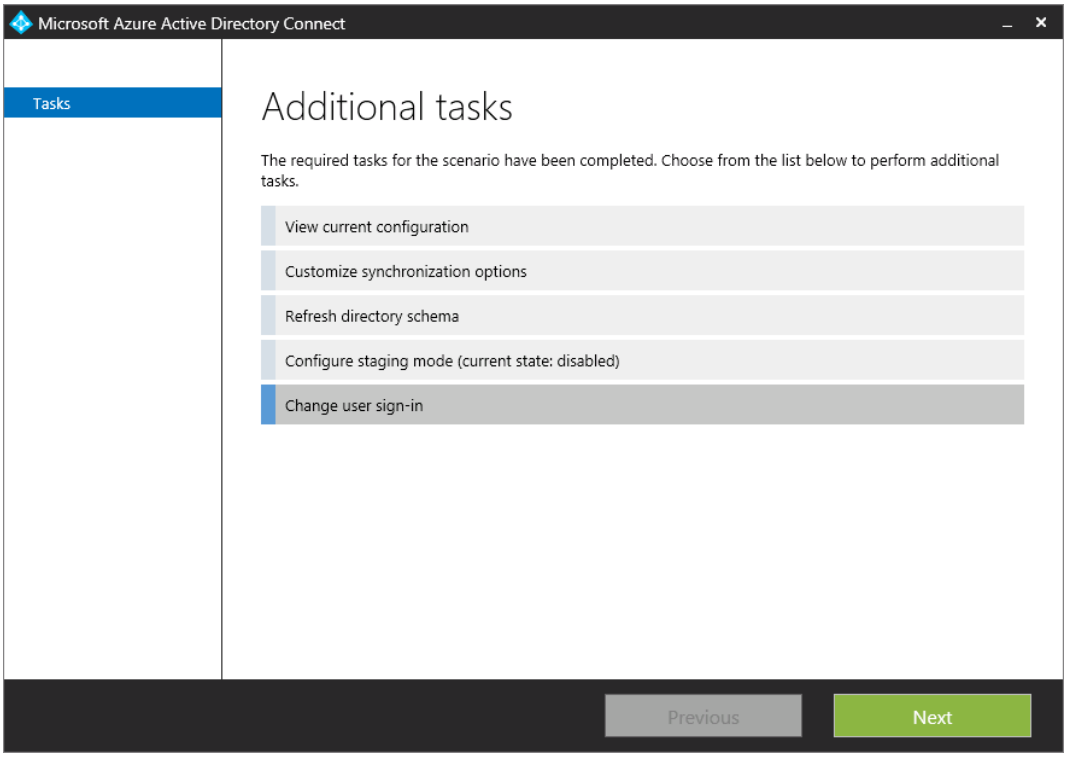


Figure 6-3: Change the user sign-in in the Azure Active Directory Connect Wizard.

You connect to Azure AD by typing in your Office 365 global administrator credentials; for example, username@contoso.onmicrosoft.com.

If you sign in as a global administrator with the same domain name as the domain you are to federate, Azure AD Connect will not allow you to complete the configuration; for example, username@contoso.com.

The error depicted in Figure 6-4 displays when you attempt to sign in as a global administrator with the same domain name as the domain to be federated.

We cannot federate an Azure AD domain while signed in to Azure AD as a user in the same domain. Please choose a different domain to federate or restart this wizard and provide different Azure AD global administrator credentials.

Figure 6-4: Error displayed when signed in to Azure AD Connect with the same domain to be federated.

The Azure Active Directory Connect Wizard can configure new AD FS and Web Application Proxy farms or it can configure the trust between an existing AD FS farm and Azure AD. This is possible as long as the underlying server operating systems are Windows Server 2012 R2 or later.

To demonstrate the configuration of AD FS, we will proceed with the Federation With AD FS option.

Select Federation With AD FS and then click Next, as demonstrated in Figure 6-5.

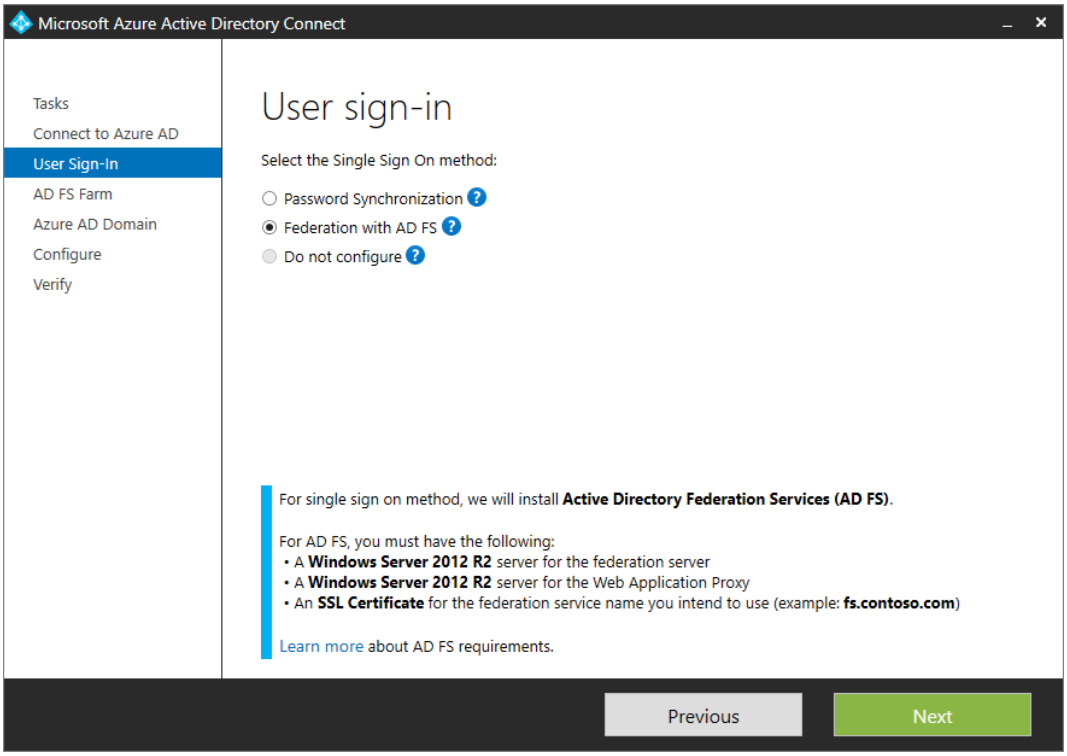


Figure 6-5: The User Sign-In page in the Azure Active Directory Connect Wizard.

On the next page, you must provide the service communications certificate or browse for an existing service communications certificate already installed on the federation servers.

If the service communication certitiicate is a wildcard certificate, you can specify the subject name prefix. If the service communication certitiicate is a SAN certificate with multiple SANs, you will be presented with a drop-down choice to select for the federation service name, as illustrated in Figure 6-6. After you make your selection, click Next.

