Cloud Access Manager 8.1.4

Quick Start Guide

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.

Cloud Access Manager Quick Start Guide
Updated - November 2018
Version - 8.1.4

Contents

1

Overview

For medium and large organizations, the proliferation of user accounts is a huge problem. As the number of line-of-business applications increases, the number of usernames and passwords that your staff are compelled to remember escalates to unmanageable levels. Over recent years the adoption of multi-tenant Software-as-a-Service (SaaS) has made the problem worse not better with each cloud application effectively managing its own independent user identity silo. The problem does not stop there, for every new user granted access to required resources a whole host of user accounts must be set up, one for each application. The cost of creating and managing these application accounts and the risk of authorization creep is significant. As the administrative processes required to manage application accounts for each individual become more time-consuming and complex, errors inevitably creep in and vulnerabilities to social engineering attacks and other such threats are introduced.

With Cloud Access Manager, whether your applications are hosted on your internal private network or in the cloud, your employees, partners, and customers require only a single username and password to gain secure access to their resources. In addition, if you demand stronger authentication, you can configure Cloud Access Manager to require a one-time-password (OTP). Users can access all of their applications through an easy-to-use, customizable application portal. You do not have to set up new user accounts across a range of applications every time you hire someone new, Cloud Access Manager will handle it all for you, creating user accounts as required.

The use of passwords to authenticate individuals is a trade-off between usability and security. If someone discovers a password by social engineering, network sniffing, shoulder surfing, keylogging or brute-force your business secrets and sensitive data are there for the taking. Because users only need to remember a single password there is no need for them to write their application passwords down, remember them, or even type them in. So, the vulnerability from this type of attack is greatly reduced. Because Cloud Access Manager only creates application accounts as needed with strong, hard-to-guess passwords, attackers do not have the easy option of compromising newly-created accounts with default initial passwords.

Cloud Access Manager delivers real productivity gains to your users while minimizing the effort needed to control access to your on-premise applications and cloud service accounts:

- Password wallet and identity federation functions provide your users with the convenience of Single Sign-On (SSO) to all applications, whether they run on your private network, or in the public cloud.

- Cloud Access Manager provides web access management functionality using its web proxy technology allowing you to securely expose your internal web applications to external users.
- An easy-to-use, customizable application portal provides your users with a convenient launchpad, allowing them to see, and navigate to the applications they are permitted to access.
- Identity federation with home realm discovery allows you to grant access to users in other forests within your own organization and external organizations.
- For extra security you can configure Cloud Access Manager to require a one-time passcode generated by an authentication token, or an X.509 certificate stored on a client computer or smart card.
- Just-in-time provisioning means that your users get access to the applications they need, when they need them and not before, giving you cost savings in license seats while at the same time reducing the administrative burden of application account provisioning.
- High availability deployment options provide continuity of service and scalability to millions of users.

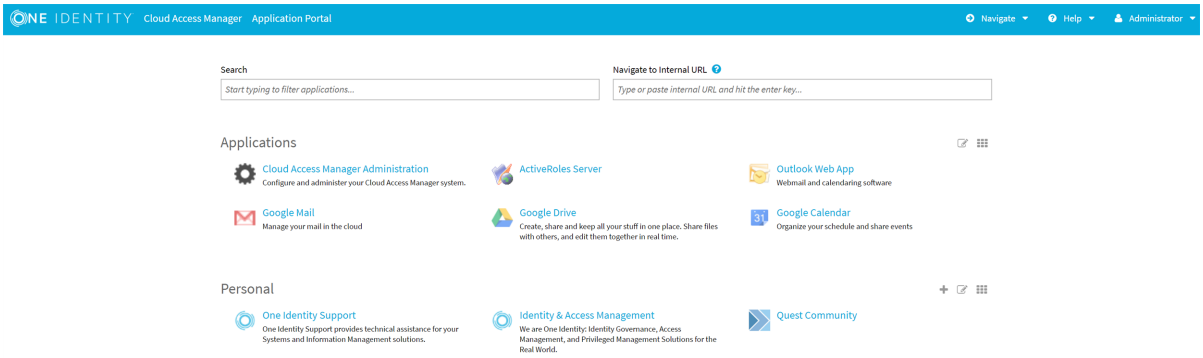
Getting started with Cloud Access Manager

This guide takes you through the steps required to deploy a demonstration Cloud Access Manager environment on a single host. When completed, we will use the environment to demonstrate the Single Sign-On (SSO) capability of Cloud Access Manager to One Identity Active Roles using Integrated Windows Authentication (IWA).

