Cloud Access Manager 8.1.4

Installation 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 Installation Guide
Updated - November 2018
Version - 8.1.4

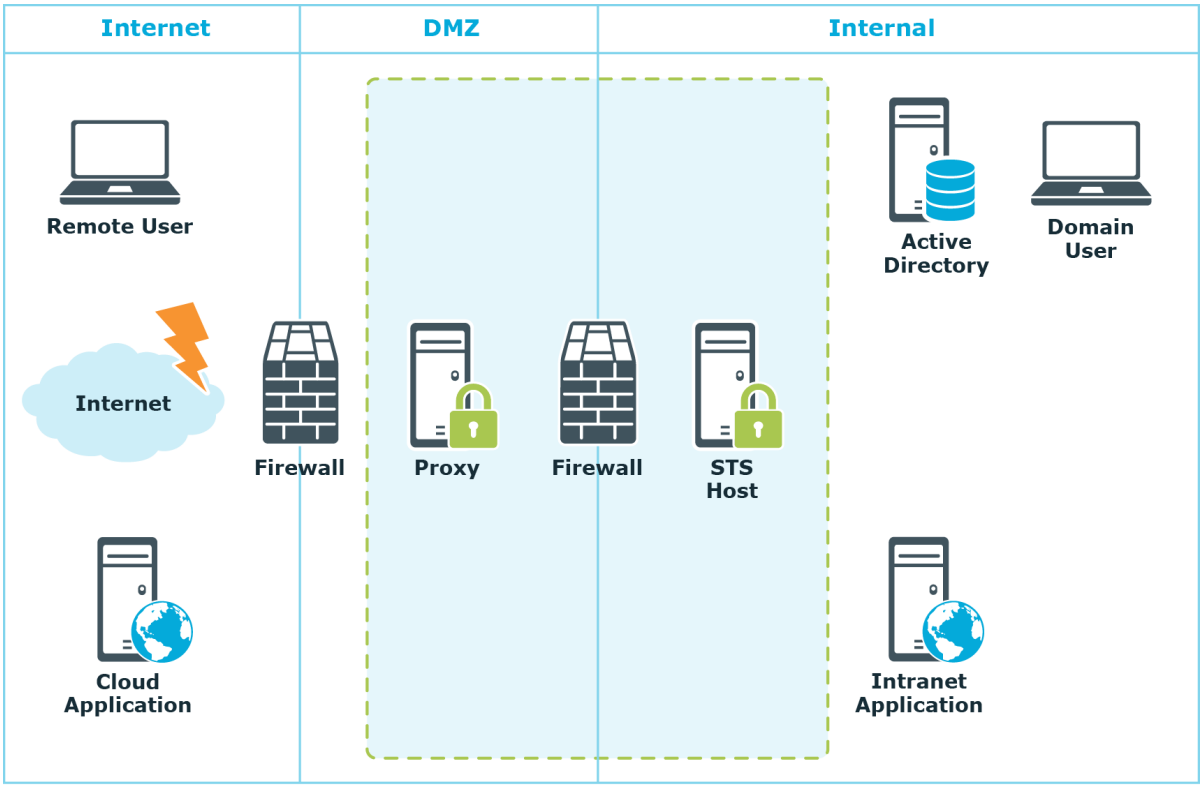
Contents

1

Installation

This guide will take you through the steps required to deploy a typical two host production installation of Cloud Access Manager. Once completed, Cloud Access Manager will allow employees to securely Single Sign-On (SSO) to internal and external web-based applications from within the company network and remotely, without the need for a virtual private network (VPN). This example uses two separate hosts, one for the Proxy and the other for the Secure Token Service (STS). The diagram below represents a typical Cloud Access Manager deployment, and shows the proxy host deployed within the DMZ area of the network and the STS host on the internal network.

Figure 1: Two host Cloud Access Manager deployment



Two host Cloud Access Manager deployment

Prerequisites

Make sure the following prerequisites are met before you attempt to install Cloud Access Manager, please refer to Proxy host and STS host on page 8 for component specific requirements.

