ONE IDENTITY™

Cloud Access Manager 8.1.4

How to Configure ServiceNow

Cloud Access Manager How to Configure ServiceNow
Updated - November 2018
Version - 8.1.4

Contents

Introduction

This guide describes how to configure ServiceNow for use with Cloud Access Manager provisioning.

Cloud Access Manager supports Just-In-Time provisioning for ServiceNow.

Prerequisites

Ensure that the following prerequisites are met before configuring ServiceNow provisioning in Cloud Access Manager.

You will need:

a. A ServiceNow administration account

b. A production deployment of Cloud Access Manager with a signed SSL certificate

Configuring ServiceNow

The ServiceNow QuickConnect connector requires configuration to work with Cloud Access Manager's method of user account provisioning.

To configure ServiceNow for user account provisioning

1. Open the web site of your ServiceNow instance as an Administrator.

2. In the left-hand pane of the ServiceNow Web site, under **System Properties**, click **Web Services**.

3. In the right-hand pane, clear the following check box:

    This property sets the elementFormDefault attribute of the embedded XML schema to the value of unqualified, if set to true. This attribute indicates whether or not locally declared elements must be qualified by the target namespace in an instance document. If the value of this attribute is 'unqualified', then locally declared elements should not be qualified by the target namespace. If the value of this attribute is 'qualified', then locally declared elements must be qualified by the target namespace. For compatibility with Clients generated from WSDL (.NET Web Reference, Axis2 stub, webMethods, etc.), set this value to false. This value defaults to true.

    For further information and documentation, please go to http://wiki.service-now.com/index.php?title=Web_Services

4. Click **Save**.

Configuring ServiceNow using the built-in SAML federation template

Cloud Access Manager provides a pre-configured template to allow easy deployment of federated SSO and Just-In-Time Provisioning to ServiceNow. Follow the instructions in the template wizard.

Please refer to *SAML federation* in the *One Identity Cloud Access Manager Configuration Guide* for an example of how to configure single sign-on for a SAML federated application.

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