



Cloud Access Manager 8.1.4

How to Configure Microsoft
SharePoint

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
Cloud Access Manager configuration prerequisites	4
Adding Microsoft SharePoint to Cloud Access Manager using WS-Federation	4
Configuring a SharePoint 2010 or 2013 WS-Federation Trust using the Cloud Access Manager for Microsoft SharePoint utility	6
Installing Cloud Access Manager for SharePoint	7
Establishing a trust between Cloud Access Manager and SharePoint	7
Manual configuration of a SharePoint 2013 Server WS-Federation Trust	8
Manual configuration of a SharePoint 2010 Server WS-Federation Trust	9
Protecting your SharePoint website with Cloud Access Manager	10
Enabling SharePoint People Picker functionality	11
Using the SharePoint People Picker	13
Adding Microsoft SharePoint to Cloud Access Manager using the reverse proxy	15
Troubleshooting	18
About us	19
Contacting us	19
Technical support resources	19

Introduction

This guide describes how to configure Microsoft SharePoint for use with Cloud Access Manager. Cloud Access Manager now supports two configuration options for Microsoft SharePoint, the Cloud Access Manager WS-Federation application template supports both SharePoint 2010 and SharePoint 2013 to simplify and automate application configuration.

In addition, you can configure the Cloud Access Manager reverse proxy to provide Single Sign-On (SSO) to web applications by automatically filling in the login form, or using either Integrated Windows Authentication (IWA) or Basic Authentication. You can also use the reverse proxy to enable secure access to internal web apps from the internet. For further information, please refer to the *One Identity Cloud Access Manager Security and Best Practices Guide*.

Cloud Access Manager configuration prerequisites

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

1. Install Cloud Access Manager as described in the *One Identity Cloud Access Manager Installation Guide* and configure 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 sign on to the portal using their Active Directory credentials and that the browser shows the portal is using a trusted Secure Sockets Layer (SSL) certificate. The ability to authenticate and an SSL certificate signed by a recognized Trusted Certification Authority are required to perform SSO to SharePoint 2013.

Adding Microsoft SharePoint to Cloud Access Manager using WS-Federation

To add SharePoint to Cloud Access Manager using the WS-Federation application template

1. Add the SharePoint application to One Identity Cloud Access Manager using the SharePoint 2010/2013 template.
2. Set the SharePoint server web application URL and the site folder.
3. Configure a realm name to later identify this connection in SharePoint.
4. Click **Save & Next**.

NOTE: While SharePoint server may include multiple sites, the Cloud Access Manager template will only auto-configure one of them for you. You can add others manually as extra application portal links when the initial SharePoint application has been created.

NOTE: The relying party realm may be any value you choose, with urn: as its prefix, for example urn:cam-sharepoint. You will enter this value in SharePoint later when you create the new authenticator.

