



Cloud Access Manager 8.1.4

How to Configure Microsoft Office 365

Copyright 2018 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Contents

Introduction	4
Prerequisites	4
Installing Cloud Access Manager	5
Adding Microsoft Office 365 to Cloud Access Manager	6
Testing Office 365	8
Adding Microsoft Outlook to the Cloud Access Manager applications portal	12
Using Microsoft Lync	14
Adding Microsoft SharePoint to the Cloud Access Manager applications portal	16
Useful download links	18
About us	20
Contacting us	20
Technical support resources	20

Introduction

This guide describes how to configure Microsoft Office 365 for use with Cloud Access Manager and how to add Microsoft Outlook, Lync, Word, Excel and PowerPoint to the Cloud Access Manager applications portal.

Prerequisites

If required, you can obtain a free 30 day trial of Microsoft Office 365 at:

<http://office.microsoft.com/en-gb/try>

Make sure the following prerequisites are met before configuring Office 365 for use with Cloud Access Manager

1. You will need:

- An external domain name hosted by a provider that allows you to modify the Domain Name System (DNS) records for your domain. This must include support for adding A, CNAME, SRV and either MX or TXT records.
- A wildcard Secure Sockets Layer (SSL) certificate signed by one of the Certificate Authorities trusted by Microsoft. Free SSL certificate providers are unlikely to work and self-signed certificates cannot be used.

NOTE: We recommend that you choose a Certificate Authority that is listed in an up-to-date Windows Server 2008/2012 under Third Party Root Certificate Authorities. A regular single hostname certificate can be used, but a wildcard certificate is recommended if you will be using Cloud Access Manager to proxy other applications.

- An external IP address that will be used to forward TCP ports 80 and 443 to the Cloud Access Manager proxy
- To add a wildcard DNS entry for your Cloud Access Manager proxy that resolves to the external IP address of the proxy, for example *.webapps.democorp.co.uk
- A minimum of two hosts; a production two host installation of Cloud Access Manager is required for this configuration of Office 365 for Cloud Access Manager
- A local instance of Microsoft Active Directory
- A copy of Office 2013 is required on any client browser server where the desktop Office clients will interact with Office 365. It is required to test configuration of the Lync and Outlook clients as described in [Adding Microsoft Outlook to the Cloud Access Manager applications portal](#) and [Using Microsoft](#)

Lync. You can download Office 2013 using your Office 365 account but this may take some time to complete. Earlier versions of Office are also supported by Office 365 (patches may be required), but with degraded functionality.

NOTE: Make sure that the following prerequisites, including the PowerShell execution policy in Step 2, are installed on all STS servers in the Cloud Access Manager deployment.

- The default version of Microsoft .NET Framework and Windows PowerShell supplied with Microsoft Windows Server 2008 R2 or Microsoft Windows Server 2012
 - To install Microsoft Windows updates
 - Microsoft Online Services Sign-In Assistant, msoidcli_64.msi
 - Windows Azure Active Directory Module for Windows PowerShell, AdministrationConfig-EN.msi
2. The PowerShell execution policy must be set to RemoteSigned using the following command:
- ```
PS> Set-ExecutionPolicy RemoteSigned
```

## Installing Cloud Access Manager

### ***To install Cloud Access Manager as a standard two host production system***

1. Make sure that you have installed Cloud Access Manager as described in the *One Identity Cloud Access Manager Installation Guide* and that you have configured an Active Directory front-end authentication method as recommended in the *One Identity Cloud access Manager Configuration Guide*.
2. Verify your configuration by confirming that a user on a domain connected workstation can single sign-on (SSO) to the portal without being prompted for their AD credentials, and that the browser shows the portal is using a trusted Secure Sockets Layer (SSL) certificate. The ability to SSO and a signed SSL certificate are required to perform SSO to Microsoft Office 365.
3. For domain connected users the experience with Microsoft Office 365 will be enhanced if Kerberos SSO is enabled on the domain. This allows SSO into Office 365 rich clients, such as Lync and Outlook, without requiring users to re-enter their credentials.

**NOTE:** Enabling SSO in the browser affects the Primary Credentials functionality in Cloud Access Manager; please refer to the *One Identity Cloud access Manager Configuration Guide* for details.