NOTE: Please be aware that domain controllers are not valid Cloud Access Manager hosts.

Browser

Table 1: Browser requirements

Platform	Browser
Windows	• Microsoft Internet Explorer (version 10 and above)[1] • Google Chrome browser (latest) • Mozilla Firefox (latest)[1]
Mac	• Safari (latest)
iOS	• Safari (latest)
Android	• Google Chrome (latest)

[1] Supported for Integrated Windows Authentication (IWA).

Proxy host

Ensure the following prerequisites are met before installation:

Deployment location

To support the scenario illustrated in Two host Cloud Access Manager deployment on page 4 where you need to expose internal applications to external users, the host should be deployed within the DMZ network.

Hardware

Ensure that the following hardware requirements are met:

Table 2: Hardware

Hardware	Requirement
CPU	Min. 2 multi-core processors
Memory	Min. 4 GB
Disk Space	Min. 25 GB

Operating system

Ensure that the following operating system requirements are met with the latest Microsoft Hotfixes applied.

Table 3: Operating system

Hardware
Microsoft Windows Server 2008 R2 Microsoft Windows Server 2008 R2 Server Core or
Microsoft Windows Server 2012 Microsoft Windows Server 2012 Server Core or
Microsoft Windows Server 2012 R2 Microsoft Windows Server 2012 R2 Server Core

Name resolution

You must configure the host to use the internal Domain Name System (DNS) server(s) so that it can resolve the hostnames of the internal web applications that will be configured. In addition to the internal DNS, Cloud Access Managerrequires a public DNS record for the proxy host and an additional public DNS record for each internal application.

Each of these DNS records must be resolvable to the proxy's public IP address from outside of your corporate network. To avoid the need to create a new DNS record each time a new application is added to Cloud Access Manager, we recommend that you create a new wildcard DNS subdomain for Cloud Access Manager to resolve any name within the new subdomain to the public IP address of the proxy.

IP addressing

The host must be assigned a private IP address which is accessible from the internal network. For external access a public IP address is required. This is typically assigned to an internet facing router where destination network address translation (DNAT) or port

forwarding is performed to route traffic destined for ports 80 and 443 on a public IP address to the private IP address of the proxy host.

Wildcard DNS subdomain

Domain hosting companies typically allow the creation of a wildcard subdomain by adding a new DNS A (Host) record for your domain in the format *.subdomain, where subdomain is the name of the new subdomain you want to create for the Cloud Access Manager Proxy. Point the new DNS record to the public IP address used by the Cloud Access Manager Proxy so that any hostname in the new subdomain resolves to the proxy's public IP address.

For example, adding a new A record *.webapps to a domain called company.com would allow the Cloud Access Manager Proxy to use hostnames such as:

- portal.webapps.company.com
- webmail.webapps.company.com
- sharepoint.webapps.company.com

Essentially <anything>.webapps.company.com, this allows each internal application to have its own internet resolvable hostname.

To create a wildcard subdomain within the Microsoft DNS server you must first add a new subdomain (zone) and then add a single A (Host) record within the subdomain with the name *. As with the previous instructions, the new DNS record should be pointed to the public IP address used by the Cloud Access Manager Proxy so that any hostname in the new subdomain resolves to the proxy's public IP address.

Wildcard SSL certificate

A signed wildcard Secure Sockets Layer (SSL) certificate is required to cover the wildcard DNS subdomain used by the Cloud Access Manager Proxy. The wildcard SSL certificate must be obtained using the Certificate Signing Request (CSR) generated by Cloud Access Manager during configuration. For example, if you created a wildcard DNS subdomain called webapps within your domain company.com, then you would need to obtain a signed wildcard SSL certificate for *.webapps.company.com for full instructions, please refer to *Managing your SSL Certificate* in the *One Identity Cloud Access Manager Configuration Guide*.

Firewall configuration

Access to TCP ports 80 and 443 on the host should be permitted from both the internal and external network. The host should also be permitted to access the internal web applications through the ports they use, typically TCP port 80 and 443.