Settings for SharePoint 2010 / 2013

Please enter the SharePoint web application URL

http://win12.sharepoint2013.local:80

Please enter the SharePoint site folder

sites/sharepoint2013

Please enter the realm SharePoint will use to identify itself

urn:cam-sharepoint

The following Application Portal links will be created

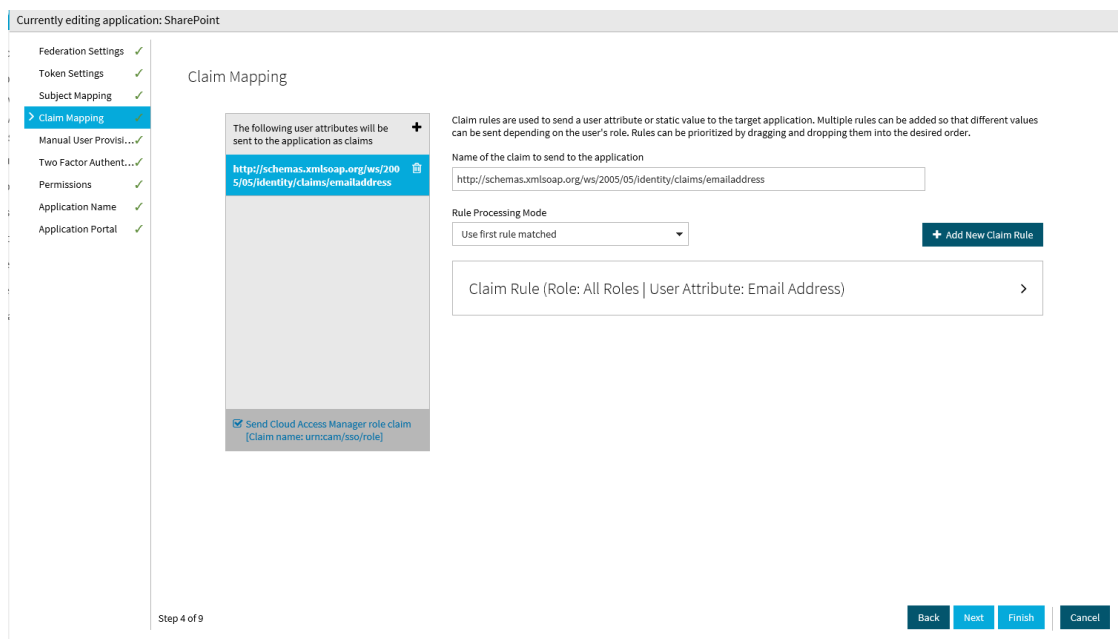
SharePoint

5. In **Subject Mapping** you must specify the attribute that Cloud Access Manager will use to derive the user's name for log in. The default attribute is **mail**. Click **Next**.

On the **Claim Mapping** page you can configure the values Cloud Access Manager will pass to SharePoint in the form of claims. By default only a user's email address is required to successfully authenticate. If you need to pass other values, for example employee id, you can add further claims on the **Claim Mapping** page and populate them with the appropriate values from the relevant front-end authenticator.

You will also need to create the associated claim type mappings when you create the new claims-based authenticator in SharePoint. The Cloud Access Manager for Microsoft SharePoint utility will do this for you automatically, or you can add the claim type mappings manually using the `New-SPClaimTypeMapping` command. For further details, please refer to [Manual configuration of a SharePoint 2013 Server WS-Federation Trust](#).

6. When complete, click **Next**.



7. You will now see the **Permissions** page. This enables you to control which users can access the application. By default, all Cloud Access Manager users have access to the application. You can restrict access to the application to users who belong to a specific role, but for this example click **Next** to allow all users to access the application.
8. Enter an Application Name, for example SharePoint 2013, then click **Next**.
9. To configure how the application is displayed on the Cloud Access Manager Portal, enter the **Title** and **Description** you want to display on the Cloud Access Manager Portal.
10. Enter the URL that you want your users to be initially redirected to.
11. Click **Get Application Icon** to locate and display the icon of the application or upload an icon of your choice.
12. Click **Finish** to complete the configuration of the application.
13. Cloud Access Manager will now generate a certificate that you must download and add to the SharePoint server.

Configuring a SharePoint 2010 or 2013 WS-Federation Trust using the Cloud Access Manager for Microsoft SharePoint utility

This section describes how to install the Cloud Access Manager for SharePoint utility and how to use it to establish a trust between Cloud Access Manager and SharePoint Server 2010 or 2013.

Installing Cloud Access Manager for SharePoint

To install Cloud Access Manager for SharePoint

1. Copy the appropriate version of the Cloud Access Manager for SharePoint installer (2010 or 2013) to a server in your Microsoft SharePoint farm.
2. Run the installer, which will install the software in its default location and add a link to your Windows Start menu.