# Adding Microsoft Office 365 to Cloud Access Manager

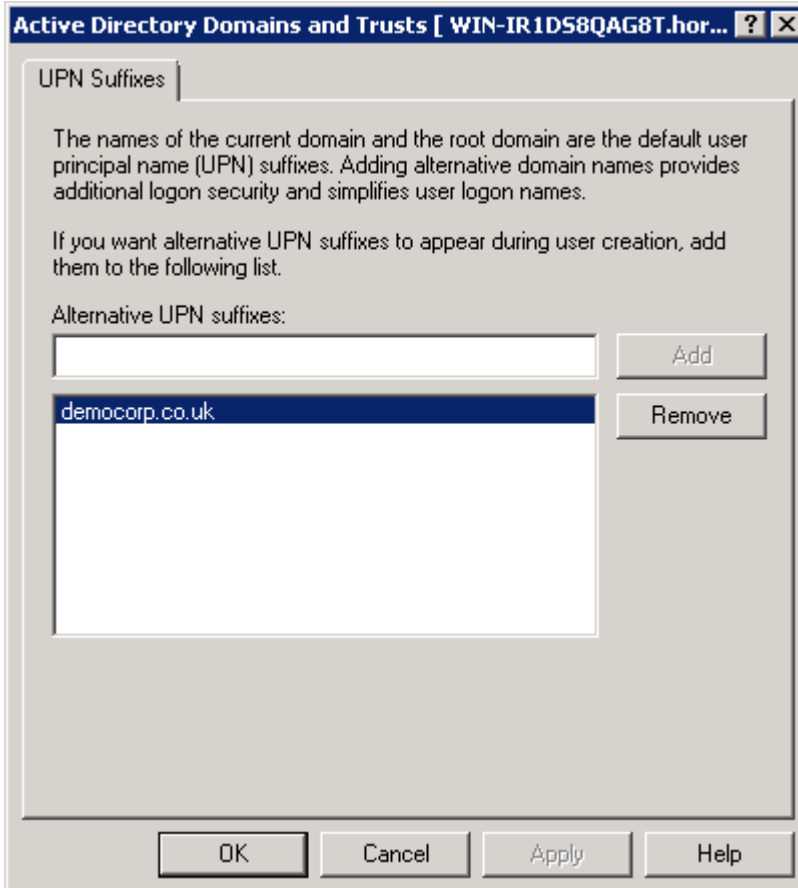
## To configure Office 365

1. Add the Office 365 application to Cloud Access Manager using the Office 365 template. Follow the steps in the wizard, making sure that you enable provisioning and click **Get Additional Options** to retrieve your available license plans. Select all of the available license plans.
2. On completion of the wizard, make a note of the federated settings, Relying Party Endpoint URL, Relying Party Realm /Identity, Certificate String and Endpoint URL.
3. Log in to <https://portal.microsoftonline.com> using your Office 365 administrator credentials and click **Domains** in the navigation bar.
4. Click **Add a domain**, then follow the steps in the wizard to register your domain with Office 365.

Depending on which provider is hosting your domain, you may need to manually configure the Domain Name System (DNS) for your domain using the details provided by the wizard.

**NOTE:** When adding your domain to Office 365 do not make it the default domain. It is not necessary to make it the default domain and it stops the Set-MsolDomainAuthentication powershell command (see step 9) from running successfully.

5. When your domain has been added and verified successfully, close the Office 365 administration console.
6. In Active Directory, add your Office 365 domain as a User Principal Name (UPN) suffix using Active Directory Domains and Trusts. Right-click the top node, then select Properties to access the UPN suffixes dialog.



7. Open a PowerShell command prompt.
8. Connect to Office 365 using the following cmdlet which will prompt for your Office 365 administrator credentials.
  - 1 Connect-MsolService
9. Run the following command to configure your new domain as a federated domain:
  - 2 Set-MsolDomainAuthentication `
  - Authentication federated `
  - DomainName democorp.co.uk `
  - ActiveLogOnUri
  - https://www.webapps.democorp.co.uk/CloudAccessManager/RPSTS/WSTrust/Service
  - .svc/trust/username `
  - FederationBrandName "Cloud Access Manager" `
  - IssuerUri urn:www.webapps.democorp.co.uk/CloudAccessManager/RPSTS `
  - LogOffUri
  - https://www.webapps.democorp.co.uk/CloudAccessManager/RPSTS/WSFed/Default.a
  - spx `
  - MetadataExchangeUri
  - https://www.webapps.democorp.co.uk/CloudAccessManager/RPSTS/WSTrust/Service
  - .svc/mex `
  - NextSigningCertificate "" `

```
-PassiveLogOnUri
https://www.webapps.democorp.co.uk/CloudAccessManager/RPSTS/WSFed/Default.a
spx
-SigningCertificate "MIID0zCCAiOg --//-- idCtmMQpRNqT"
3
```