Port 8553

Port 8553 is the admin port used to configure the Cloud Access Manager Proxy. The proxy host downloads its configuration and then locally uses port 8553 to load the configuration. Ensure that port 8553 is not already being used by another application. If port 8553 is already in use, enter an alternative port number in the Cloud Access Manager proxy Installation Wizard. This port does not need to be open on the proxy host for Cloud Access Manager to function.

Smart card authentication

If you enable smart card authentication you will need to open the configured port. The default is port 8443.

STS host

Deployment location

The host should be deployed within the internal network.

Hardware

Ensure that the following hardware requirements are met:

Table 4: Hardware requirements

Hardware	Requirements
CPU	Min. 8 multi-core processors
Memory	Min. 8 GB
Disk Space	Min. 50 GB
Operating System	Any of the following: • Microsoft Windows Server 2008 R2 (with latest updates applied) • Microsoft Windows Server 2008 R2 Server Core (with latest updates applied) • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 Server Core • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 R2 Server Core

Domain membership

If Active Directory will be used to source users for SSO, the Security Token Service (STS) host must be a member of the Active Directory domain containing these users. Cloud Access Manager can also use federated identities from third party domains using SAML 2.0 or WS-Federation.

Name resolution

You must configure the host to use the internal Domain Name System (DNS) server(s) so that it can resolve the hostnames of the internal web applications that will be configured.

Database

Ensure that the following database requirements are met:

Table 5: Database specifications

Database	
Database Server	Microsoft SQL Server 2008-2017
Disk space (guideline, assuming typical usage)	200MB + 2K per user + 2K per user per day (audit)

Cloud Access Manager requires an instance of Microsoft SQL Server 2008-2017, to store its configuration, audit and session data. Microsoft SQL Server Express can also be used for small deployments, for example, where high availability of the database is not required.

Cloud Access Manager can either create its database within a new dedicated instance of Microsoft SQL Server installed directly on the Security Token Service (STS) host, or in an existing remote instance of Microsoft SQL Server deployed within your internal network.

NOTE: If you choose to use a dedicated instance of Microsoft SQL Server on the STS host, ensure that it is installed before you run the Cloud Access Manager installer.

Additional software

When you install Cloud Access Manager using the **Autorun**, as described in Installing Cloud Access Manager on page 11, the following software is automatically installed. This software is required for support purposes only.

- Microsoft .NET
- Windows Identity Foundation v3.5 (Pre 2012)
- LocalDB (if Proof of Concept installation)

- Microsoft System CLR Types for SQL Server 2012
- Microsoft SQL Server 2012 Management Objects

The UI/STS msi will install using Deployment Image Servicing and Management (DISM), (command line in brackets):

- IIS (`/online /enable-feature /featurename:IIS-WebServerRole/featurename:IIS-StaticContent /featurename:IIS-DefaultDocument /featurename:IIS-DirectoryBrowsing /featurename:IIS-HttpErrors /featurename:IIS-ISAPIExtensions /featurename:IIS-ISAPIFilter /featurename:IIS-HttpLogging /featurename:IIS-RequestFiltering /featurename:IIS-HttpCompressionStatic /featurename:IIS-ManagementConsole`)
- IIS, Server Core (`/online /enable-feature /featurename:IIS-WebServerRole/featurename:IIS-StaticContent /featurename:IIS-DefaultDocument /featurename:IIS-DirectoryBrowsing /featurename:IIS-HttpErrors /featurename:IIS-ISAPIExtensions /featurename:IIS-ISAPIFilter /featurename:IIS-HttpLogging /featurename:IIS-RequestFiltering /featurename:IIS-HttpCompressionStatic /featurename:IIS-ManagementService`)
- HTTP Activation, 2008 R2 (`/online /enable-feature /featurename:NetFx3 /featurename:IIS-NetFxExtensibility /featurename:WAS-ProcessModel /featurename:WAS-WindowsActivationService /featurename:WAS-NetFxEnvironment /featurename:WAS-ConfigurationAPI /featurename:WCF-HTTP-Activation`)
- HTTP Activation, 2008 R2 Server Core (`/online /enable-feature /featurename:NetFx3-ServerCore /featurename:IIS-NetFxExtensibility /featurename:WAS-ProcessModel /featurename:WAS-WindowsActivationService /featurename:WAS-NetFxEnvironment /featurename:WAS-ConfigurationAPI /featurename:WCF-HTTP-Activation`)
- HTTP Activation, 2012 and above (`/online /enable-feature:WCF-HTTP-Activation45 /all`)
- WCF Services, 2012 and above (`/online /enable-feature:WCF-Services45`)
- ASP .NET 4.5, 2012 and above (`/online /enable-feature: NetFx4Extended-ASPNET45 /all`)