www.dbooks.org

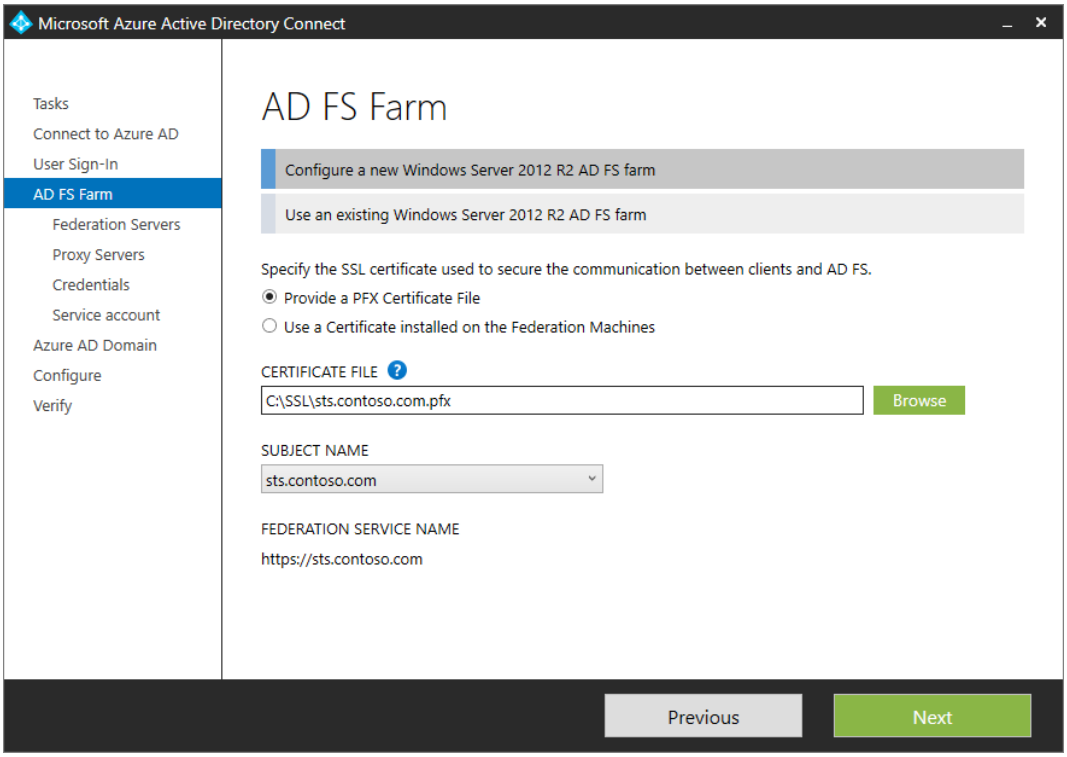


Figure 6-6: AD FS Farm page with configuration options and service communication certificate selection in the Azure Active Directory Connect Wizard.

You have the option to configure an existing Windows Server 2012 R2 or Windows Server 2016 AD FS farm. You would need to specify the primary server in the preexisting AD FS farm, or if your farm uses SQL server, provide the name of any node in the farm.

If you are prompted to provide credentials, you must specify the credentials of the local administrator of the AD FS server/farm to be able to connect and proceed with the configuration.

You can add multiple AD FS servers and Azure AD Connect will configure them as one farm.

You can choose to install the Web Application Proxy servers through the Azure Active Directory Connect Wizard. You can choose to skip the Web Application Proxy server configuration by just clicking next without specifying any server names.

To be able to configure the Web Application Proxy servers, you will need to provide the local administrator credentials to connect to the server and configure the Web Application Proxy services.

You would also need to ensure that the Web Application Proxy servers can communicate back to the AD FS servers on TCP port 443. Additionally, the Web Application Proxy servers must be able to resolve the federated service name to the internal IP address of the AD FS servers or load-balanced VIP.

It is not possible to configure AD FS and Web Application Proxy on the same servers. The Web Application Proxy servers must not have been part of an AD FS farm; otherwise, the wizard will display an error.

Ideally, the Web Application Proxy servers would reside in a perimeter network and not joined to a domain.

Click Next to proceed.

The next page requires domain administrator credentials to configure the federation service. Type in the domain administrator user name and password—for example, CONTOSO\DomainAdmin—and then click Next.

On the next page, you configure the group Managed Service Account (gMSA). These accounts are a feature of Windows Server 2012 and later, and you can use them across multiple servers. The benefit of a gMSA is that Service Principal Name (SPN) management and password management is done for you. For automatic SPN and password management, a domain-functional level of Windows Server 2008 R2 or higher is required.

At least one domain controller that runs Windows Server 2012 or later is required for gMSAs to be created because the passwords are generated by the Group Key Distribution Services (GKDS) running on domain dontrollers that are Windows Server 2012 or higher. If it cannot find a Windows Server 2012 or higher domain controller in the forest, Azure AD Connect turns off this option, and you need to specify an existing service account in the domain.

If you want to create a gMSA, you would need to specify the enterprise administrator credentials to generate the Key Distribution Services (KDS) root key, as shown in Figure 6-7. Click Next to continue.

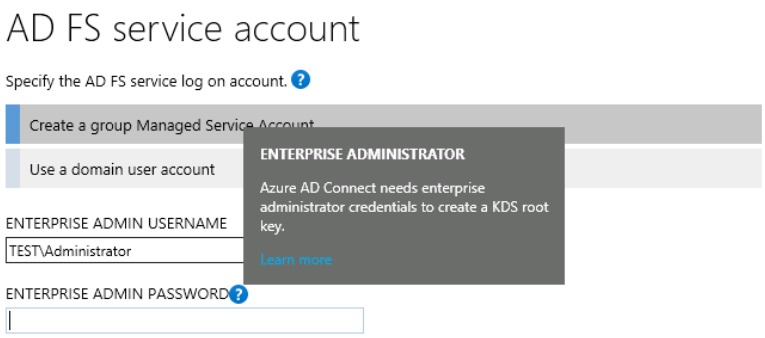


Figure 6-7: You must provide enterprise administrator credentials to generate a KDS when the Group Manged Service Accounts option is selected.

On the Azure AD Domain page, you must specify the verified domain name that will be converted to a federated domain; for example, contoso.com.

Be aware that if this domain name is used for synchronized identities, users will temporarily be unable to sign in with their synchronized passwords in Office 365.

Additional domains that are verified in Office 365 can be added at a later time by performing this step again through Azure AD Connect.

When you click Next, the Configure page opens (see Figure 6-8). Password synchronization will be turned off, the name of the federation service name will be confirmed, and the number of AD FS and Web Application Proxy servers will be confirmed. You have the choice to install without starting the synchronization process soon automatically. If you choose to not start the synchronization process automatically after the configuration completes, you will need to start the synchronization manually by using Windows PowerShell.

www.dbooks.org

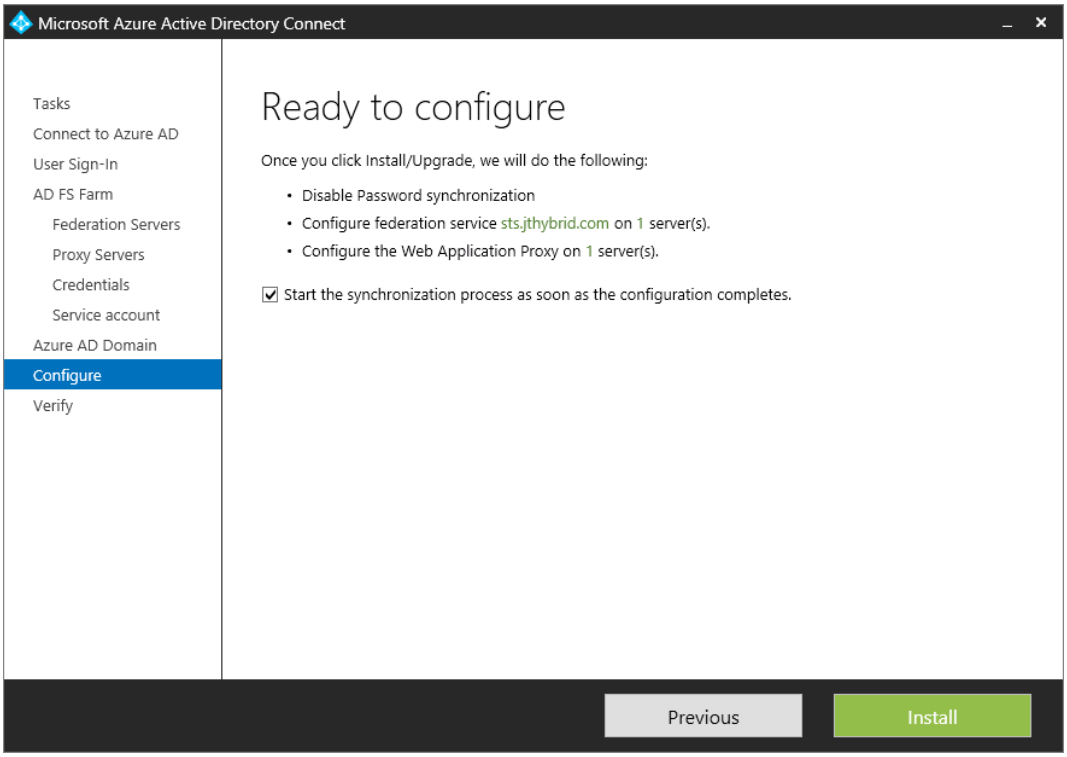


Figure 6-8: The Azure Active Directory Connect Wizard is ready to configure the AD FS server and the Web Application Proxy server.

I recommend that you recheck to verify DNS A host records are configured and pointing to the correct IP addresses. In the pane on the left, click Verify to perform the DNS verification. Take note of the IP addresses that were verified by Azure AD Connect, and then close the wizard.

