Cloud Access Manager 8.1.3

Overview

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.

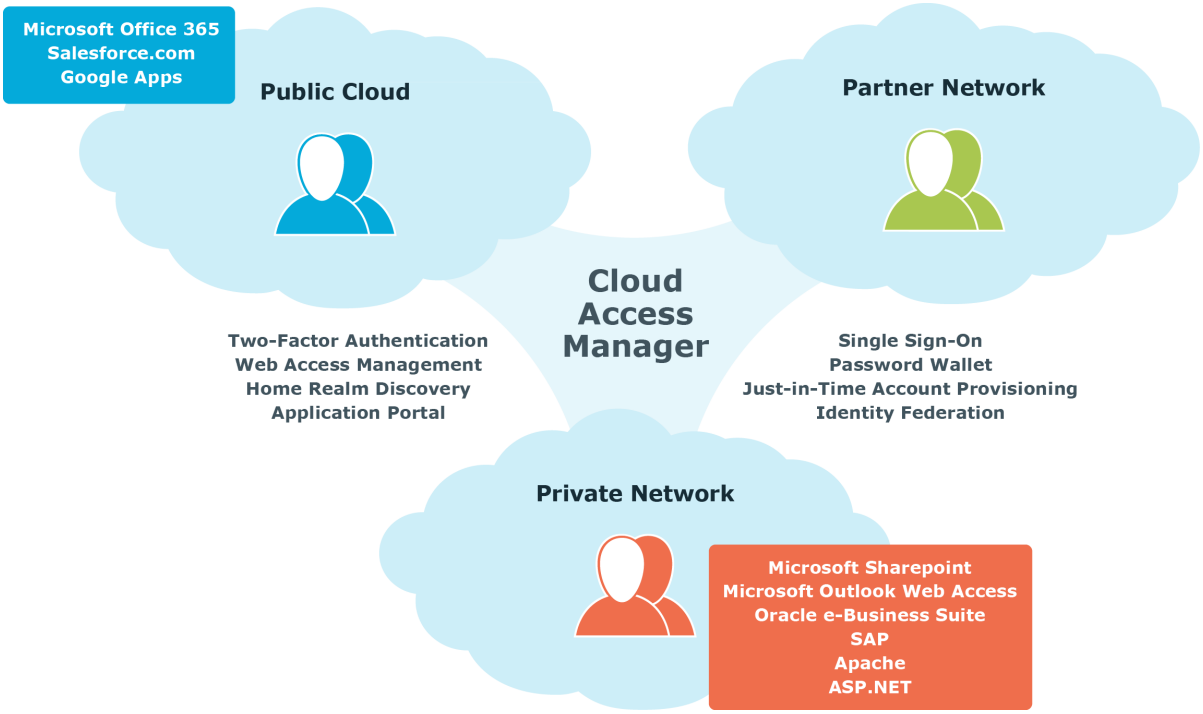
IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Cloud Access Manager Overview
Updated - October 2017
Version - 8.1.3

Contents

Overview

Cloud Access Manager is an identity bridge. It connects your users, your partners, and your customers to the applications they need.



Cloud Access Manager delivers real productivity gains to your end 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 (SS0) 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 expose your internal web applications securely 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 have access to.
- Identity federation with home realm discovery allows you to grant access to users in other forests within your own organization and in external organizations.
- For extra security you can configure Cloud Access Manager to require two-factor authentication for external users, or to protect sensitive applications.
- 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.
- vWorkspace integration seamlessly brings application virtualization to the Cloud Access Manager environment, allowing vWorkspace application links to be displayed in the application portal, along with other web applications.
- For extra security you can configure Cloud Access Manager to require two-factor authentication for external users, or to protect sensitive applications.
- The Security Analytics Engine provides adaptive authentication, this enables the types of authentication users require to access applications to vary based on a variety of risk factors.