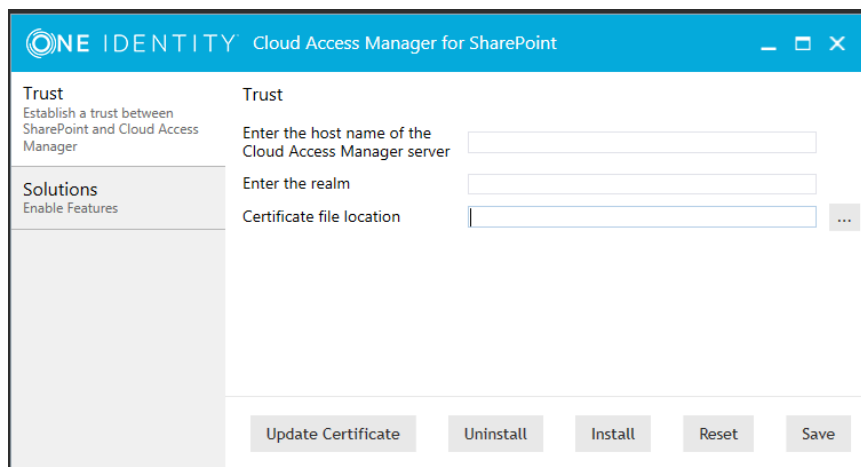
NOTE: Cloud Access Manager for SharePoint requires Microsoft .NET framework version 4.5 installed on your host.

3. Click the link on the Start menu to open the application.

Establishing a trust between Cloud Access Manager and SharePoint

To establish a trust between Cloud Access Manager and SharePoint

1. Download the certificate from your SharePoint application in Cloud Access Manager, then copy it to the SharePoint server where Cloud Access Manager for SharePoint is running.
2. Complete the fields on the **Trust** tab. You can obtain the realm value from the Cloud Access Manager SharePoint application configuration, **Federation Settings | Relying Party Realm / Identity**.
3. Browse to the location of the Cloud Access Manager trust certificate file, and click **Install**.



The trust has now been established between Cloud Access Manager and SharePoint Server 2013. Next you will need to enable it to protect your sites.

Manual configuration of a SharePoint 2013 Server WS-Federation Trust

This section guides you through the steps required to manually configure your SharePoint 2013 server for claims-based authentication using WS-Federation.

NOTE: These steps are an alternative method to using the Cloud Access Manager for Microsoft SharePoint utility described in [Configuring a SharePoint 2010 or 2013 WS-Federation Trust using the Cloud Access Manager for Microsoft SharePoint utility](#).

For instructions on how to configure SharePoint 2010, please refer to [Manual configuration of a SharePoint 2010 Server WS-Federation Trust](#).

To configure your SharePoint 2013 Server for claims-based authentication

1. On the SharePoint server, open the SharePoint 2013 Management Shell and enter the following commands to set up a new claims-based WS-Federated authenticator:

```
$cert=New-Object System.Security.Cryptography.X509Certificates.X509Certificate2  
("<location of certificate>")
```

```
New-SPTrustedRootAuthority -Name "<Name of Certificate>" -Certificate $cert
```

```
$email=New-SPClaimTypeMapping -IncomingClaimType  
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" -Incoming  
ClaimTypeDisplayName "EmailAddress" -SameAsIncoming
```

```
$realm = "<realm as defined in Cloud Access Manager template>"
```

```
$x=New-SPTrustedIdentityTokenIssuer -Name "<Name for authenticator>" -  
Description "Cloud Access Manager" -realm $realm -ImportTrustCertificate $cert -  
ClaimsMappings $email -SignInUrl "<Endpoint URL>" -IdentifierClaim  
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
```

NOTE: If you have added extra claims to the Claim Mapping page in the Cloud Access Manager SharePoint template, then you will need to add mappings for each extra claim here.

To do this:

- use extra `New-SPClaimTypeMapping` commands, as for the `EmailAddress` default shown above.
- then use the `-ClaimsMappings` parameter in the `New-SPTrustedIdentityTokenIssuer` command to create them in the Trust.

The trust has been established between Cloud Access Manager and SharePoint Server 2013. Next you need to enable it to protect your sites.

Manual configuration of a SharePoint 2010 Server WS-Federation Trust

This section guides you through the steps required to manually configure your SharePoint 2010 server for claims-based authentication. Configuring SharePoint 2010 is similar to configuring SharePoint 2013, with additional steps to enable the claims-based authentication mode.