The Active Directory Federation Services Configuration wizard

You can choose to install the AD FS components before running the Azure Active Directory Connect Wizard.

There are two ways to configure AD FS without the Azure Active Directory Connect Wizard: you can configure AD FS through the Active Directory Federation Services Configuration Wizard or by using Windows PowerShell. Each gives you the ability to specify a SQL server to host the Active Directory databases, as illustrated in Figure 6-9.

In SQL server, AD FS creates two databases:

- AdfsArtifactStore
- AdfsConfigurationV2

The SQL sign-in account is the service account or gMSA specified in the installation. The sign-in is the db_geneveaservice database role membership for both the databases.

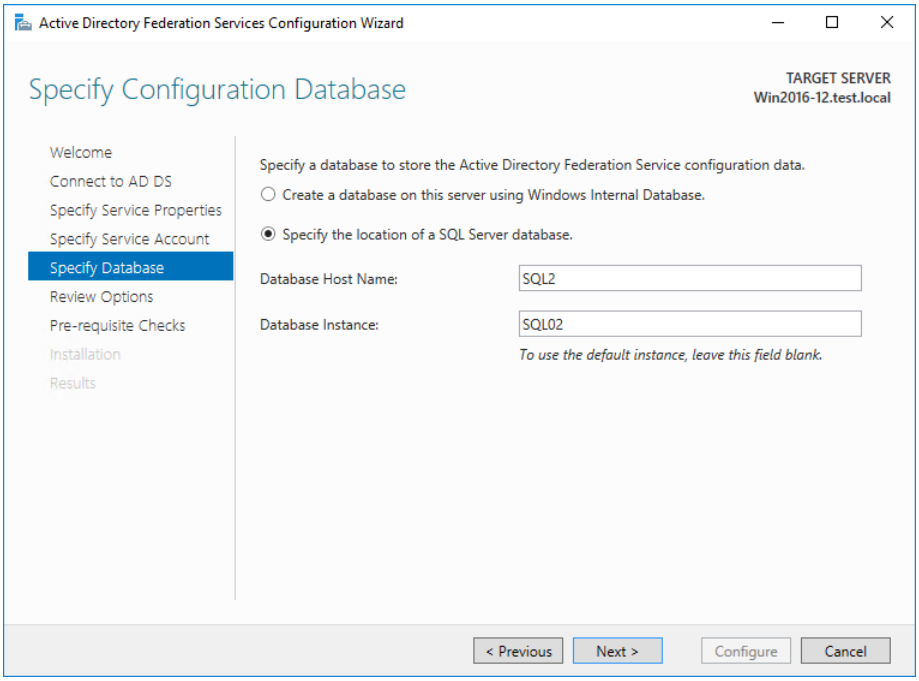


Figure 6-9: You can specify a SQL server to host AD FS databases in the Active Directory Federation Services Configuration Wizard.

After you configure AD FS, you won't be able to run the wizard again on that server. If you want to reconfigure AD FS on that server, you will need to run the AD FS Windows PowerShell command Install-AdfsFarm with the -overwriteconfiguration switch.

Installing AD FS by using Windows PowerShell

You can install and configure AD FS by using Windows PowerShell. On the server that you want to configure as a federation server, run the following in an elevated Windows PowerShell window:

```
Install-WindowsFeature adfs-federation -IncludeManagementTools
```

AD FS installs on the first server and is ready to be configured.

To configure AD FS, you need to run the Windows PowerShell command Install-AdfsFarm, as shown in the code example that follows. If you are configuring AD FS with a pre-created service account, you can replace the -GroupServiceAccountIdentifier switch with -ServiceAccountCredential. You would need to manually create the SPN by running setspn.exe -s HOST/sts.contoso.com CONTOSO\ADFSsvcAcc after updating it with your federation service name and the intended AD FS service account.

If you are planning to use a gMSA, the SPN will be created automatically for you.

Here is an example:

```
Import-Module ADFS
Install-AdfsFarm
-CertificateThumbprint:"24FE112AC6568D60AB6C87A533567A69C66B8C61" `

-FederationServiceDisplayName:"STS Contoso" `

-FederationServiceName:"sts.contoso.com" `

-GroupServiceAccountIdentifier:"CONTOSO\aadcsvc`$" `

-SQLConnectionString:"Data Source=SQL1\SQL01;Initial Catalog=ADFSConfiguration;Integrated Security=True;Min
Pool Size=20"
```


www.dbooks.org

More info The preceding Windows PowerShell command is for illustration purposes only. To learn more about the Install-AdfsFarm command for configuring AD FS by using Windows PowerShell, go to https://technet.microsoft.com/library/dn479416(v=wps.630).aspx.

The Web Application Proxy Configuration Wizard

The Web Application Proxy is a role service of the Remote Access role in Windows Server 2012 R2 and later. It's the Web Application Proxy that provides AD FS proxy functionality for the AD FS servers. You can install the Web Application Proxy role by opening the Add Server Roles And Features Wizard, selecting Remote Access Role, and then specifying the Web Application Proxy role service, as illustrated in Figure 6-10.

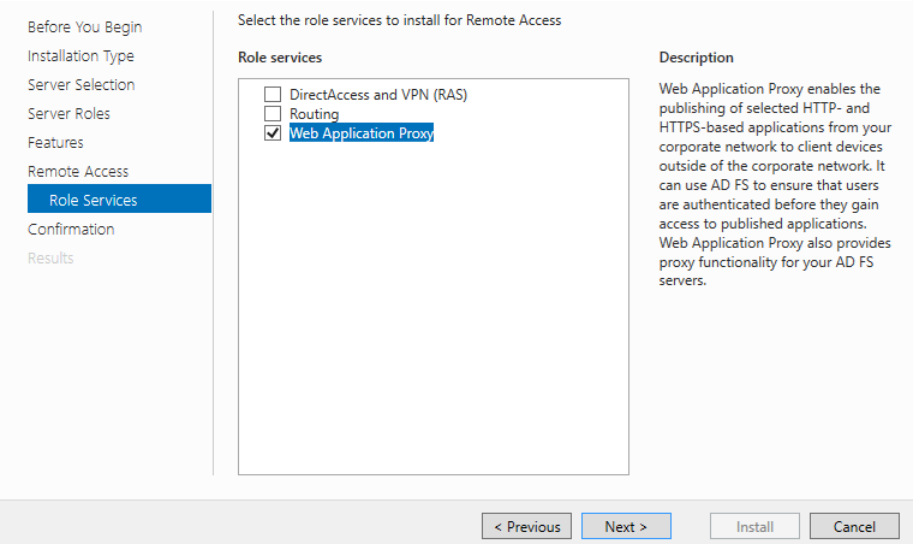


Figure 6-10: Web Application Proxy is a role service under the Remote Access role.

Following installation, the configuration is done by the Web Application Proxy Configuration Wizard, which you can start via the Remote Access Management Console, as depicted in Figure 6-11.

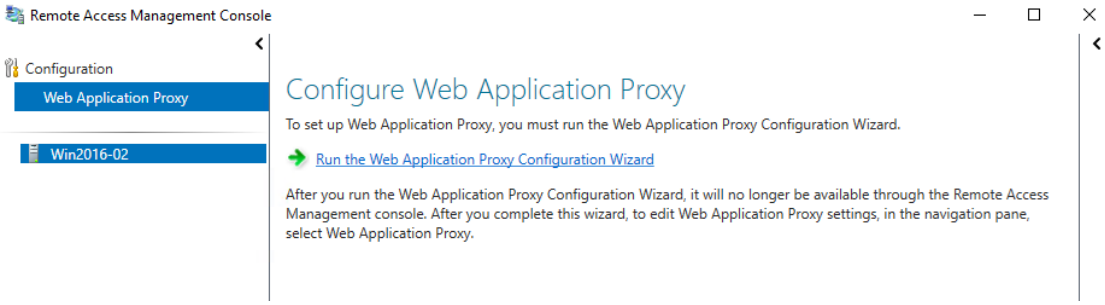


Figure 6-11: You can start the Web Application Proxy Configuration Wizard via the Remote Access Management Console.

You need to specify the federation service name such as sts.contoso.com, the AD FS server's local administrator credentials, and specify the AD FS proxy certificate. When this is complete, the Web Application Proxy configuration is identical for all Web Application Proxy servers that are connected to the same AD FS server. You can manage the Web Application Proxy server via the Remote Access Management console.

