



Cloud Access Manager 8.1.4

How to Configure vWorkspace Integration

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
Deployment	4
Enabling vWorkspace integration	5
Troubleshooting	5
About us	7
Contacting us	7
Technical support resources	7

Introduction

This guide describes how to configure Cloud Access Manager to communicate with a vWorkspace server to display vWorkspace resources on the Cloud Access Manager Application Portal. In this way vWorkspace integration seamlessly brings application virtualization to Cloud Access Manager.

NOTE: vWorkspace integration requires vWorkspace 8.0 MR1 Hotfix 362760.

For information on configuring Cloud Access Manager, please refer to the *One Identity Cloud Access Manager Configuration Guide*.

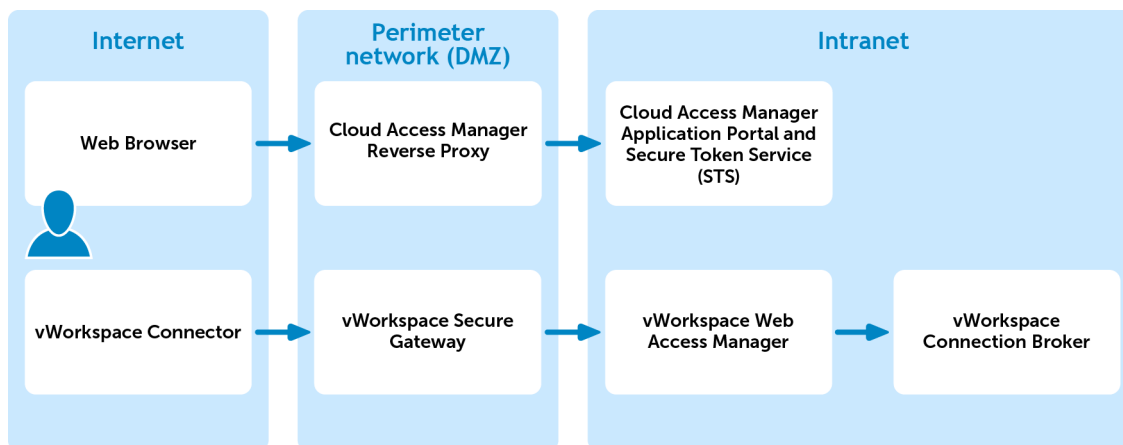
Prerequisites

Cloud Access Manager requires access to the vWorkspace Web Access service. To provide access to vWorkspace applications for external users, you must install the vWorkspace Secure Gateway in your perimeter network (DMZ). Please refer to the vWorkspace documentation for installing the Web Access service and Secure Gateway.

Before users can access vWorkspace applications using the Cloud Access Manager Application Portal, the vWorkspace client application must be installed on their client computers. Please refer to the *vWorkspace Administration Guide* for details on how to deploy vWorkspace connectors to client devices.

Deployment

The following diagram shows a recommended deployment architecture in which a Cloud Access Manager host links to vWorkspace apps for internal and external users.



Enabling vWorkspace integration

By default, vWorkspace integration is not enabled in Cloud Access Manager.

To enable vWorkspace integration

1. Log in to the Administration Console, navigate to the **Settings** page and click **Turn Features On/Off**.
2. Select the **Enable vWorkspace integration** check box.
3. Complete the **vWorkspace Web Access URL** field.

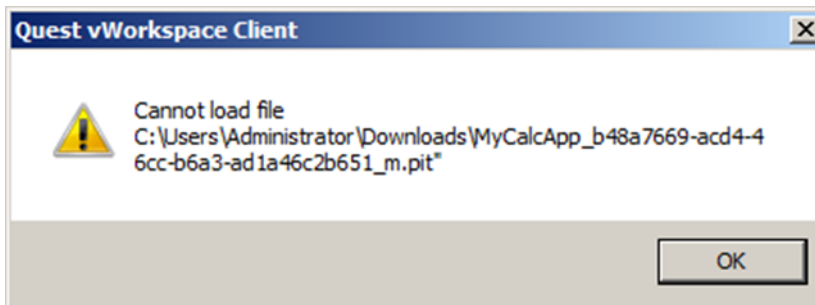
Optionally, select the roles that are allowed to access vWorkspace applications. By default, all Cloud Access Manager users will have access. However, you can restrict access to users who belong to a specific role.

NOTE: The vWorkspace Web Access URL must start with Secure HTTP (https).

Troubleshooting

vWorkspace connector and SSL

An error, with a similar message to the one shown below, is generated by the vWorkspace Connector when it does not trust the Secure Sockets Layer (SSL) connection.



There are two solutions to this condition:

- The SSL certificate of the vWorkspace server must be signed by a recognized Certification Authority
- Install the certificate of the vWorkspace server with the Trusted Root Certification Authorities on the client computer.

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