NOTE: One Identity Active Roles is a separate product, refer to https://www.oneidentity.com/products/active-roles/ for further information.

To add SSO to additional applications, for example Google Apps service using SAML Authentication, please refer to the *One Identity Cloud Access Manager Configuration Guide*. We recommend that this installation is performed within your local network on an Active Directory member server.

Figure 1: Cloud Access Manager Application Portal



Prerequisites

Make sure that the following prerequisites are met before installation, with the latest Microsoft Hotfixes applied.

- Operating system
  - Microsoft Windows Server 2008 R2
  - Microsoft Windows Server 2008 R2 Server Core
  - Microsoft Windows Server 2012
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2012 Server Core
  - Microsoft Windows Server 2012 R2 Server Core.
  - Microsoft Windows Server 2016
- Domain member server — the host should be joined to the Active Directory domain containing the users that require SSO.

  NOTE: Please be aware that Domain controllers are not valid Cloud Access Manager hosts.
- Hardware — the Cloud Access Manager host must have:
  - 2 GHz Processor
  - 2 GB Memory
  - 30 GB Hard Disk.
- Internet connection — an internet connection is required for the installation process.
- Enhanced Security Configuration (ESC) is enabled in Internet Explorer by default on Windows Server platforms. This may prevent some features of Cloud Access

Manager from functioning correctly. If you want to temporarily disable ESC, click the **Configure IE ESC** link in Windows Server Manager.

- If the browser on the Cloud Access Manager host is configured to use a proxy server, add the fully qualified domain name or IP address of the Cloud Access Manager host to the proxy's exceptions list to make sure that the Cloud Access Manager host is not proxied.
- On a Proof of Concept installation, port 10443 is used to host the user interface (UI) and Security Token Service (STS). Make sure that port 10443 is not already being used by another application, this port is only used internally on the host.

NOTE: For a full list of installation prerequisites and additional software installed automatically during the **Autorun**, please refer to the *One Identity Cloud Access Manager Installation Guide*.

Installing Cloud Access Manager

To install Cloud Access Manager

1. Start the **Autorun** and navigate to the **Install** section.

   NOTE: The **Autorun** cannot be used to install Cloud Access Manager on hosts running the Server Core installation option of Microsoft Windows Server. You must run the installer files directly from the command line.

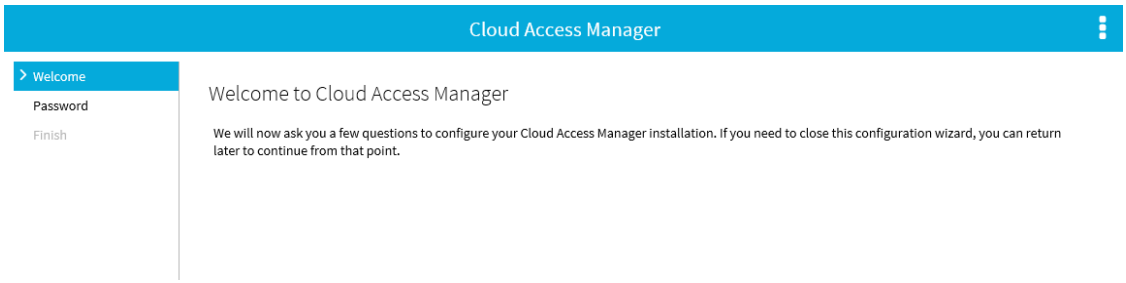
2. Click **Install** on the **Cloud Access Manager IIS Components**.
3. Accept the license agreement. Click **Next**.
4. Click **Proof of Concept Installation**.
5. Click **Install** to deploy the components required for Cloud Access Manager.

   NOTE: Cloud Access Manager requires Microsoft .NET framework version 4.5. If this is not already installed on the host, the installer will download and install .NET framework from the Internet. Alternatively, an offline .NET 4.5 installer is available from the Cloud Access Manager Autorun, which you can install before Cloud Access Manager.