Clientless web single sign-on

Cloud Access Manager can automatically log users on to almost any web application. While its web proxy component can automate login to applications that require Kerberos, NT LAN Manager (NTLM), HTTP, or forms-based authentication, its built-in security token service (STS) can provide Single Sign-On (SS0) to claims-aware applications that comply with either SAML or WS-Federation standards.

Cloud Access Manager's secure Password Wallet holds the user's application credentials. Once Cloud Access Manager has learned the user's credentials for an application, it will store them in the Password Wallet, and subsequently automatically forward them to the application whenever it is launched by the authenticated user through Cloud Access Manager.

In a Windows Active Directory environment, a Kerberos ticket is created and stored on a user's computer when the user logs in. This ticket allows the user to access services on the network without having to enter their username and password again. Because Cloud Access Manager can accept Kerberos tickets as a form of authentication, Windows authenticated users can launch their application portal directly, without the need to log on again.

In addition, because Cloud Access Manager uses a proxy-based approach to SSO, your users do not have to download any client software. Their credentials are stored safely in the Cloud Access Manager Password Wallet on your private network.

Web access management

Cloud Access Manager's web proxy component acts as a security gateway to protected applications on a private network. You do not have to install and manage plugins on all of your individual web servers — configuration, auditing and control is centralized through Cloud Access Manager — and because your applications can continue to run on your internal network, they are safely protected from many web-based attacks. In addition, you can grant access to application URLs through Cloud Access Manager's Role Editor.

Role-based access control

Privileges can be granted or denied easily and quickly through Cloud Access Manager's Role Editor. You can create roles for members and individual users from internal and external directories and the roles can then be applied to applications, groups of applications, and Cloud Access Manager administration functions.

Application portal

Users can view and access their applications through the customizable application portal. While applications granted by the Cloud Access Manager administrator appear automatically on the application portal page users can also add their own bookmarks to their favorite applications. In addition, users can access their Password Wallet from the application portal, to change the credentials that have been stored for a particular application, or configure auto-form fill behavior.

Federation with other identity providers

If you have multiple directory forests in your organization that need access to the same applications, or if you need to provide access to users in different organizations, you can do that with Cloud Access Manager. Cloud Access Manager can federate with any identity provider that can accept and process a SAML or WS-Federation authentication request.

Cloud Access Manager will extract the claims from the incoming assertion and use them to make authorization decisions based on its role configurations. At logon, Cloud Access Manager will allow the user to select the identity provider that they belong to. Using cookies, Cloud Access Manager will remember which identity provider was chosen.

Strong authentication options

You can configure Cloud Access Manager to require two-factor authentication for all users. When a user accesses Cloud Access Manager, in addition to their normal username and password, they will be prompted to enter a one-time password (OTP). To allow a user to supply a valid OTP they must physically possess an authentication device, this provides the additional assurance that the user attempting to log on is indeed who they claim to be.

Cloud Access Manager has the potential to only require two-factor authentication for users when the perceived threat level is above a certain threshold. This functionality requires the Security Analytics Engine which will determine the threat level based on a number of factors such as the location from which the user is logging in, the time of day, or if the user is running a different internet browser than expected.

NOTE: The strong authentication option requires One Identity Defender or another third-party strong authentication solution that supports the Remote Authentication Dial-In User Service (RADIUS) protocol.

Just-in time user account provisioning

When an authorized user needs access to an application for the first time, a new account must be set up for that user. Traditionally, as part of the hiring process, application user accounts are pre-emptively created for each user, whether they really need access to those accounts or not. This approach to user account provisioning can cause so-called authorization creep, where individuals are given access to systems that they may not even use and those privileges are never removed from the users.

Alternatively, accounts are provisioned manually as and when required. This promotes the principle of least privilege, by only giving your users access to resources that they need to do their job, but to do this manually for a large user population and a large number of applications is a significant management overhead.

Cloud Access Manager's just-in-time user account provisioning feature means that your users can access the applications they need at the point they need them with the minimum of administrative effort. For applications that are licensed per user, this can deliver significant savings since user accounts are no longer created unless they are actually used.

vWorkspace integration

You can configure Cloud Access Manager to connect to a vWorkspace server and retrieve a list of allowed resources, which can then be displayed on the Cloud Access Manager application portal.