Configuring Web Application Proxy by using Windows PowerShell

You can configure the Web Application Proxy by using the following Windows PowerShell command:

```
Install-WindowsFeature Web-Application-Proxy -IncludeManagementTools
```

The next step is to configure the Web Application Proxy. You would need to install the service communication certificate in the Personal certificate store of the Local Computer.

To get the certificate thumbprint, run the following command:

```
Get-ChildItem -path cert:\LocalMachine\My
```

Copy the thumbprint for use in the next command.

```
Install-WebApplicationProxy
-FederationServiceTrustCredential System.Management.Automation.PSCredential
–CertificateThumbprint '24EF112CA6568C60AB6C87A533567A69C998D61'
-FederationServiceName 'sts.contoso.com'
```

High availability

If you have an existing AD FS server, you can add additional nodes to create an AD FS farm. Multiple AD FS servers provides redundancy and fault tolerance to minimize downtime when an AD FS server is removed from service for maintenance. You can add additional nodes to an existing Web Application Proxy server. You must use a hardware or software load balancer such as Windows Network Load Balancing (NLB) to achieve high availability.

Adding a new AD FS node

You can add a node to an existing AD FS farm either by using the Active Directory Federation Services Configuration Wizard on the new AD FS node server or by using the Add-AdfsFarmNode Windows PowerShell command.

> **More info** To learn more about adding node to an existing AD FS farm, go to https://technet.microsoft.com/library/dn479385(v=wps.630).aspx.

Adding a new Web Application Proxy node

You can add a Web Application Proxy node via the node's Remote Access Management Console. The steps are identical to how you would set up a new Web Application Proxy server through the Web Application Proxy Configuration wizard.

To get the certificate thumbprint, run the following command:

```
Get-ChildItem -path cert:\LocalMachine\My
```

This will list all of the local computer personal certificates. Identify the appropriate certificate based on common name (CN) in the subject column in the output window. Copy the thumbprint for use in the following command:

```
Add-WebApplicationProxyApplication -BackendServerUrl 'https://sts.contoso.com/' -
ExternalCertificateThumbprint '24EF112CA6568C60AB6C87A533567A69C998D61'-ExternalUrl
'https://sts.contoso.com/' -Name 'sts.contoso.com' -ExternalPreAuthentication PassThrough
```

Verification

The following are different steps to verify that you have configured SSO correctly. I recommend that you reboot both AD FS and Web Application Proxy servers and perform these tests. This helps to validate that all of the necessary services start without any issues.

www.dbooks.org

A successful verification result is that you should be able to see your SharePoint online team site without typing in your credentials from within the on-premises corporate network with a domain-joined machine. If you are outside of the corporate network on a machine that is not domain-joined, you might be prompted for your credentials. Additionally, you might be prompted for a multifactor authentication (MFA) sign-in, if this is turned on.

Windows service startup checklist

The following are the different services that you need to ensure are started after a reboot of the AD FS and WAP servers:

Server	Service display name	Service name	Startup type
AD FS server	Active Directory Federation Services	adfssrv	Automatic (Delayed Start)
AD FS server	Windows Internal Database	MSSQL$MICROSOFT##WID	Automatic
WAP server	Active Directory Federation Services	adfssrv	Automatic (Delayed Start)
WAP server	Web Application Proxy Controller Service	appproxyctrl	Manual
WAP server	Web Application Proxy Service	appproxysvc	Automatic (Delayed Start)
AAD Connect Server	Microsoft Azure AD Sync	ADSync	Automatic
AAD Connect Server	Azure AD Connect Health Sync Insights Service	AzureADConnectHealthSyncInsights	Automatic (Delayed Start)
AAD Connect Server	Azure AD Connect Health Sync Monitoring Service	AzureADConnectHealthSyncMonitor	Automatic (Delayed Start)

AD FS verification

To verify federation service name resolution, ping the federation service name internally and externally to ensure DNS resolves to the correct IP addresses.

```
ping sts.contoso.com
```

To verify AD FS Web Application Proxy and AD FS services are running, go to the federation service metadata endpoint by appending federationmetadata/2007-06/federationmetadata.xml to the federation service name; for example, https://sts.contoso.com/federationmetadata/2007-06/federationmetadata.xml.

The federation metadata should display something similar to that shown in Figure 6-12.



Figure 6-12: The output of AD FS Federation metadata.

Ensure that the SSL certificates have been installed on each AD FS server.

Web Application Proxy verification

Ensure that your internal federation service DNS A records point to the Web Application Proxy server's IP address or load-balanced IP address if relevant. You need to ensure that the Web Application Proxy is successfully displaying the federation metadata.

To verify federation service name resolution, ping the federation service name from the Web Application Proxy server to ensure it resolves to the correct IP address.

```
ping sts.contoso.com
```

To verify the federation metadata is displaying, browse to the federation service metadata endpoint by appending federationmetadata/2007-06/federationmetadata.xml to the federation service name; for example, https://sts.contoso.com/federationmetadata/2007-06/federationmetadata.xml.

The federation metadata should display something similar to that shown in Figure 6-12.

Finally, ensure that the service communication certificate is installed on each Web Application Proxy server.

SSO verification

To verify SSO, go to to the AD FS sign-in page (your federation service name appended with adfs/ls/idpinitiatedsignon.aspx; for example, https://sts.contoso.com/adfs/ls/idpinitiatedsignon.aspx.

You might need to set the EnableIdPInitiatedSignonPage property in AD FS to true.

```
(Get-AdfsProperties).EnableIdPInitiatedSignonPage
Set-AdfsProperties -EnableIdPInitiatedSignonPage $true
(Get-AdfsProperties).EnableIdPInitiatedSignonPage
```

Going to the idpinitatedsignon page should make it possible for you to test SSO by clicking the Sign In and Sign Out button without having to provide any of your credentials, as illustrated in Figure 6-13.

www.dbooks.org

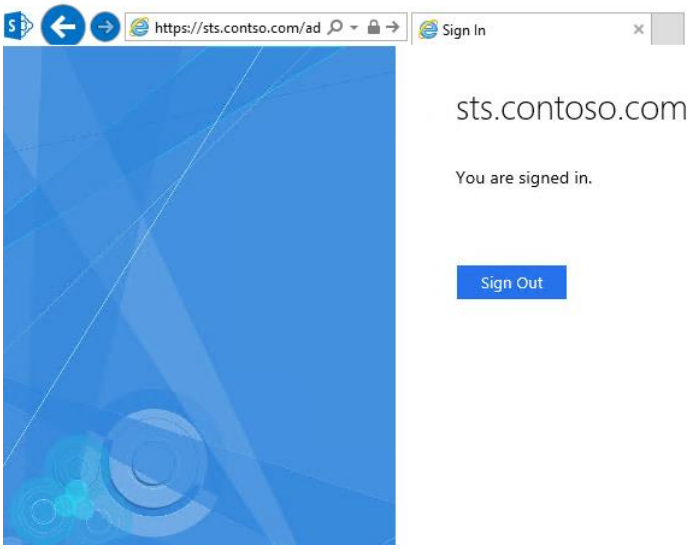


Figure 6-13: Performing an SSO test with the idpinitatedsignon page.

Verify SharePoint online SSO

Ensure that you can sign in to the Office 365 portal to verify that the user accounts for your local directory have been created. You should perform a test sign-in to your Office 365 tenant SharePoint online teamsite; for example, https://contoso.sharepoint.com.

If you are prompted for a user name and password, you would need to ensure that https://contoso.sharepoint.com is among the list of Local Intranet sites in your Internet properties. For example, you will see a Windows Security authentication prompt when connecting to https://contoso.sharepoint.com, as shown in Figure 6-14. You will see a message "Connecting to sts.contoso.com."

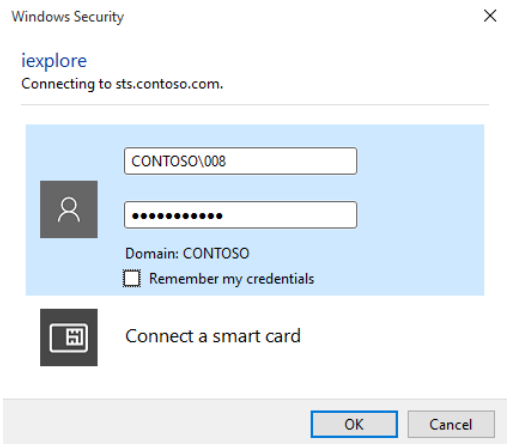


Figure 6-14: Windows security authentication prompt connecting to sts.contoso.com.