NOTE: These steps are an alternative method to using the Cloud Access Manager for Microsoft SharePoint utility described in [Configuring a SharePoint 2010 or 2013 WS-Federation Trust using the Cloud Access Manager for Microsoft SharePoint utility](#).

To configure your SharePoint 2010 Server for claims-based authentication

1. On the SharePoint server, open the SharePoint 2010 Management Shell, and enter the following commands to change SharePoint 2010 from classic-mode to claims-based authentication:

```
$WebAppName = "http://SharePoint WebApp URL"  
$wa = get-SPWebApplication $WebAppName  
$wa.UseClaimsAuthentication = $true  
$wa.Update()
```

For example, the SharePoint WebApp URL would be, `http://share.point2010.local:8`

2. Configure the policy to enable the current logged on user to have Full Control, for example, the account being used to make these changes to SharePoint:

```
$account = "yourDomain\yourUser"  
$account = (New-SPClaimsPrincipal -identity $account -identitytype  
1).ToEncodedString()  
$wa = get-SPWebApplication $WebAppName  
$zp = $wa.ZonePolicies("Default")  
$p = $zp.Add($account, "PSPolicy")  
$fc=$wa.PolicyRoles.GetSpecialRole("FullControl")  
$p.PolicyRoleBindings.Add($fc)  
$wa.Update()
```

3. Perform user migration:

```
$wa.MigrateUsers($true)
```

4. Perform user provisioning:

```
$wa.ProvisionGlobally()
```

5. Set up a new claims-based WS-Federated authenticator, as for SharePoint 2013:

```
$cert=New-Object System.Security.Cryptography.X509Certificates.X509Certificate2  
("<location of certificate>")
```

```
New-SPTrustedRootAuthority -Name "<Name of Certificate>" -Certificate $cert
```

```
$email=New-SPClaimTypeMapping -IncomingClaimType  
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" -  
IncomingClaimTypeDisplayName "EmailAddress" -SameAsIncoming
```

```
$realm = "<realm as defined in Cloud Access Manager template>"
```

```
$x=New-SPTrustedIdentityTokenIssuer -Name "<Name for authenticator>" -  
Description "Cloud Access Manager" -realm $realm -ImportTrustCertificate $cert -  
ClaimsMappings $email -SignInUrl "<Endpoint URL>" -IdentifierClaim  
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
```

NOTE: If you have added extra claims to the Claim Mapping page in the Cloud Access Manager SharePoint template, then you will need to add mappings for each extra claim here.

To do this:

- use extra New-SPClaimTypeMapping commands, as for the EmailAddress default shown above.
- then use the -ClaimsMappings parameter in the New-SPTrustedIdentityTokenIssuer command to create them in the Trust.

The trust has now been established between Cloud Access Manager and SharePoint Server. Next you will need to enable it to protect your sites.

Protecting your SharePoint website with Cloud Access Manager

Now the trust has been established between Cloud Access Manager and SharePoint Server, you can protect your SharePoint website with Cloud Access Manager.

To protect your SharePoint website with Cloud Access Manager

1. Open the **SharePoint Central Administration console** and navigate to **Manage Web Applications**.
2. Select the **Application** to protect and then click **Authentication Providers**.
3. Select the required **Zone**.
4. Scroll down to the **Trusted Identity provider** section and ensure that **Trusted Identity provider** is selected.
5. Select the **Cloud Access Manager** authenticator you created previously.

NOTE: If you created the authenticator using the utility, it will be called CAM.

NOTE: Clear the **Enable Windows Authentication** check box. If more than one authenticator is specified, the user will be prompted to select which authenticator to use when SharePoint opens.

