



Cloud Access Manager 8.1.3

How to Configure User Mapping

Copyright 2017 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
Mapping users when you configure the application	4
Mapping users after the application has been configured	6
Un-mapping users	6
About us	7
Contacting us	7
Technical support resources	7

Introduction

This guide describes how to configure Cloud Access Manager with the user mapping tool. The user mapping tool enables you to map user applications to their user account in Active Directory where the username is not derived from subject mapping.

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

Mapping users when you configure the application

When an application account is provisioned in Cloud Access Manager, the attribute specified in the **Take the username from the following attribute** field on the **Subject Mapping** page determines how the usernames associated with the application are derived, for example sAMaccountname or mail. For further information, please refer to the *One Identity Cloud Access Manager Configuration Guide*.

If the user has an existing account for an application that has provisioning enabled in Cloud Access Manager, but the user's existing username for the application does not comply with the attribute specified on the **Subject Mapping** page, you can apply the user mapping tool to map their existing application username to their user account in Active Directory.

To map users

1. When you have completed the application configuration wizard, click Go to **User Mapping** on the **Federation Settings** page.

User Mapping

If you already have existing users within your application then Cloud Access Manager can map these users to your local front-end authentication method users. If you would like to do this then click the "Go to User Mapping" button.

Federation Settings

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

IDP Login URL

<https://camod.dom1.def.local/CloudAccessManager/RPSTS/Saml2/Default.aspx>

Issuer (Entity ID for IDP)

<urn:camod.dom1.def.local/CloudAccessManager/RPSTS>

Federation metadata URL ([Download Metadata](#))

<https://camod.dom1.def.local/CloudAccessManager/RPSTS/Saml2/Metadata.ashx?AppId=11>

Certificate ([Download](#) | [View Details](#))

```
-----BEGIN CERTIFICATE-----
MIIDBjCCAggqAwIBAgIQAVz0vD1aLVa5UebFczBj4TANBgkqhkiG9w0BAQsFAAD8
NTowOAYDVQQDDDFPbmUgSWR1bnRpdHkgQ2xvdmV0eW9uZjZKNzE1hbnRnZXIqQXBw
IEVyb2dsZSBBCzBzMCMDTE3MTAkdHJlbnRpdHkgQ2xvdmV0eW9uZjZKNzE1hbnRn
MTowOAYDVQQDDDFPbmUgSWR1bnRpdHkgQ2xvdmV0eW9uZjZKNzE1hbnRnZXIqQXBw
IEVyb2dsZSBBCzBzMCMDTE3MTAkdHJlbnRpdHkgQ2xvdmV0eW9uZjZKNzE1hbnRn
PjE4bW9uZjZKNzE1hbnRnZXIqQXBwIEVyb2dsZSBBCzBzMCMDTE3MTAkdHJlbnRpdHkg
L01uZG90eW9uZjZKNzE1hbnRnZXIqQXBwIEVyb2dsZSBBCzBzMCMDTE3MTAkdHJlbnRpdHkg
XPMCLaM/6k3dR92FIpHdUdTjpPL7WnquF9X+90dCMeyngRT+vk73qel2a7SNTzGH
T7R57PH/2r2jH3p3yxnZWoynsveFMLyGcnOvd+GEJazRDhqcEoySUMI5xow/LCZ
Li2iKR4+HpxXWqmrNbuIX5IMZjCEONrzsDgVr4jNLVISM/Svb5LEGMOSMBE4BT
HEmJyD8EByT01qE1YwIDARBAADQCSqGSIBo3DQEBCwUAA4EBAQABAgEBAQEBAQAB
HyHr4dG9jVGF6A665xN8bfqntzFZuKONIzFKXxwzCU0SeeevFL9XLLQeFqg1P
o3gH33M2vufGFSwLITQAM+q+7jFw+xxafOnaXyXIN9pm6gDEjVQbaOGvYWSz0Tu7
Hg00rVpLR5Uj7zs2bxK1CHGvDeocW244+oh2acMR2mHNDSXB2fzq0/joX7bz2Fb+
d11NoZAcVgn8EZSVV0T2d354zEYlWbEJymIn3ULE2r31uFmRPwJ6DU2270qazW
HNDSQFevV6bz1DLg5sToaM0bTLLeof8W+Sppp7S1r0CqA10Xv2Bw63NO8qg/5KZs
VL/v1pw1
-----END CERTIFICATE-----
```

NOTE: The user mapping tool lists the users in the:

- Directories that are configured in the Cloud Access Manager front-end authenticators
- Application you are configuring.

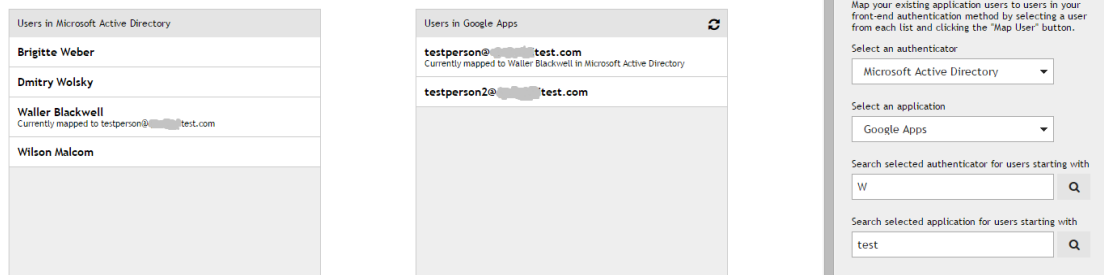
You can filter these lists to pinpoint the users that you want to map.

2. Select the users you want to map and click **Map User**.

The screenshot displays the 'User Mapping' tool interface. On the left, there are two panels: 'Users in AD' and 'Users in Google Apps'. The 'Users in AD' panel lists three users: Brigitte Weber, rwiggm, and Waller Blackwell. The 'Users in Google Apps' panel lists four users: testadmin@questapitest.com, testets@questapitest.com, testperson1@questapitest.com, and testperson2@questapitest.com. A modal dialog is open on the right, titled 'Map your existing application users to users in your front-end authentication method by selecting a user from each list and clicking the "Map User" button.' It contains dropdowns for 'Select an authenticator' (AD) and 'Select an application' (Google Apps). There are search boxes for 'Search selected authenticator for users starting with' (w) and 'Search selected application for users starting with' (tes). At the bottom of the modal are buttons for 'Map User', 'Un-Map User', 'Close', and 'Get Users'.

3. The current mapping for the username is shown in the Active Directory list and in the application list.

User Mapping



4. The application will appear in the user's application catalog. When the user clicks the application to add it to the application portal, Cloud Access Manager will detect that the user already has an account and will not provision a new account for that user.

Mapping users after the application has been configured

As the administrator, you can map users when you configure the application in Cloud Access Manager, or you can map users after the application has been configured.

You can map users after the application has been configured, either:

- From the **Provisioning** page of the application editor:
- Or by selecting **User Mapping** from the Users section on the Cloud Access Manager landing page:
 1. Click **Manage Users | User Mapping**.
 2. Select an application from the list in the user mapping pane and map the users.

Un-mapping users

To un-map a user

1. Navigate to the **User Mapping** page.
2. From the front-end authenticator **Users** list, select the required mapped user.
3. Select the corresponding mapped user from the application **Users** list.
4. Click **Un-Map User**.

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