How Cloud Access Manager Works

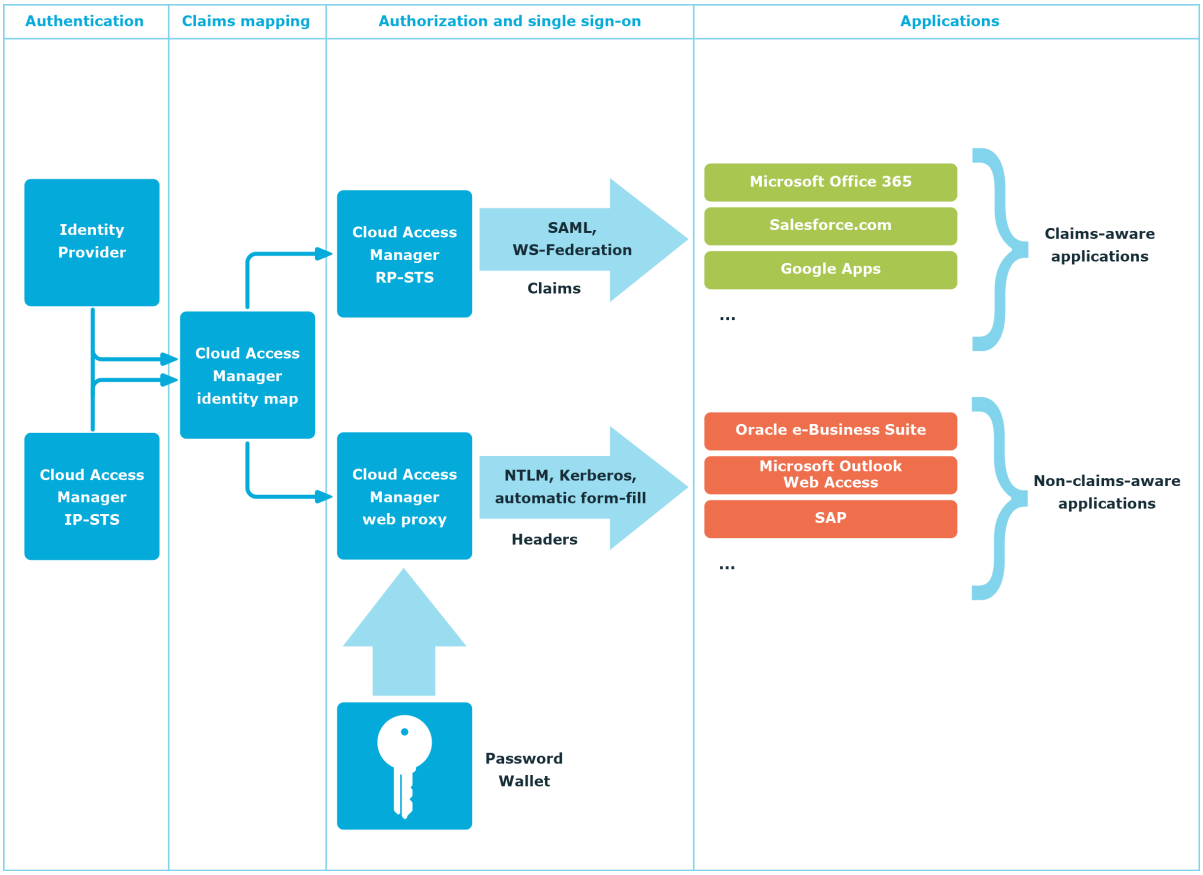
This section provides detailed information on how Cloud Access Manager works and describes:

Single sign-on

Cloud Access Manager uses protocol transition to translate credentials supplied to it at login into a form. The form can be consumed by applications the user accesses through Cloud Access Manager.