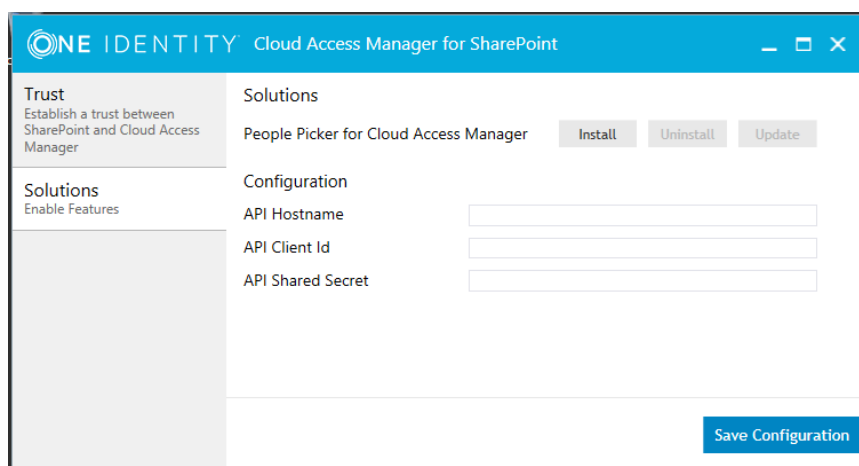
6. Click **Save** and return to Application Management.

Finally you need to set permissions for users and groups to access your SharePoint sites.

Enabling SharePoint People Picker functionality

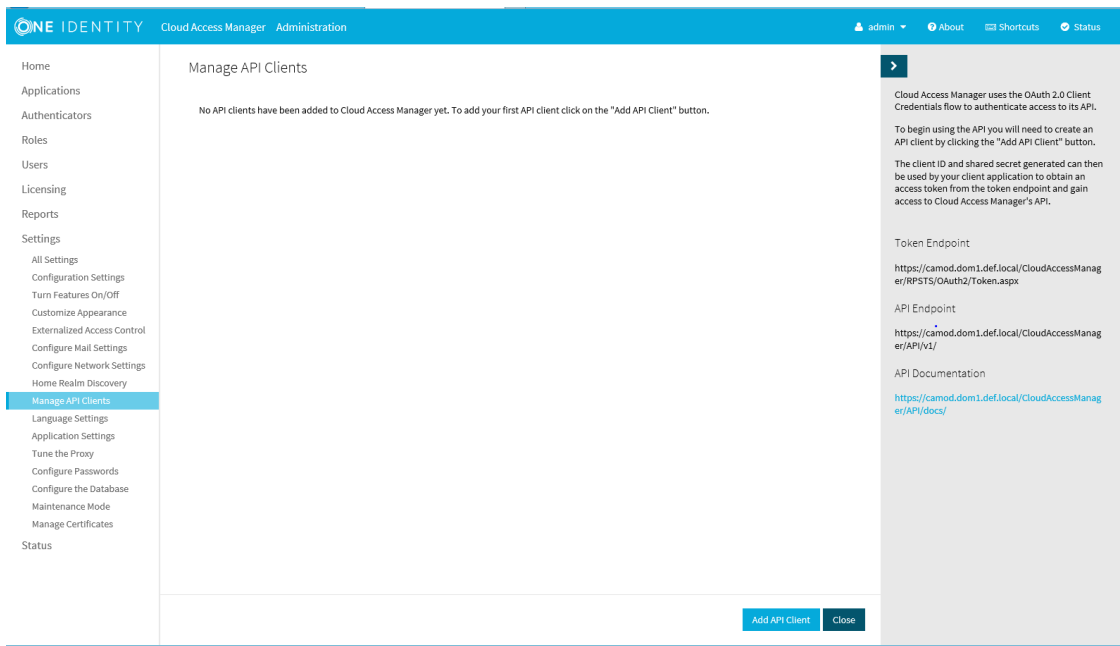
To enable SharePoint People Picker functionality with Cloud Access Manager for Microsoft SharePoint

1. In the **Cloud Access Manager for SharePoint** application, select the **Solutions** tab.



2. In the **API Hostname** field, enter the Cloud Access Manager Server hostname.
3. In the **Cloud Access Manager Application Portal**, select **Settings**, then **Manage**

API Clients.



4. Click **Add API Client**.

API Client Settings

The following values are required for Cloud Access Manager to grant access to the API for a client application.