6. When the installation is complete, click **Launch** to start the configuration wizard.

   NOTE: The configuration wizard may take a few moments to open when accessed for the first time; this is due to Internet Information Services (IIS) initializing and starting the web applications. Please wait until Internet Explorer opens and displays the Cloud Access Manager Welcome page.

7. When the configuration wizard has loaded, click **Next**.

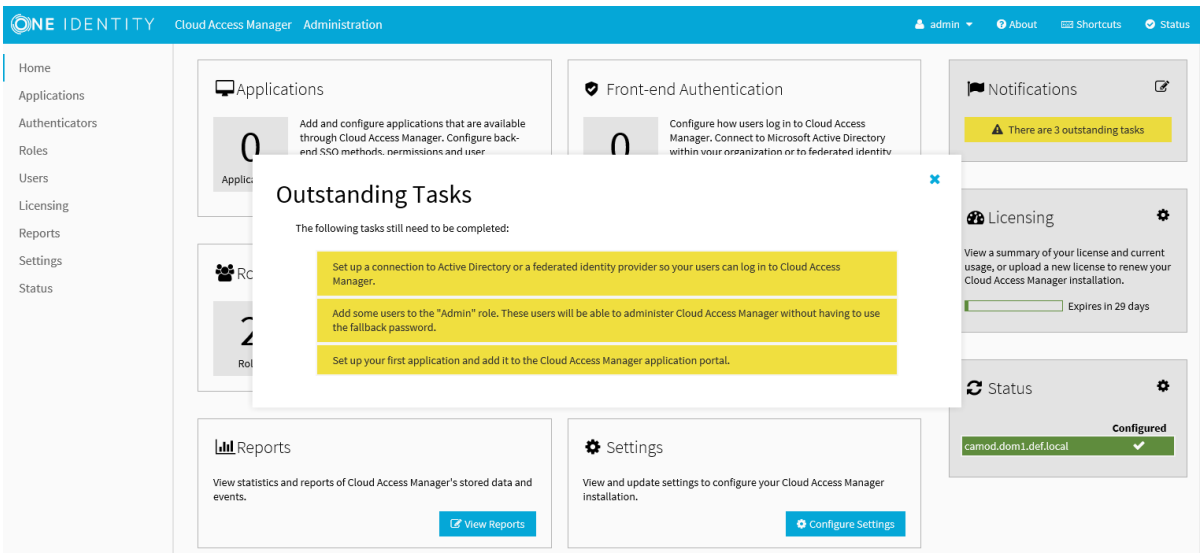


8. Enter a fallback password in the **Password** and **Confirm password** fields. You can use this password to access the Cloud Access Manager Administration interface, using the fallback link in the Start Menu, in the event that Active Directory authentication is unavailable. Click **Next**.
9. Cloud Access Manager will now configure its required components. When the configuration is complete, click **Finish**.

NOTE: For a full list of the steps required to deploy, backup, restore and upgrade a typical two host production installation of Cloud Access Manager, please refer to the *One Identity Cloud Access Manager Installation Guide*.

Configuring the front-end authentication service

When you have successfully installed the Cloud Access Manager software, the Cloud Access Manager Administration Console is displayed.