10. Run the following command to verify the domain federation settings:

```
4 Get-MsolDomainFederationSettings -DomainName democorp.co.uk
```

You should see the following output:

```
ActiveLogOnUri :
https://www.webapps.democorp.co.uk/CloudAccessManager/RPSTS/WSTrust/Service
.svc/trust/username
FederationBrandName : Cloud Access Manager
IssuerUri : urn:www.webapps.democorp.co.uk/CloudAccessManager/RPSTS
LogOffUri :
https://www.webapps.democorp.co.uk/CloudAccessManager/RPSTS/WSFed/Default.a
spx
MetadataExchangeUri :
https://www.webapps.democorp.co.uk/CloudAccessManager/RPSTS/WSTrust/Service
.svc/mex
NextSigningCertificate :
PassiveLogOnUri :
https://www.webapps.democorp.co.uk/CloudAccessManager/RPSTS/WSFed/Default.a
spx
SigningCertificate :
MIIC8DCCAdigAwIBAgIQALTSvTAuaEIJ2DvWxvPYHTANBgqhkiG9w0BAQUFADAzMTEwLwYDVQ
QDDChEZWxsIENsb
3VkJEFjY2VzcyB5BNYw5hZ2Z2VjIEFwcCBPZmZpY2UgMzY1MCAXDTE0MDMwNDAwMDAwMFOYDzIwN
T...
```

11. To edit or update the domain federation settings, use the Set-MsolDomainFederationSettings command with the appropriate parameters.

For example, to update the signing certificate:

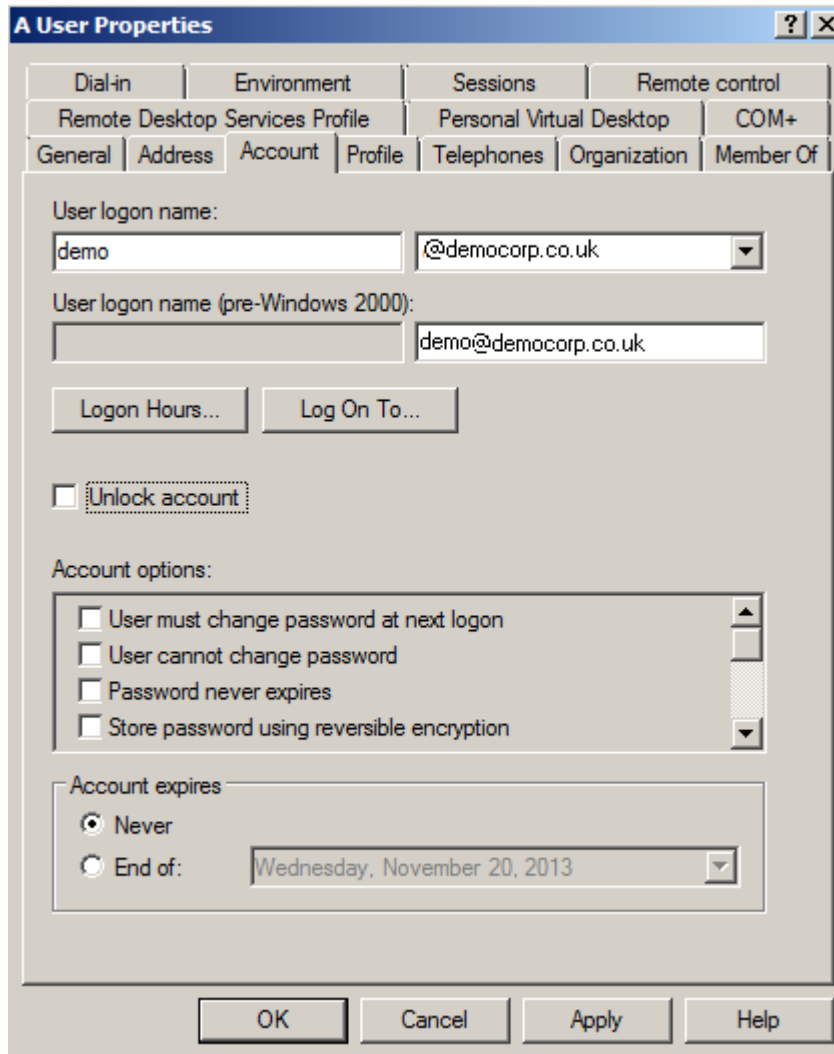
```
Set-MsolDomainFederationSettings -DomainName democorp.co.uk -SigningCertificate
"MIIC8DCCAdig --//-- SPQTHw9aYYeC"
```