API Client Name

Allowed Scopes

Resources	Actions
<input type="checkbox"/> apps	<input type="checkbox"/> edit
<input type="checkbox"/> authenticators	
<input type="checkbox"/> creds	
<input type="checkbox"/> roles	
<input type="checkbox"/> users	
<input type="checkbox"/> dirusers	

At least one resource scope must be selected

All prefixed with "urn:CloudAccessManager/API/Scopes/"

You may need to configure the client application with the following information.

API Endpoint

Token Endpoint

Client ID

Shared Secret

5. Enter a name for the client and select **roles** and **dirusers** in the **Allowed Scopes** section.
6. Copy and paste the **Client ID** and **Shared Secret** into the appropriate fields in the Cloud Access Manager for SharePoint application and then click **Save**.
7. In the Cloud Access Manager for SharePoint application click **Save Configuration**, and then click **Install**.

Using the SharePoint People Picker

Before you use the Cloud Access Manager SharePoint people picker solution you need to ensure that Ambiguous Name Resolution (ANR) is enabled for all Active Directory attributes that you are using to map your Cloud Access Manager users to SharePoint user accounts. By default this is the mail attribute. For details on how to configure ANR in Active Directory, please refer to Microsoft TechNet:


<http://social.technet.microsoft.com/wiki/contents/articles/22653.active-directory-ambiguous-name-resolution.aspx>

To use the SharePoint People Picker

1. To allow user access through your authenticator use the **User Policy** editor in the SharePoint application ribbon for your SharePoint web application.
2. Select **All Zones**, then click **Next**.
3. Select **Add Users**.
4. To open the **SharePoint People Picker**, select the address book icon below the **Users** field. If you have installed the **Cloud Access Manager for People Picker**, you will see Cloud Access Manager in the tree with two sub-categories of **Users** and **Roles**.

Select People and Groups



Find  List View

Display Name	E-mail Address	Title	Department
Type into the search box above then press "Enter" to search			

Organizations
Active Directory
All Users
Cloud Access Manager
 Users
 Roles

Add ->

OK Cancel

5. If you do not enter any search criteria in the **Find** field to search the Cloud Access Manager address book, all available Cloud Access Manager roles will be found.
6. If you enter search criteria in the **Find** field to search the Cloud Access Manager address book, any users or roles that match the criteria you specified will be found.
7. Select the users or roles you want to allow access to your SharePoint sites.

Policy for Web Application



OK

Adding or updating Web application policy with new users or groups will trigger a SharePoint Search crawl over all content covered by that policy. This can reduce search crawl freshness and increase crawl load. Consider using security groups at the policy level and add/remove users from security groups to avoid this.

Add Users | Delete Selected Users | Edit Permissions of Selected Users

<input type="checkbox"/>	Zone	Display Name	User Name	Permissions
<input type="checkbox"/>	(All zones)	NT AUTHORITY\LOCAL SERVICE	NT AUTHORITY\LOCAL SERVICE	Full Read
<input type="checkbox"/>	(All zones)	Search Crawling Account	i:0#.w sharepoint2013\administrator	Full Read, Full Control
<input type="checkbox"/>	(All zones)	SHAREPOINT2013 \Administrator	SHAREPOINT2013\Administrator	Full Control
<input type="checkbox"/>	(All zones)	administrator	i:05.t camclaimsauth administrator	Full Control

NOTE: If you add users manually from the Active Directory address book, they must be added by their email address to the new authentication provider — not by their sAMAccountName or other identifier. Remember to check that test users have the **mail** attribute populated in Active Directory as it is not populated by default.

You can now Single Sign-On (SSO) to the SharePoint application from a Cloud Access Manager user log in.

Adding Microsoft SharePoint to Cloud Access Manager using the reverse proxy

This section describes how to configure your SharePoint Server for authentication using the reverse proxy, including how to configure SharePoint for form-fill configuration.

In addition you need to configure SharePoint Server for forms based authentication to allow a Cloud Access Manager form-fill application to operate. For further information, please refer to Microsoft TechNet for [SharePoint Server 2010](#) and [SharePoint Server 2013](#) configuration steps.