When a user enters their username and password at login this information can be used to:

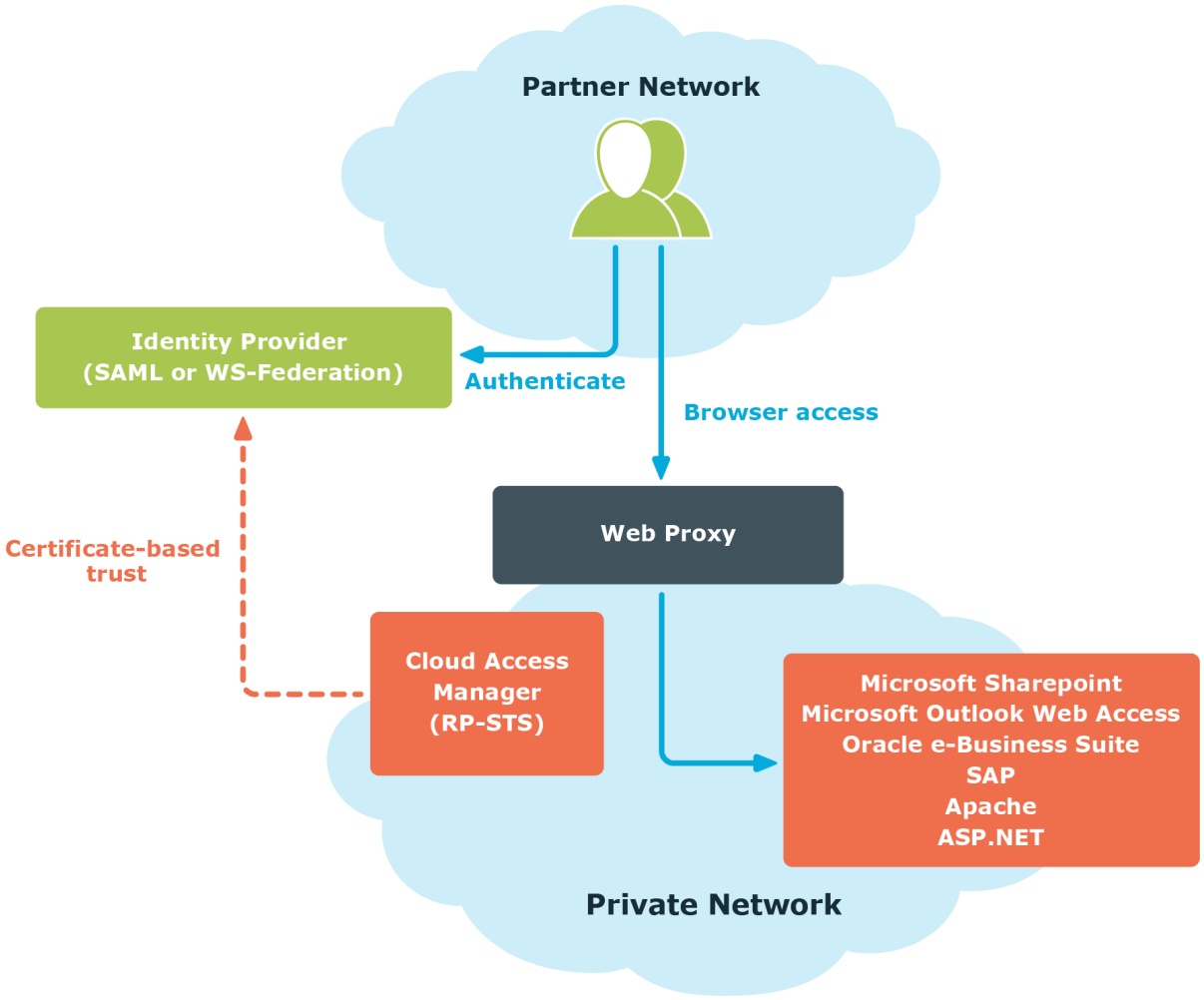
- Create a Kerberos ticket on-the-fly using delegation protocols to automate login to a web site supporting Windows Integrated Authentication.
- Generate a SAML assertion or WS-Federation security token — signed using Cloud Access Manager's identity provider certificate — to support Single Sign-On (SS0) to a claims-aware application.
- Key into the user's Password Wallet containing the usernames and passwords that Cloud Access Manager has remembered for that user, which in turn can be used to automate login to applications that support forms based, NTLM digest, or HTTP basic authentication.
- Generate an HTTP header containing the subject information, and forward it to the firewalled application. The application is modified to recognize and trust the header as an authentication token.