## Testing Office 365

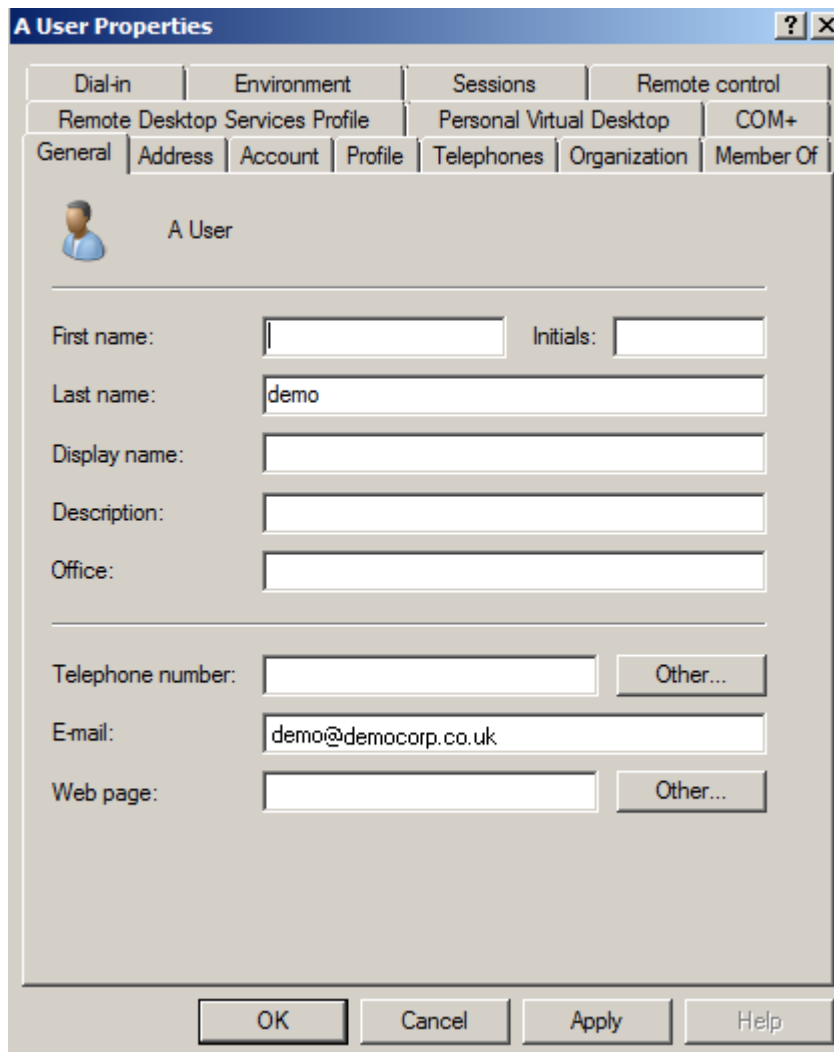
### To test Microsoft Office 365

1. Create a new user in Active Directory.
2. Set the new user's User Principal Name (UPN) suffix to be your Office 365 domain.