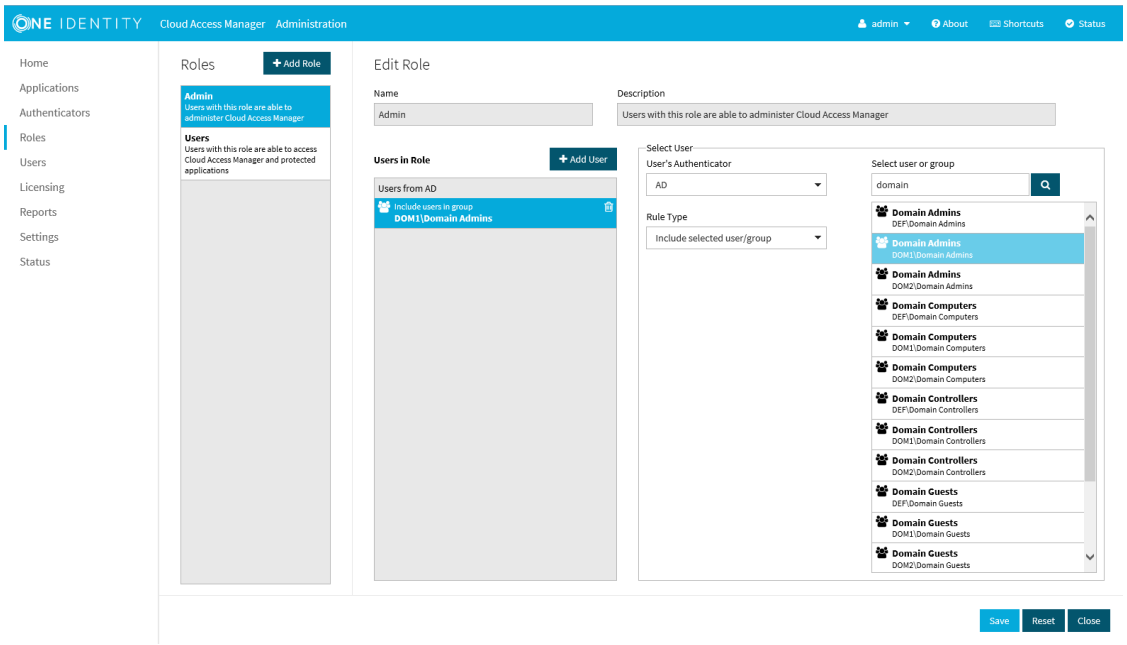


Before users and administrators can login to Cloud Access Manager, you need to configure a front-end authentication method. Typically, this would involve configuring the Microsoft Active Directory authenticator to authenticate users to your corporate domain, but equally you could configure the SAML or WS-Federated authenticator to authenticate users to a

different identity management system. This example will use the Active Directory authentication method to authenticate users and administrators accessing Cloud Access Manager.

To configure the front-end authentication service

1. Click **Add New** within the **Front-end Authentication** section on the home page.
2. Select **Microsoft Active Directory**, then click **Next**.
3. Enter the username and password of a Windows domain account, and then click **Test Connection**. This will test that Cloud Access Manager can connect to the domain which has read access to all user and group objects in the forest. Usually, a regular user account belonging to the Domain Users group is sufficient. When successful, click **Next**.
4. On the **Primary Authentication** page, do not change any check box settings. Click **Next**.
5. On the **Two Factor Authentication** page, leave the **Two factor authentication mode** selection as **Don't use two factor authentication**. Click **Next**.
6. In the **Authenticator Name** field, enter the name that will be used to identify the authenticator within Cloud Access Manager, for example enter Active Directory, then click **Finish**.
7. You have now created the front-end authentication method. Click **Edit Roles**.
8. Before Cloud Access Manager administrators and users can login to Cloud Access Manager using their Active Directory credentials, you must define how the user and administrator roles are to be derived from Active Directory group membership.



9. Click **Admin**.
10. Click **+Add User**.
11. From **Rule Type** select **Include Selected user/Group**.

12. In the **Select new user or group** text box, type **Dom**, then press **Enter** or click the magnifying glass.
13. Select the **Domain Admins** group from the list.
14. Click **Save**.
15. By default, all users are allowed access to Cloud Access Manager. If you want to restrict the set of users allowed access to Cloud Access Manager, click **Users** and follow step 15 through Step 20.
16. Click **Users**.
17. Click **+Add User**.
18. From **Rule Type** select **Include Selected user/Group**.
19. In the **Select new user or group** text box, enter the name of the user or group you want to add, then press **Enter** or click the magnifying glass.
20. Select the user or group from the list.
21. Click **Save**.
22. Click **Close** to return to the Cloud Access Manager Administration Console. The configuration is now complete. Cloud Access Manager administrators and users can now login to Cloud Access Manager using their Active Directory credentials.