Authentication and identity federation

Cloud Access Manager allows you to set up front-end authentication to use any Lightweight Directory Access Protocol (LDAP) compliant user directory using its built-in Security Token Service (STS). If users in other organizations or forests need access to your applications, this can be achieved through identity federation. To do this, an identity provider must be installed on the remote network. If the identity provider is SAML or WS-Federation compliant, Cloud Access Manager can use it to authenticate the user.

You can configure Cloud Access Manager to extract claims from the security token sent by the identity provider. This information can make authorization decisions within Cloud Access Manager and can also be forwarded to the user's applications.



Two-factor authentication

You can configure Cloud Access Manager to enforce two-factor authentication. When the user attempts to access a Cloud Access Manager resource after entering their username and password, Cloud Access Manager makes a program call to an authentication service such as that provided by One Identity Defender. Cloud Access Manager will broker the authentication request between the user and the authentication service. The user will be asked for additional credentials according to the policy defined at the authentication service. For instance, the authentication service may require the user to enter a one-time password as generated by a handheld authentication device, usually referred to as an authentication token.

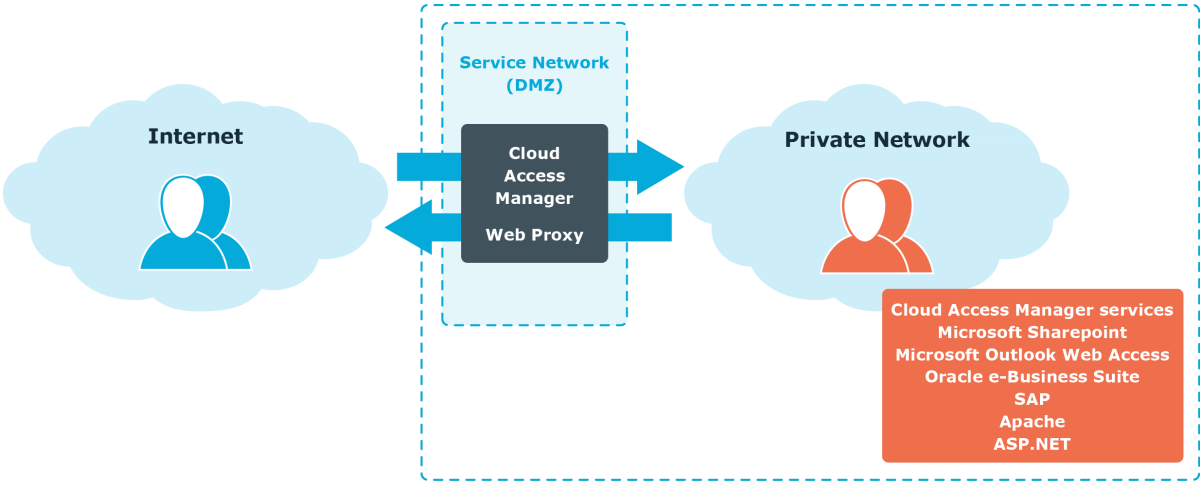
If you only want users to be prompted for two-factor authentication when they are accessing Cloud Access Manager at places or times that are atypical, you can use the integration with the Security Analytics Engine to implement this. The Security Analytics Engine takes input from the current user session as well as historical information about the user, and can potentially accept input from other sources, such as SonicWall devices, to

determine a threat level for the user. Cloud Access Manager then takes this threat level and uses it to determine whether the user is allowed immediate access, requires two-factor authentication, or is denied access.