You are presented with an Office 365 sign-in page, as demonstrated in Figure 6-15. After you type in your email address, you will be automatically signed in. This is essential for the home realm discovery of the user; for example, username@contoso.com, where contoso.com is the home realm. If you select the Keep Me Signed In check box, you will never be signed out.

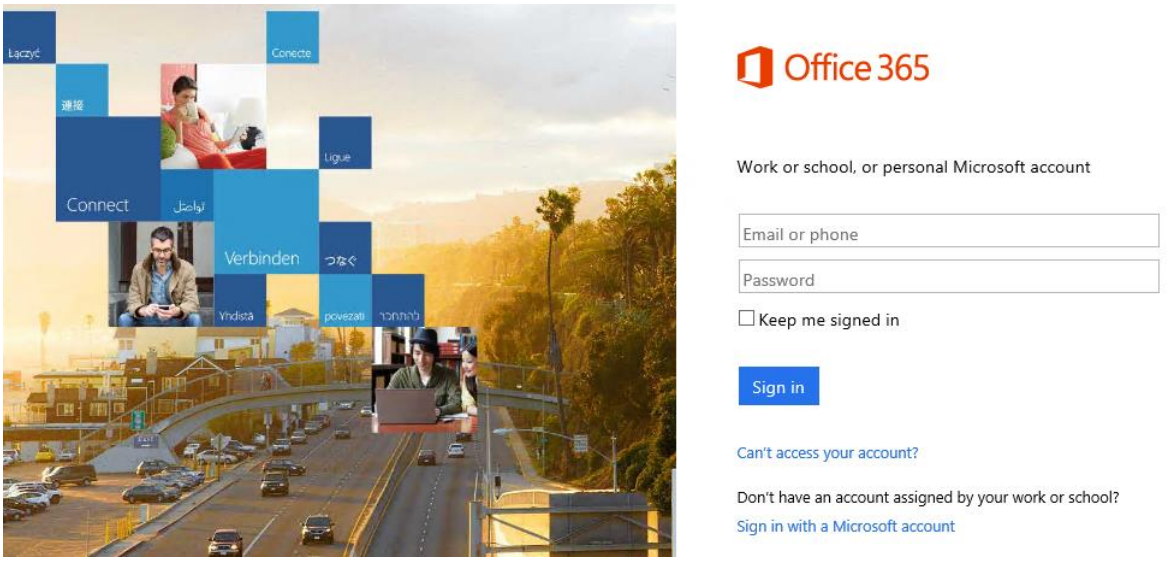


Figure 6-15: The Office 365 sign-in page.

Verify settings by using Azure AD Connect

You can also verify settings by opening up the Azure Active Directory Connect Wizard and selecting Verify ADFS Login (see Figure 6-16).

1. Type the global administrator credentials, such as globaladmin@contoso.onmicrosoft.com.
2. Provide the credentials of a domain administrator such as CONTOSO\domainadmin.
3. Type the credentials of a user that is already licensed and configured for AD FS.

The Azure Active Directory Connect Wizard will validate the credentials supplied against Azure AD and the AD FS STS hosted on-premises.

www.dbooks.org

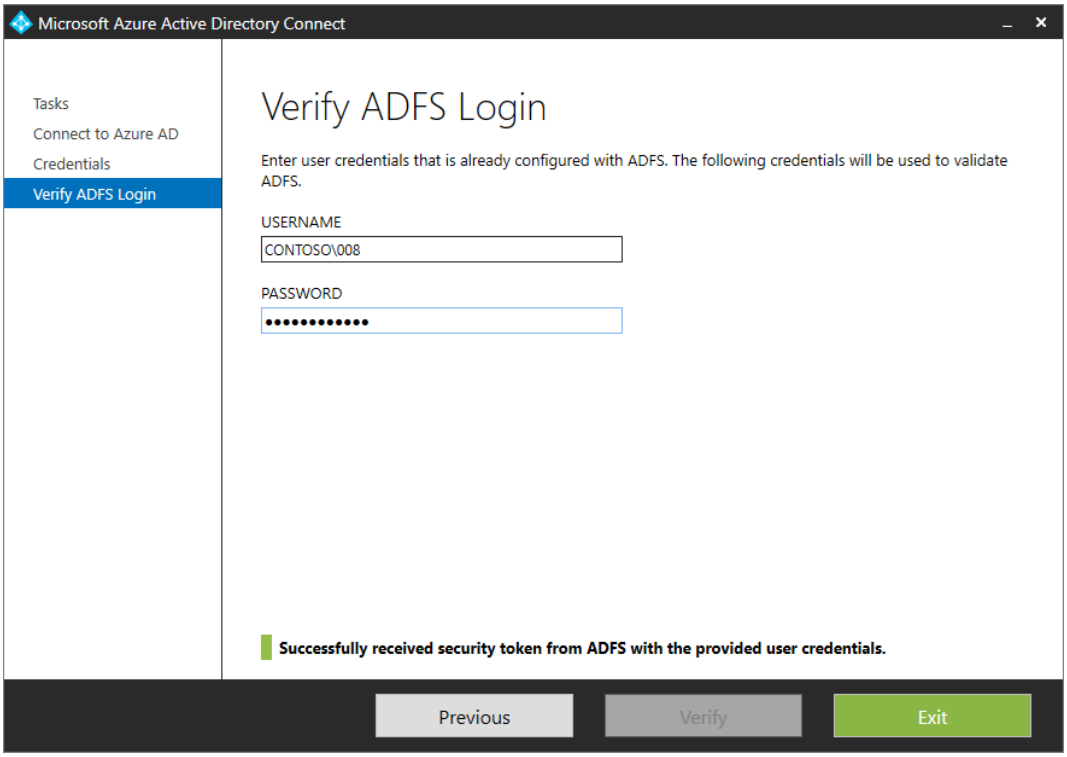


Figure 6-16: The Verify AD FS Login page in the Azure Active Directory Connect Wizard.

Validate your AD FS configuration

It is important to understand the AD FS settings while you are validating your current configuration.

Verify that you have a relying party trust with the following name in AD FS: Microsoft Office 365 Identity Platform, as shown in Figure 6-17.

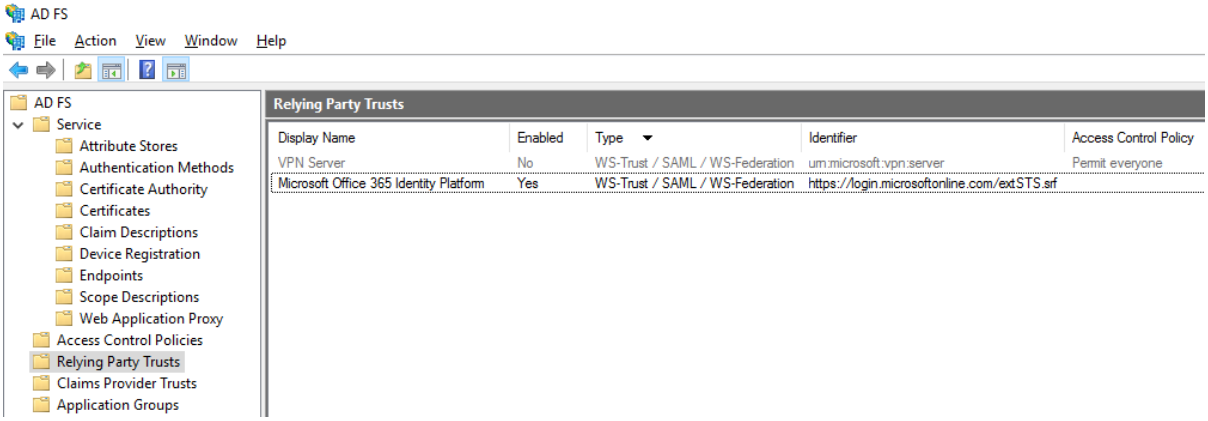


Figure 6-17: Microsoft Office 365 Identity Platform relying party trust displayed in AD FS.

Right-click the Microsoft Office 365 Identity Platform relying party trust and then, on the shortcut menu that opens, click Edit Claims Rules to view the rules created through the Azure Active Directory Connect Wizard, as shown in Figure 6-18.

