



Cloud Access Manager 8.1.3

How to Configure for SSO to SAP  
NetWeaver using SAML 2.0

## 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](http://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

<b>Introduction</b> .....	<b>4</b>
Prerequisites and requirements .....	4
Supported versions .....	4
DNS settings .....	4
User mappings .....	5
NetWeaver configuration (Service Provider Role) .....	5
Cloud Access Manager configuration - (Identity Provider Role) .....	6
NetWeaver configuration .....	8
Cloud Access Manager as an Identity Provider (IDP) .....	8
Enabling SSO to SAP NetWeaver applications .....	9
<b>About us</b> .....	<b>10</b>
Contacting us .....	10
Technical support resources .....	10

# Introduction

This guide provides step-by-step configuration instructions for Single Sign-On (SSO) access to SAP NetWeaver using Cloud Access Manager using the SAML 2.0 protocol.

## Prerequisites and requirements

Ensure that the following prerequisites and requirements are met before you configure SSO to SAP Netweaver using SAML 2.0.

- [Supported versions](#)
- [DNS settings](#)

## Supported versions

The SAML 2.0 protocol is supported on the following SAP NetWeaver versions:

- Java 7.2x, 7.3x, 7.4x
- ABAP 7.02, 7.3x, 7.4x

## DNS settings

If internal NetWeaver applications will be accessed by users on the Internet using the Cloud Access Manager proxy, the DNS settings should be as follows:

- End-user computers must be able to resolve the public Cloud Access Manager proxy FQDN
- The Cloud Access Manager proxy computer must be able to resolve the FQDN of the NetWeaver server on the internal network.

If users will access NetWeaver applications directly from their internal network, end-user computers must be able to resolve both the Cloud Access Manager proxy machine FQDN and the NetWeaver server FQDN.

# User mappings

In the following example Cloud Access Manager is deployed using Active Directory as the user store, and the logon ID of NetWeaver internal users matches the sAMAccountName of Cloud Access Manager users.

- [NetWeaver configuration \(Service Provider Role\)](#)
- [Cloud Access Manager configuration - \(Identity Provider Role\)](#)

## NetWeaver configuration (Service Provider Role)

### To configure NetWeaver (Service Provider Role)

1. In the SAP NetWeaver admin interface, navigate to **Configuration | Security | Authentication and Single Sign-On**. Select the **SAML 2.0** tab.

2. Click **Enable** SAML 2.0 support.
3. In the **Provider Name** field, type NetWeaver and click **Next**.
4. Click **Browse**, located next to the **Signing Key Pair** field. In the **Select Keystore Entry** box, click **Create**. In the **Entry Settings** window under **Entry Name**, type **test** and click **Next**.
5. In the **Subject Properties** window, in the **Common Name** field type **test**. Click **Finish**, and then click **OK**.
6. Click **Next** to advance to **Service Provider Settings**.
7. Under **Identity Provider Discovery**, switch **Selection Mode** to **Automatic**.

**NOTE:** This hides the NetWeaver home realm discovery interface. It is not needed here since Cloud Access Manager is the only configured identity provider.

8. Click **Finish**.
9. Click **Edit** then click the **Service Provider Settings** tab.
10. Click **Add** in the **Relay State Mappings** section and insert the following entry to facilitate IDP-initiated SSO later:  
RelayState = portal  
Path = /irj/portal
11. Click **OK** and then **Save**.

## Cloud Access Manager configuration - (Identity Provider Role)

### *To configure Cloud Access Manager (Identity Provider Role (IDP))*

1. Log in to the Administration Console using the desktop shortcut **Cloud Access Manager Application Portal** and select **Add New from the Applications** section on the home page.
2. Click **Configure Manually**. Select **Using SAML**, and then click **Next**.
3. Under **Federation Settings**, set **Recipient** value to:  
`https://<NetWeaver_server_fqdn>:<port>/saml2/sp/acs`  
Where **<NetWeaver\_server\_fqdn>** is the fully-qualified domain name of your SAP NetWeaver server, and **<port>** is the port number used by the NetWeaver server to listen on, for example <https://srvnwce73.demo.sap.corp:50001/>.
4. Set **Audience / SP Identity** to NetWeaver and click **Next**.

## Federation Settings

If your service provider provides a federation metadata URL enter it below or if they provide a file containing federation metadata you can select it below. Otherwise consult the documentation or administrative interface for the application for the values you should enter here.

Federation metadata URL

Upload federation metadata file

The following values are required for Cloud Access Manager to sign the user in to the application.