NOTE: This feature requires authentication software, for example One Identity Defender, which is compliant with the Remote Authentication Dial-In User Service (RADIUS) protocol.

Web proxy and password wallet

Cloud Access Manager's web proxy component runs on a network perimeter and acts as a security gateway between users located on an untrusted network and applications running on a trusted network. It acts as a Secure Sockets Layer (SSL) endpoint relaying Secure HTTP (HTTPS) packets between the user's browser and the web application.



In addition to providing URL-based access control to firewalled applications, the web proxy also protects Cloud Access Manager web components such as the Security Token Service (STS) login pages, application portal and administration interface. The web proxy enforces authentication and authorization policies to applications running on the trusted network.

Because the web proxy stands between the user's browser and the web application, it can automatically log the user onto their applications by learning the user's application credentials, and inserting them when the user launches the application. When you configure an application, you can associate a login page URL with that application.

When the user attempts to access that URL, Cloud Access Manager automatically inserts the stored application user name and password into the appropriate form controls and posts the completed form back to the server. If Cloud Access Manager does not know the user's application credentials it prompts the user for them. The user's application credentials are encrypted in a Password Wallet within Cloud Access Manager's configuration database, the user can view and update the Password Wallet from the Application Portal.

Form-fill single sign-on without a proxy

While the use of a reverse HTTP proxy is effective as a method of exposing internal applications to external users, it also carries with it an associated cost, such as hardware deployment and maintenance and implies a performance degradation. For this reason if alternatives are available, the use of a reverse proxy solely to effect automated sign on to a web application is not the preferred method.

Cloud Access Manager makes it possible to launch certain web applications directly from the application portal, without the need to proxy the application. This can be useful in scenarios where extranet access to the application is not required.

Application coverage and support

Cloud Access Manager offers a number of options for implementing Single Sign-On (SS0) to applications, as well as the ability to expose applications to users using a reverse HTTP proxy.

While the majority of applications are supported using the technologies delivered by Cloud Access Manager, there may be certain applications that are not supported. Please contact Support if you have questions regarding support for any specific application.

NOTE: Public multi-tenant, cloud based applications are subject to change, possibly without warning, and usually beyond the control of the subscribing organization. Since form fill SSO methods can be adversely affected by such changes, we recommended that federated authentication is used in preference, where available.

Just-in-time user account provisioning

Cloud Access Manager allows users to request their own application accounts. If the user is in a group that is authorized to access a particular application, a user account can be automatically created for them as they select the application from their application catalog and add it to their portal page.

Cloud Access Manager is shipped with directory connectors that allow user accounts to be provisioned from Cloud Access Manager into:

- Google Apps service
- Salesforce.com
- Microsoft Office 365
- ServiceNow

When a user adds an application to their portal page by selecting it from their application catalog, Cloud Access Manager automatically checks whether they already have a user

account in that application's directory. If the user does not, then an account is created for them using one of Cloud Access Manager's directory connectors.

vWorkspace integration

Cloud Access Manager retrieves a list of allowed applications and desktops from the vWorkspace server and displays them on the application portal. The vWorkspace Connector must be installed on the client computer in order to launch a vWorkspace application. This requires vWorkspace 8.0 MR1 Hotfix 362760.

NOTE: The vWorkspace software uses an enhanced version of the Microsoft Remote Desktop client to deliver a user environment with a rich media and graphics experience, with applications delivered seamlessly from any number of sources, such as Microsoft Application Virtualization (App-V) or Remote Desktop Services (RDS) servers.

3

Summary

Cloud Access Manager is the next generation identity bridge, bringing together users, corporate web applications and cloud-based services into a cohesive ecosystem. Your organization makes significant productivity gains in terms of user account management, while access to your systems is protected with the level of security that you need.

Support for identity federation protocols allows you to extend access to your applications from other organizations securely and quickly, and a suite of reporting functions allows you to track, audit, and monitor identity management events, and to also analyze application and account usage.

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