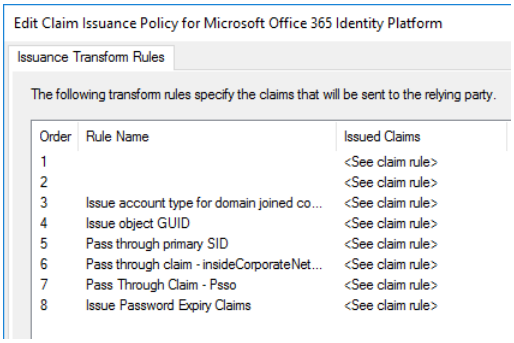


Figure 6-18: The claims rules for Microsoft Office 365 Identity Platform.

To validate your configuration, run the following Windows PowerShell commands on your AD FS Server:

```
Get-ADFSProperties
```

Figure 6-17 shows the output from that command.

```
PS C:\Users\Administrator.TEST> Get-AdfsProperties


AcceptableIdentifiers                   : {}
AddProxyAuthorizationRules              : exists([Type ==
                                          "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value
                                          == "S-1-5-32-544", Issuer =~ "^AD AUTHORITY$"]) => issue(Type =
                                          "http://schemas.microsoft.com/authorization/claims/permit", Value =
                                          "true");
                                                  c:[Type ==
                                          "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid",
                                          Issuer =~ "^AD AUTHORITY$" ]
                                                                  => issue(store="_ProxyCredentialStore",types=("http
                                          ://schemas.microsoft.com/authorization/claims/permit"),query="isProxyTrust
                                          ManagerSid({0})", param=c.Value );
                                                  c:[Type ==
                                          "http://schemas.microsoft.com/ws/2008/06/identity/claims/proxytrustid",
                                          Issuer =~ "^SELF AUTHORITY$" ]
                                                                  => issue(store="_ProxyCredentialStore",types=("http
                                          ://schemas.microsoft.com/authorization/claims/permit"),query="isProxyTrust
                                          Provisioned({0})", param=c.Value );
ArtifactDbConnection                    : Data Source=np:\\.\pipe\microsoft##wid\tsql\query;Initial
                                          Catalog=AdfsArtifactStore;Integrated Security=True
AuthenticationContextOrder              : {urn:oasis:names:tc:SAML:2.0:ac:classes:Password,
                                          urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport,
                                          urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient,
                                          urn:oasis:names:tc:SAML:2.0:ac:classes:X509...}
AuditLevel                              : {Basic}
AutoCertificateRollover                 : True
CertificateCriticalThreshold            : 2
CertificateDuration                     : 365
CertificateGenerationThreshold          : 20
CertificatePromotionThreshold           : 5
CertificateRolloverInterval             : 720
CertificateSharingContainer             : CN=c3961d3f-6691-4dc1-9d0f-17eb107d3505,CN=ADFS,CN=Microsoft,CN=Program
                                          Data,DC=test,DC=local
CertificateThresholdMultiplier          : 1440
ClientCertRevocationCheck               : None
```

Figure 6-19: Verify settings with the output of Get-AdfsProperties.

Note the settings displayed after running the command. Observe the certificate-related attributes such as the following:

- AutoCertificateRollover Default value: True

  This specifies whether the system will manage certificates for the administrator and generate new certificates before the expiration date of current certificates. You can choose to modify the token signing certificate and the token decryption certificate by turning off automatic certificate rollover by running the Windows PowerShell command Set-AdfsProperties -AutoCertificateRollver $false.

- CertificateCriticalThreshold Default value: 2 days

  Specifies the period of time (in days) before a current primary signing or decryption certificate expires. When this threshold occurs, the federation service initiates the autorollover service, generates a new certificate, and promotes it to be the primary certificate. This rollover process occurs even if the critical threshold interval does not provide sufficient time for partners to

www.dbooks.org

replicate the new metadata. This should be a short period of time that is used only in extreme conditions when the federation service has not been able to generate a new certificate in advance.

- CertificateGenerationThreshold Default value: 20 days

  Specifies the period of time (in days) before a new primary certificate is generated to replace the current primary certificate. When this threshold occurs, the federation service initiates an autorollover process that generates a new certificate and adds it to the secondary collection. This rollover process occurs so that federation partners can consume this metadata in advance and trust is not broken when this newly generated certificate is promoted to be a primary certificate.

- CertificatePromotionThreshold Default value: 5 days

  Specifies the period of time (in days) during which a newly generated certificate remains a secondary certificate before being promoted to be the primary certificate.

More info To read more about the attributes for Get-AdfsProperties, go to https://technet.microsoft.com/library/ee892317.aspx.

Troubleshooting SSO issues

Chapter 5 covers troubleshooting issues related to directory synchronization. For more assistance with troubleshooting Azure AD Connect issues, refer to the troubleshooting synchronization issues there. As mentioned in Chapter 5, Azure AD Connect writes its trace logs to C:\Users\%username%\AppData\Local\AADConnect. Looking up the trace log files can be a great place to begin troubleshooting Azure AD Connect issues.

This section focusses on issues involving AD FS and SSO. The following points are meant to assist you in troubleshooting a variety of common issues associated with configuring and managing SSO.

- Event logs

  AD FS and the AD FS proxy capability in Web Application Proxy servers log events to Applications and Services Logs\AD FS\Admin, as illustrated in Figure 6-20.

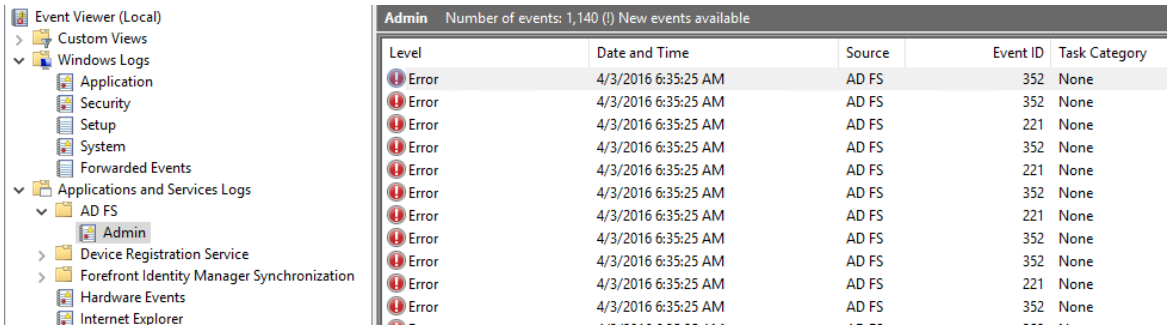


Figure 6-20: AD FS Admin events logged under Application and Services Logs.

  The Application, Security, and System events are important places to look for troubleshooting warnings and errors, too.

- Issues creating the Azure AD Trust

  You might receive the following error when running the Convert-MsolDomaintoFederated command or via the Azure Active Directory Connect Wizard (see also Figure 6-21):

  The remote name could not be resolved 'nexus.microsoftonline-p.com'