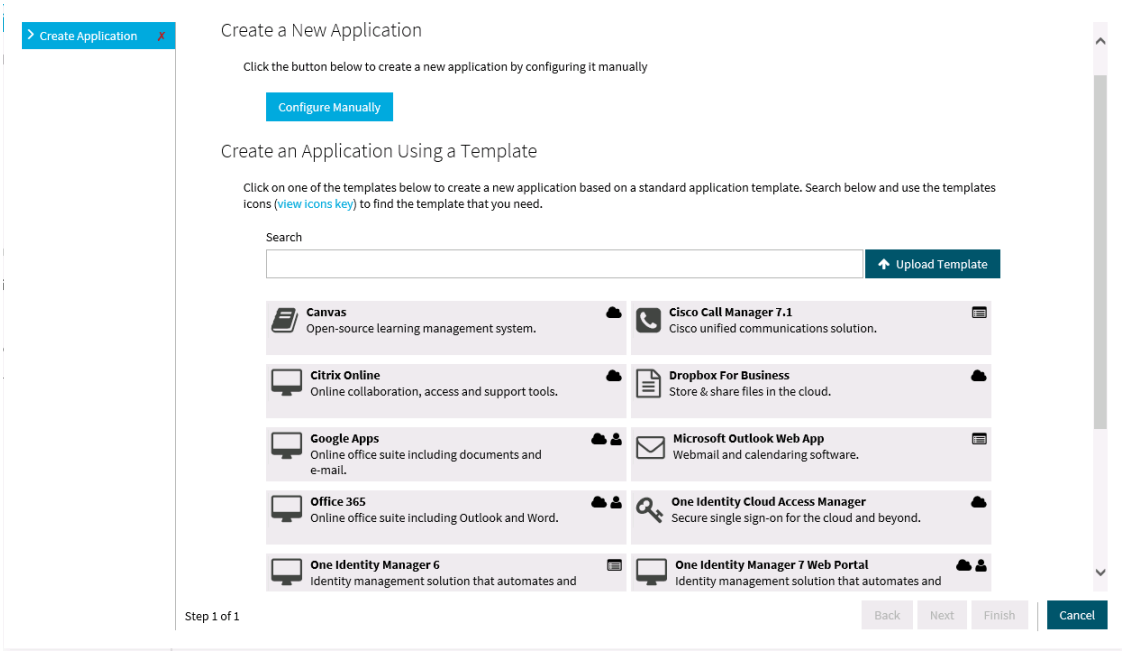
    For example, users who belong to the Active Directory Domain Admins security group can login and configure Cloud Access Manager, and Domain Users can login to the Cloud Access Manager portal using their Active Directory credentials.

Configuring an application for single sign-on

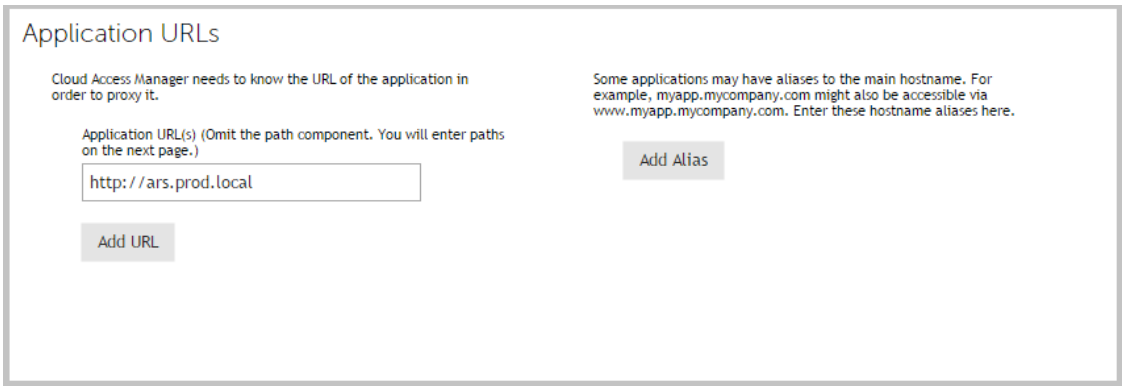
In this section we will demonstrate how to configure an Integrated Windows Authentication (IWA) application for Single Sign-On (SSO). We will use One Identity Active Roles as our example application, but the procedure is similar for any other IWA application.

To configure an IWA application for SSO

1. Click **Add New** within the **Applications** section on the home page.
2. Click **Configure Manually**.



3. Select **Using Integrated Windows Authentication**, then click **Next**.



4. Select the protocol used by the application and enter its fully-qualified domain name. Click **Next**.

> NOTE: You can obtain the protocol and fully-qualified domain name from the URL used to access the application. For example, if you normally access the application using https://ars.prod.local/ARServerAdmin, the protocol will be Secure HTTP (HTTPS) and ars.prod.local will be the fully-qualified domain name.