- 1 **NOTE:** Integrated Windows Authentication (IWA) and HTTP basic authentication are also valid authentication configuration options when using the reverse proxy. For further information, please refer to the *One Identity Cloud Access Manager Configuration Guide*.
- 1 **NOTE:** Microsoft Office rich client applications, for example desktop Microsoft Office 2007 and Microsoft Office 2013, are not supported when Cloud Access Manager is used to proxy SharePoint 2013; you should use WS-Federation if rich client support is required.

To enable Cloud Access Manager to use the reverse proxy with SharePoint Server

1. Manually configure a SharePoint application using the form-fill authentication method as described in the *One Identity Cloud Access Manager Configuration Guide*.

- 1 **NOTE:** For SharePoint Server 2013, configure the **Application URLs** to use two proxy aliases for the root-to-root mapping of your SharePoint Server and Office Web Apps Server.

The application URLs you add for the Office Web Apps farm may differ in format depending on the authentication type used. For example, you may need to add the simple server name for the Office Web Apps farm as an alias for proxying SharePoint 2013. This is due to the way SharePoint constructs its URLs.

Application URLs

Cloud Access Manager needs to know the URL of the application in order to proxy it.

Application URL(s) (Omit the path component. You will enter paths on the next page.)

Add URL

- 1 **NOTE:** The SharePoint Office Web Apps server farm cannot be accessed using the proxy server until a valid Secure Sockets Layer (SSL) certificate is in place on the Cloud Access Manager Proxy.

A signed wildcard SSL certificate is required to cover the proxy server and the two previously created aliases. However, you do not need to create a new Secure Sockets Layer (SSL) certificate specific to the SharePoint configuration. For further details, please refer to Managing your SSL certificate in the *One Identity Cloud Access Manager Configuration Guide*.

2. Next, log in to the Administration Console, and navigate to the **Settings** page.
3. Click **Show Advanced Settings**.
4. Click **Tune the Cloud Access Manager Proxy**.
5. In the **Proxy Filters**, edit the Class listed as **RewriteHTMLFilter**, appending the

Mime Type with text/plain* as the value.

Edit Proxy Filter

Filter Name
html

Class
RewriteHTMLFilter

Mime Type
text/html* text/plain*

Enabled

Debug Level
0

Include

Exclude
ns=PendingRequest&ev=PendingNotificationRequest

Force Include

Application
All Applications

Save

6. Click **Save**.
7. On the **Add Proxy Property** page add a new property. In the **Property** field, enter the string `cam.disableAddingXFrameOptionsHeader`.
8. In the **Value** field, enter **true**. Ensure the **Enabled** check box is selected, this will allow Office Web Apps to load in an iFrame embedded in the SharePoint page.

x

Add Proxy Property

Property
cam.disableAddingXFrameOptionsHeader

Value
true

Description

Enabled

Application
All Applications

Save

Cancel

9. Click **Save** to save your settings. When you have completed these steps all links using Office Web Apps will function as expected, this includes opening and editing documents.

The application configuration is now complete.

Troubleshooting

Persistent cookies in Microsoft SharePoint

By default, SharePoint uses persistent cookies which enable a user to shut down an internet browser, and then re-open it while maintaining their original session. However, if a user does not fully log out of SharePoint, the situation can arise where a different user can access the original account using the same internet browser.

Debugging claims provider trust issues in Microsoft SharePoint 2013

If you encounter access or permissions issues when you try to log into SharePoint using Cloud Access Manager, tracing the root of the issue can be difficult. ULS Viewer is a helpful free utility that shows the SharePoint logs in real time as you perform tasks in SharePoint and will clearly report errors such as problems with the trust certificate chain. You can download it from:

<https://www.microsoft.com/en-gb/download/details.aspx?id=44020>

Using an internal certificate authority

If you are deploying Cloud Access Manager and SharePoint internally and you choose to use your own certificate authority (CA), you will need to configure a trust for this CA in SharePoint. This may also be necessary if you use any external certificate authority not on the published list of Trusted Certificate Authorities.

To configure a trust for your internal certificate authority

1. On your SharePoint server navigate to **Central Administration console | Security | General Security | Manage Trust**.
2. Add a new trust.
3. Upload your CA's root signing certificate.

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
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product