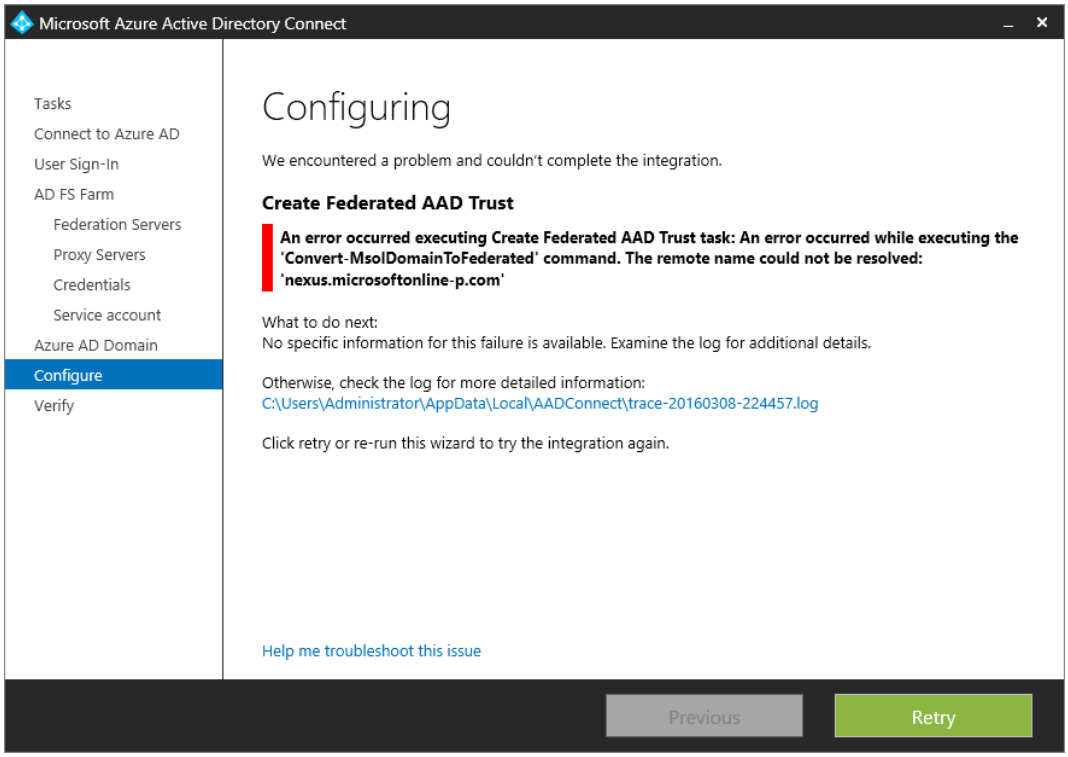


Figure 6-21: When you run the Convert-MsolDomaintoFederated command, you might see this message if the remote name could not be resolved

You would need to ensure that the server on which you running the Azure Active Directory Connect Wizard or Windows PowerShell command has access to the following URL: https://nexus.microsoftonline-p.com/FederationMetadata/2006-12/FederationMetadata.xml.

Also ensure that you are able to resolve the domain names nexus.microsoftonline-p.com, login.microsoftonline.com, and ppsanamespace.service.microsoftonline-p.net from the server.

- Web Application Server resolving the internal federation service name; for example, sts.contoso.com

  You might receive an error such as "The remote name could not be resolve 'sts.contoso.com' when you configure the Web Application Proxy server or run the Windows PowerShell command Install-WebApplicationProxy."

  An error occurred when attempting to establish a trust relationship with the federation service. Error: The remote name could not be resolved: 'sts.contoso.com'

  You would need to ensure that the Web Application Proxy server can resolve the internal federation service name, such as sts.contoso.com, as illustrated in the Figure 6-21. You need to create an entry in the Web Application Proxy Server HOSTS file to resolve the federation service name to point to the AD FS server.

- Web Application Proxy server errors when attempting to establish a trust relationship with the federation service

  You might receive an error similar to that shown in Figure 6-22 when running the Install-WebApplicationProxy command or using the Azure Active Directory Connect Wizard during the configuration of the Web Application Proxy.

www.dbooks.org

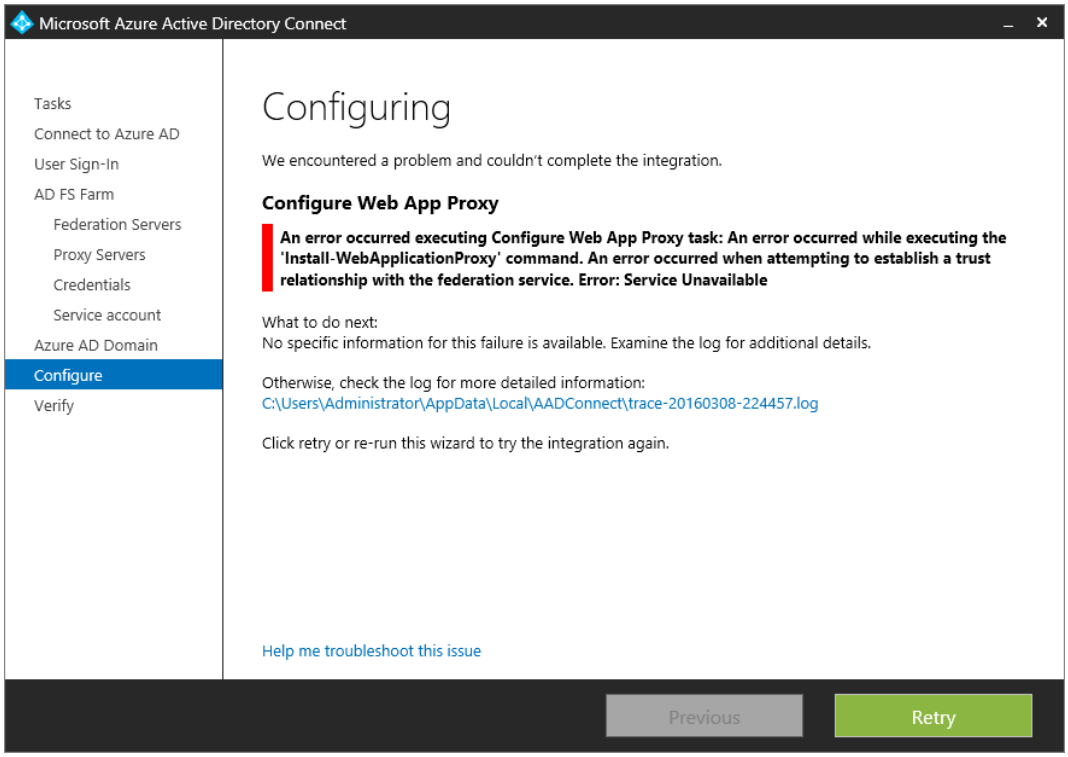


Figure 6-22: An error occurred when attempting to establish a trust relationship with the federation service. Error: Service Unavailable

This issue can occur due to a variety of reasons:

- The AD FS server cannot be reached from the Web Application Proxy server due to a network or communications issue such as the load-balanced VIP.
- A firewall blocked connectivity between the Web Application Proxy server and the AD FS server.
- The AD FS and related Windows services have not started. Ensure that the following Windows service is running:

  AD FS server Active Directory Federation Services

  I recommend that you restart the AD FS server or farm to test if this service starts each time.
- AD FS might have issues connecting to its database. Check the connectivity to the SQL server or the state of the Windows Internal Database.

- Troubleshoot SSO by using the Remote Connectivity Analyzer

  You can diagnose SSO issues by using tools such as the Remote Connectivity Analyzer. This is a cloud-based app that is provided by Microsoft to troubleshoot common Office 365 problems. It validates the ability to sign in to Office 365 with your on-premises credentials and performs basic AD FS configuration.

  To run Remote Connectivity Analyzer, go to https://testconnectivity.microsoft.com, and then click the Office 365 tab. In the Office 365 General Tests section, select Office 365 Single Sign-On Test, as depicted in Figure 6-23.

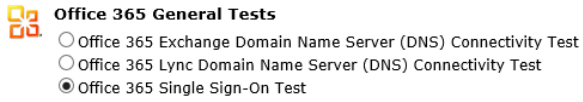


Figure 6-23: The Office 365 Single Sign-On Test is available in the Remote Connectivity Analyzer.

Follow the steps shown in Figure 6-24 to perform the test and, review the results, and ensure that you address any reported issues.

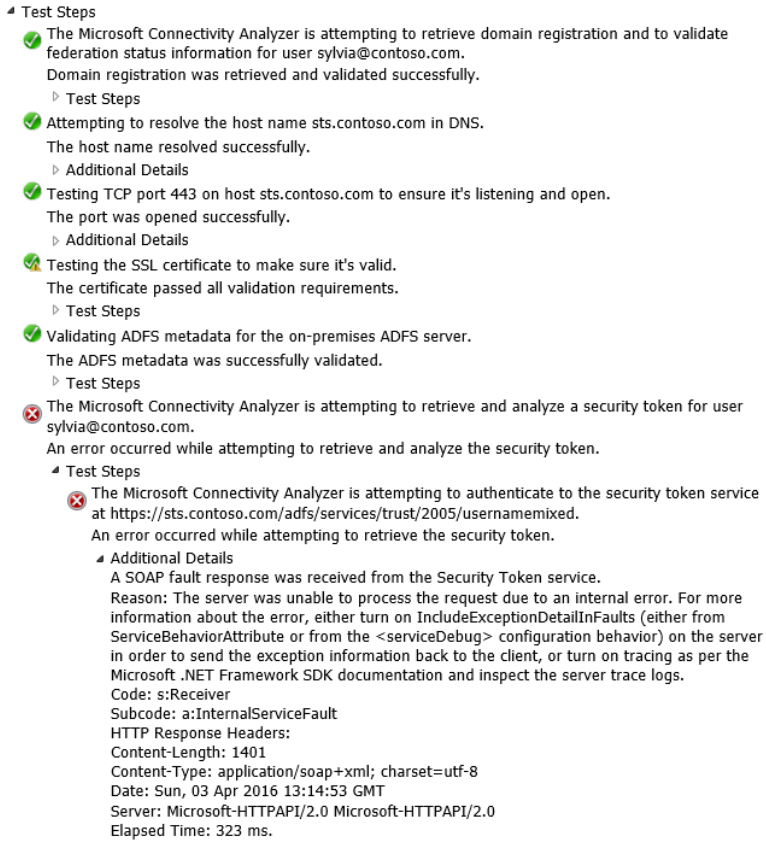


Figure 6-24: The results of the Office 365 Single Sign-On Test displaying an error connecting to the STS.