In order to perform SSO to a non-federated web application, Cloud Access Manager must proxy the HTTPS traffic between the browser and the application. When the application requests authentication credentials, the proxy automatically intercepts the request, retrieves the credentials from the user's Password Wallet and forwards them to the application.

To proxy the HTTPS traffic to the application, the user's browser must navigate to a proxy URL, which in turn maps to the real application URL. When the user clicks a link to the application on his application portal he is really clicking a link to the proxy service. Using the settings you provide, the proxy then relays incoming traffic to the correct application URL.

In a typical production scenario the proxy service is installed on a host in the perimeter network (DMZ). The application's public proxy URL is resolved to the IP address of the host on which the proxy service is installed.

When you install Cloud Access Manager in Proof of Concept mode the proxy component is automatically installed on the same computer as the other components. This means the application's proxy URL must resolve to the IP address of this Cloud Access Manager computer.

You can do this either by adding a canonical name (CNAME) entry to the Domain Name System (DNS) service your computer is using, or for testing on a single computer, you can add an entry to your computer's hosts file.

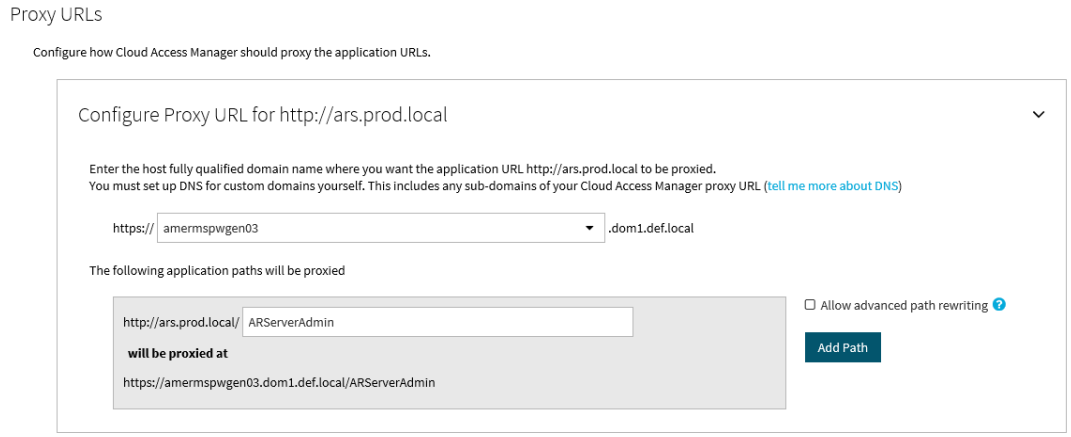
In this case, we will add an entry to our hosts file, %WINDIR%\system32/drivers/etc/hosts as follows:

xxx.xxx.xxx.xxx ars.webapps.democorp.com

Where *xxx.xxx.xxx.xxx* is the IP address of the Cloud Access Manager computer.

Now save this file.

5. Enter the application's proxy URL into the **Proxy URLs** page of the application wizard in Cloud Access Manager. Click **Next**.



NOTE: Make sure that the URL path is entered in the correct case. In the example, ARServerAdmin must be the URL path.

6. You will now see the **Permissions** page that 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 particular role, but for this example, click **Next** to allow all users to access the application.

7. Enter an **Application Name**, for example Active Roles Server. On this page you may also set whether the application uses the user's primary log in credentials. If this is set, the user will be logged into the application with the same credentials they use to log in to Cloud Access Manager. Click **Next**.
8. Configuration of the application is now complete. Click **Next**, and then click **Finish**.

To verify that the application is configured correctly

1. Close Internet Explorer to end your Cloud Access Manager session.
2. Open the Cloud Access Manager Portal using the desktop shortcut **Cloud Access Manager Application Portal**.
3. Log in to the Cloud Access Manager Portal using a test user account defined in your Active Directory forest, and click the **Active Roles Server** application.
4. The first time a user launches this application through Cloud Access Manager, they will be prompted to enter their application username and password. These credentials will be saved in the Password Wallet, to open the Password Wallet, click the username in the top right of the screen. When the application is next launched, the saved credentials are automatically submitted to the application.
5. You are now automatically signed into One Identity ActiveRoles Server.

Configuration of SSO to One Identity ActiveRoles Server is now complete. For more information on configuring SSO for applications, please refer to the *One Identity Cloud Access Manager Configuration Guide*.

About us

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