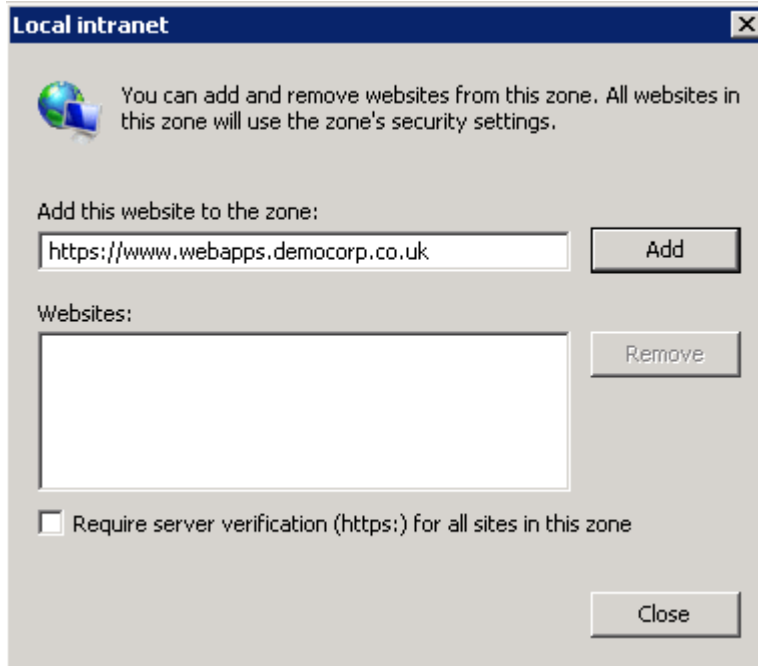




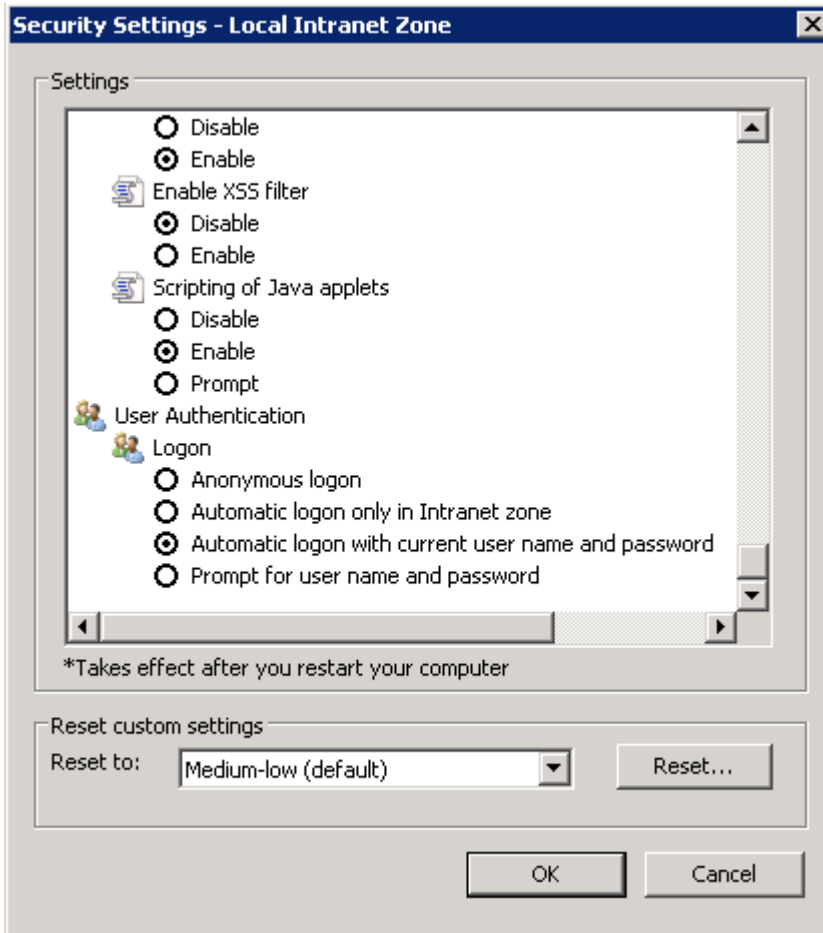
3. Make sure that the user has an email address defined within the Office 365 domain.



4. Log in to Windows as the new user.
5. Access Cloud Access Manager using Internet Explorer.
6. Add Cloud Access Manager to the Internet Explorer Local intranet zone.



7. On the **Security Settings - Local Intranet Zone** page, make sure that **Automatic logon with current user name and password** is selected.