- Office 365 Client Performance Analyzer

  The Office 365 Client Performance Analyzer is designed to diagnose network performance issues. This is a downloadable .msi file and that can run on server and desktop operating systems. It has the ability to run in the background and gather performance statistics for you. To download the Office 365 Client Performance Analyzer, go to http://go.microsoft.com/fwlink/p/?LinkId=506979. When you install and run the app, you see the screen shown in Figure 6-25.

www.dbooks.org

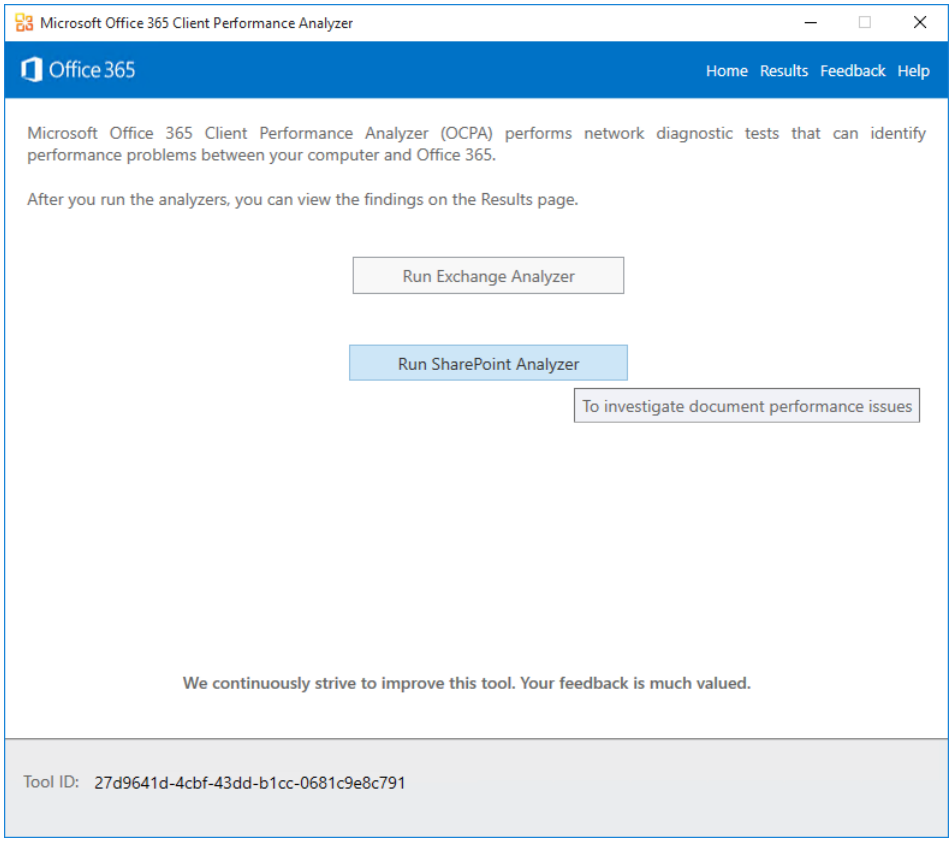


Figure 6-25: The Microsoft Office 365 Client Performance Analyzer.

Azure AD Connect Health

Azure AD Connect Health is a feature of Azure AD premium that provides insights about health, performance, and sign-in activity with AD FS–enabled federated identity systems. Azure AD Connect Health helps organizations monitor the reliability of AD FS, which is a critical component for federated identity authentication.

A downloadable health agent is available for AD FS monitoring and reporting. Azure AD Connect Health for AD FS supports AD FS 2.0 on Windows Server 2008 R2, AD FS in Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016. Azure AD Connect Health also includes support for AD FS Proxy servers and Web Application Proxy servers with AD FS proxy configured.

You need to turn on auditing on AD FS so that Azure AD Connect Health can collect the required usage analytics. For specific steps, go to http://go.microsoft.com/fwlink/?LinkId=532545.

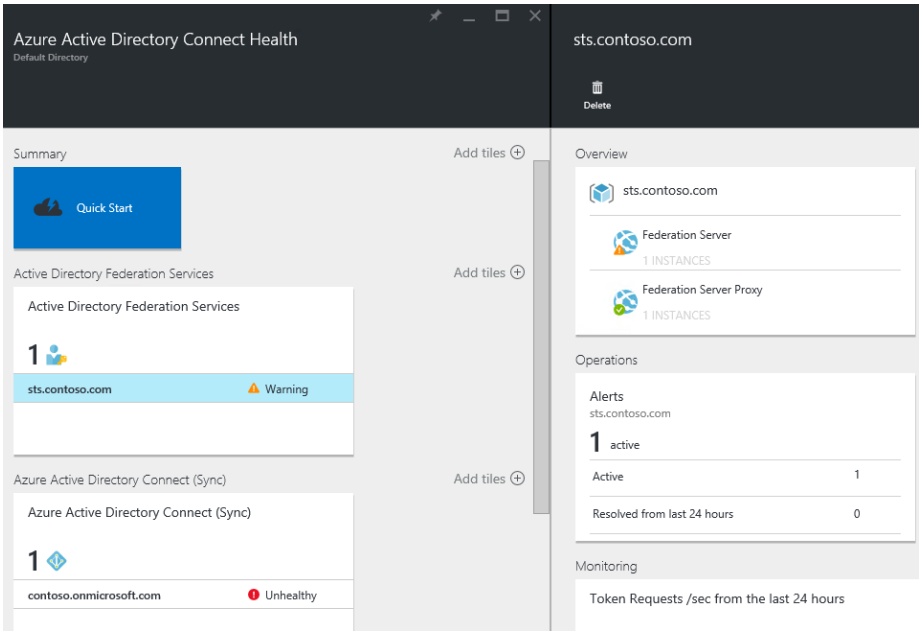


Figure 6-26: The dashboard for the Azure Active Directory Connect Health app.

> **Note** To access the Azure AD Connect Health, go to https://aka.ms/aadconnecthealth.

The following points summarize the main capabilities of Azure AD Connect Health for AD FS:

- Monitoring of AD FS, AD FS Proxy, and Web Application Proxy server health.
- Email alerts of critical health events, configuration information, and synthetic transactions.
- Performance and usage data trend analysis with forecasting.
- Graph reporting for AD FS usage insights (requires that auditing is turned on for AD FS servers) with multiple pivots. Audits are generated by the user's sign-in and activities for applications.
- Reporting on key performance indicators across multiple servers, such as processor, memory, and latency.

Azure AD Connect Health for Sync monitors the on-premises Azure AD Synchronization engine. The following are the main capabilities of Azure AD Connect Health for Sync:

- Monitoring the health of the Azure AD Connect synchronization engine
- Alerts if degradation is detected in the synchronization engine's health
- synchronization operational insights including latency charts for Sync Operations
- Reporting with forecasting for synchronization operations such as object adds, deletes, and renames.

> **More info** For more information on Azure AD Connect Health, go to http://go.microsoft.com/fwlink/?LinkID=618587.

www.dbooks.org

About the author



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. With cyber security and the cloud in mind, Jeremy has undergone cyber security training and is a Certified Ethical Hacker (CEH) from EC-Council.

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.



From technical overviews to drilldowns on special topics, get *free* ebooks from Microsoft Press at:

www.microsoftvirtualacademy.com/ebooks

Download your free ebooks in PDF, EPUB, and/or Mobi for Kindle formats.

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

www.dbooks.org