Assertion Consumer Service URLs		
Index	Recipient	Default
0	https://srnwce73.demo.sap.corp:50001/saml2/sp/acs	<input checked="" type="checkbox"/>
<input type="button" value="+ Add ACS Entry"/>		

Audience / SP Identity

Application Logout URL

If your service provider signs their authentication requests then you may upload their signing certificate to verify that the requests come from a trusted source.

Upload signing certificate

If your service provider requires authentication responses to be encrypted then you may upload their encryption certificate.

Upload encryption certificate

5. On the **Subject Mapping** page, select **Derive the username from an attribute**, and enter **sAMAccountName** in the attribute name. Do not add extra claim mappings. Click **Next**.
6. Choose whether to proxy the application. Select **Proxy this application** if you want to expose your NetWeaver application to users on the Internet. If you choose this option, then you must:
  - a. Set the value of the application URL to **https://<NetWeaver\_server\_fqdn>:<port>** for example **https://srnwce73.demo.sap.corp:50001**. Click **Next**.
  - b. Set the proxy URL to the publicly-accessible proxy URL for the application. Click **Next**.
7. Allow a role which includes your sample user to access the application. Click **Next**.
8. Name the application **SAP NetWeaver**. Click **Next**.
9. In the **Application Portal** section, change the title of the first entry to **SAP NetWeaver Portal**.

10. Switch the **SSO Mode** to **IDP initiated**. In the **Relay State (optional)** field type **portal**.
11. Click **Finish**. On the **Application Created** page, click **Download Metadata** and then **Download Certificate**. Save both files to a location that can be accessed by the NetWeaver admin browser. Click **Close**.

## NetWeaver configuration

The following sections explain how to configure NetWeaver:

- [Cloud Access Manager as an Identity Provider \(IDP\)](#)
- [Enabling SSO to SAP NetWeaver applications](#)

## Cloud Access Manager as an Identity Provider (IDP)

### *To configure Cloud Access Manager as an identity Provider*

1. In NetWeaver administration on the **Configuration | Security | Authentication and Single Sign-On | SAML 2.0** page, click the **Trusted Providers** link. Click **Add**, and choose **by uploading metadata file**.
2. In the **Select Metadata** step, choose the `CloudAccessManagerMetadata.xml` document downloaded in step 11 of [Cloud Access Manager configuration - \(Identity Provider Role\)](#) and click **Next**.
3. In the **Metadata Verification** step, choose the certificate (PEM file) downloaded in step 11 of [Cloud Access Manager configuration - \(Identity Provider Role\)](#) and click **Next**.
4. In the **Provider Name** step, type the alias name **Cloud Access Manager** and click **Next**.
5. In the **Signature and Encryption** step, change the **Single Sign-On Authorization Request Sign** parameter to **Never** and click **Next**.
6. Click **Next** through to the end, then click **Finish**.
7. Click **Edit**, then under the **Identity Federation** tab, click **Add** to add a Name ID format.
8. Under **Format Name**, choose **Unspecified**. Under **Source Name**, choose **Logon ID**.
9. Click **OK** and then **Save**.
10. Click **Enable**.



# Enabling SSO to SAP NetWeaver applications

## To allow single sign-on (SSO) to your NetWeaver applications

1. In **NetWeaver Admin**, select **Configuration | Security | Authentication and Single Sign-On**.
2. On the **Authentication** tab, highlight the **ticket** policy configuration. On the **Authentication Stack** tab, click **Edit**.
3. Under **Login Modules**, click **Add**. Choose **SAML2LoginModule** from the dropdown list. Click **Add** again, and choose **CreateTicketLoginModule** from the list.
4. Change the order and the flag status of the five login modules to match the following, then click **Save**. This will use federation, and fall back to forms if federation fails.

EvaluateTicketLoginModule	SUFFICIENT
<b>SAML2LoginModule</b>	<b>OPTIONAL</b>
<b>CreateTicketLoginModule</b>	<b>SUFFICIENT</b>
BasicPasswordLoginModule	REQUISITE
CreateTicketLoginModule	OPTIONAL

**Details of policy configuration "ticket"**

Authentication Stack | Properties

Edit Save Cancel

Used Template:

Session Fixation Protection: Strict

**Login Modules**

Add Remove Move Up Move Down

Login Module Name	Flag
Evaluate TicketLoginModule	SUFFICIENT
<b>SAML2LoginModule</b>	<b>OPTIONAL</b>
Create TicketLoginModule	SUFFICIENT
BasicPasswordLoginModule	REQUISITE
Create TicketLoginModule	OPTIONAL

**Options of login module "SAML2LoginModule"**

Add Remove

Name	Value

## 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