8. Close Internet Explorer.
9. Check that you can access Cloud Access Manager without providing a username and password.


## Adding Microsoft Outlook to the Cloud Access Manager applications portal

### *To add Microsoft Outlook to the Cloud Access Manager applications portal*




1. Log in as the new user and log in to Cloud Access Manager.
2. Add **Outlook** to the portal using the applications catalog.
3. Return to the Cloud Access Manager applications portal and click **Outlook** to verify that this button opens the Web version of Outlook.
4. Run the Outlook connectivity test as the new user. You will see results similar to those on the **Microsoft Remote Connectivity Analyzer** page shown below. At

least one auto discovery method must be successful.

Microsoft®  
Remote Connectivity Analyzer

 Connectivity Test Successful with Warnings

**Test Details** Start Over Run Test Again

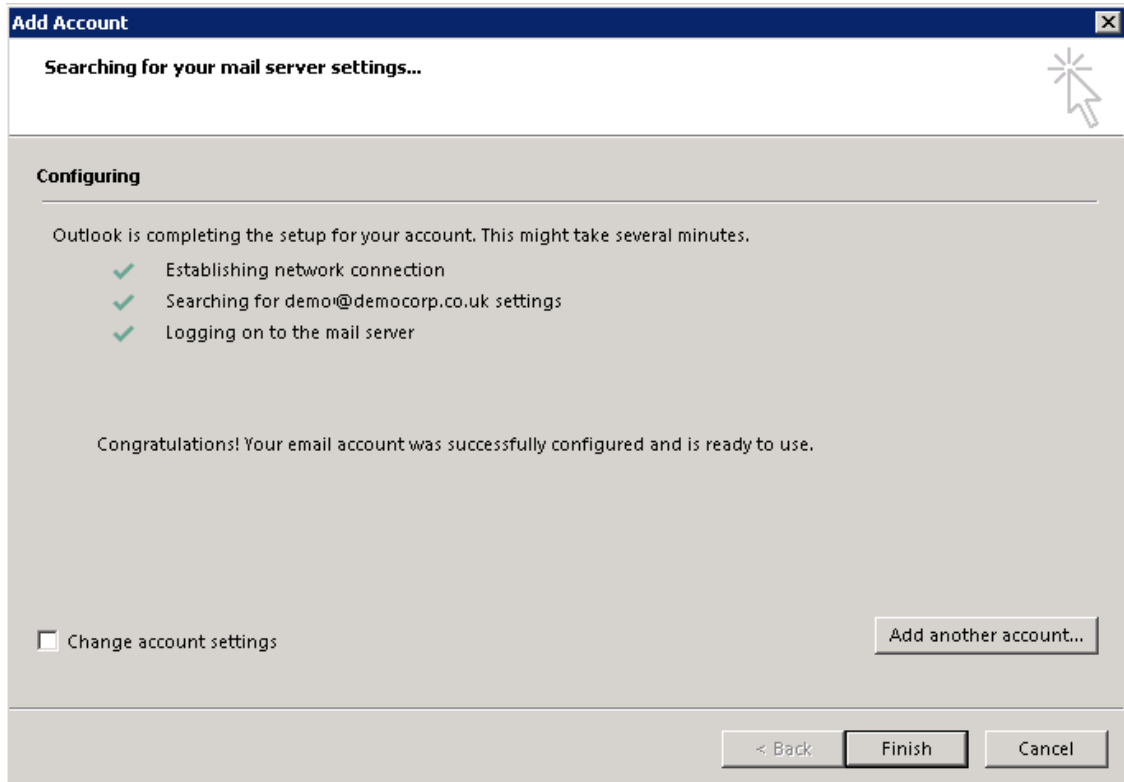
Expand All   

- Attempting the Autodiscover and Exchange ActiveSync test (if requested).  
Autodiscover was successfully tested for Exchange ActiveSync.
  - Test Steps
    - Attempting each method of contacting the Autodiscover service.  
The Autodiscover service was tested successfully.
      - Test Steps
        - Attempting to test potential Autodiscover URL `https://democorp.co.uk/AutoDiscover/AutoDiscover.xml`  
Testing of this potential Autodiscover URL failed.
          - Test Steps
        - Attempting to test potential Autodiscover URL `https://autodiscover.democorp.co.uk/AutoDiscover/AutoDiscover.xml`  
Testing of this potential Autodiscover URL failed.
          - Test Steps
        - Attempting to contact the Autodiscover service using the HTTP redirect method.  
The Autodiscover service was successfully contacted using the HTTP redirect method.
          - Test Steps

Start Over Run Test Again

5. Start the desktop version of Outlook 2013.
6. Follow the **Add Account** wizard to set up a new account based on the user's detected email address.

**NOTE:** You may be prompted for the user's credentials more than once. Select **Remember password**.



7. When Outlook is open, select the bottom-right status bar to view any connectivity errors.
8. To check that the address book is working, send an email to the user by entering their full name, not their email address. Check that the user receives the email.

## Using Microsoft Lync

### ***To add Microsoft Lync to the Cloud Access Manager applications portal***

1. Open the desktop version of Microsoft Lync.
2. If you are using a computer that is a member of a domain, enter your user name in the sign-in address. There is no need to enter your password.



# Lync®

## Sign in



Sign-in address:

[Delete my sign-in info](#)

[Need help signing in?](#)

Sign in as:

© Microsoft Corporation. All rights reserved.

- 1 **NOTE:** If you are using a computer that is not a member of a domain, enter your user password, and select the **Save my password box** and click **Yes** to save the sign-in information for next time.



## Do you want us to save your Lync sign-in info?

Would you like us to save this info and sign you in automatically next time?

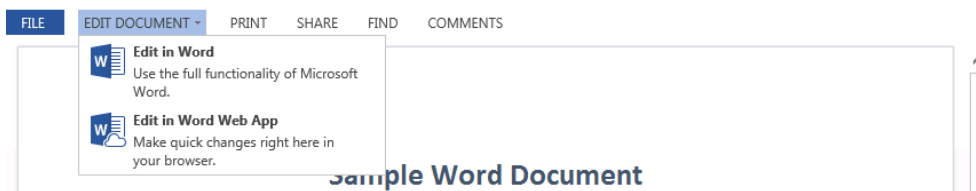
3. To confirm connectivity with Microsoft Exchange Server, check that the meeting icon is displayed in the top left corner of the Lync dialog box shortly after log in. If a user is not currently signed in to Outlook, they will be prompted for their Exchange credentials. This is true for both domain and non-domain joined users.

# Adding Microsoft SharePoint to the Cloud Access Manager applications portal

This section describes how to add Microsoft SharePoint to the Cloud Access Manager applications portal and how to configure it to work with Microsoft Word. You can also use these instructions to configure Microsoft Excel and PowerPoint with SharePoint.

## To add Microsoft SharePoint

1. Add **SharePoint** to the portal using the applications catalog.
2. Return to the portal and click **SharePoint** to verify that the new button opens the SharePoint Team Site.
3. Add a new Word document or open an existing Word document, and verify that it opens in the web version of Word.
4. Click **Edit Document**, then **Edit in Word**.



5. The desktop version of Word opens and you are prompted to enter the user's Office 365 email address.





# Sign in

Call us overprotective, but we need to verify your account again before opening this document.

Next

When you sign in, your documents and settings are online

[Learn more](#) | [Privacy statement](#)

6. Next, you are prompted to enter the user's password. Be sure to select the **Keep me signed in** box.



# Sign In

User ID:

Password:

Keep me signed in

Can't access your account?

© 2012 Microsoft Corporation  
Privacy | Legal

7. Verify that you can open, edit and save the document correctly.

## Useful download links

### Manage Azure Active Directory using Windows PowerShell Documentation

<http://technet.microsoft.com/en-us/library/jj151815.aspx>

### Microsoft Online Services Sign-In Assistant

<http://www.microsoft.com/en-gb/download/details.aspx?id=28177>

### Windows Azure Active Directory Module for Windows PowerShell 64-bit version

<http://go.microsoft.com/fwlink/p/?linkid=236297>

## **Update Microsoft Office 2010 to work with Office 365**

<https://support.office.com/en-us/article/Set-up-Office-2010-desktop-programs-to-work-with-Office-365-for-business-3324B8B8-DCEB-45E2-AC24-C642720108F7>

## **Update Microsoft Office 2013 to work with Office 365**

<https://support.microsoft.com/en-gb/gp/office-2013-365-update>

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

## Contacting us

For sales or other inquiries, visit <https://www.oneidentity.com/company/contact-us.aspx> or call +1-800-306-9329.

## Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at [www.YouTube.com/OneIdentity](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product