If you want to install this software using a local path, rather than the default internet sourcing use the `DismSource` switch to specify where the Cloud Access Manager bootstrapper will instruct the DISM tool to look for the required files. For example, if the installation CD is in drive D then you could specify:

```
“Cloud Access Manager Setup.exe" DismSource=d:\sources\sxs
```

As an example, this will result in a call to DISM similar to the following:

```
dism.exe /online /enable-feature:Windows-Identity-Foundation /source:d:\sources\sxs
```

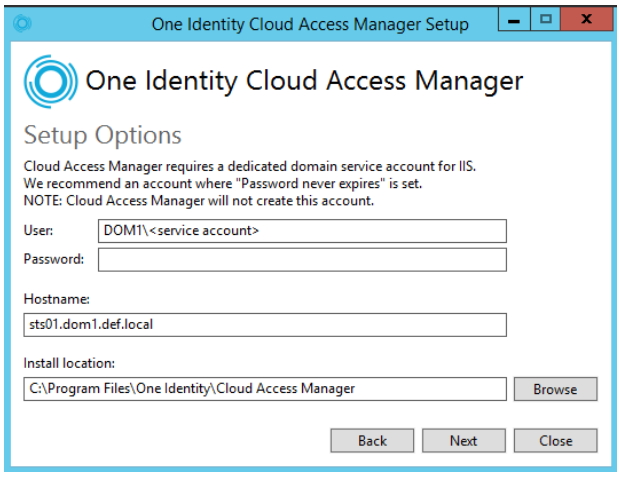
Installing Cloud Access Manager

To install Cloud Access Manager

1. On the Security Token Service (STS) host, either mount the hotfix ISO or extract the hotfix ZIP file to a temporary location.
2. Start the **Autorun** and navigate to the **Install** section.

   NOTE: The Autorun cannot be used for Cloud Access Manager STS and Proxy host installations running Server Core installations of Microsoft Windows Server. You must run the installer files directly from the command line.

3. Click **Install** on the **Cloud Access Manager IIS Components**.
4. Accept the License Agreement. Click **Next**.
5. Click **Production Installation**.



6. Choose the account to run the STS components, enter the username and password of an Active Directory domain account. This account does not require special administrative privileges but a dedicated service account is recommended, ideally with **Password never expires** set.

   NOTE: The account specified must exist prior to installation of Cloud Access Manager. The account credentials entered must be successfully verified before you can proceed with the installation.

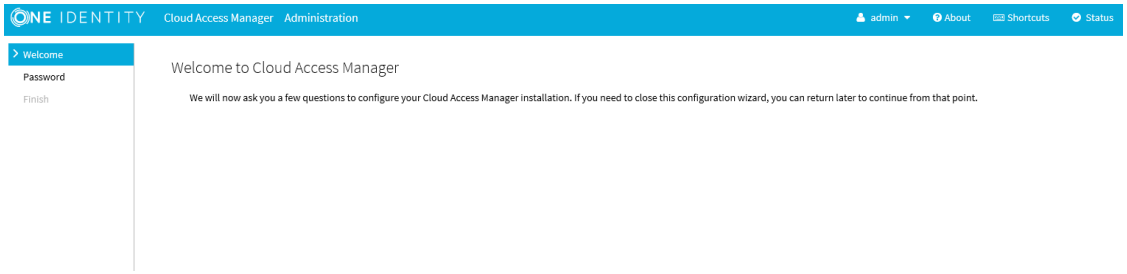
7. Click **Install** to deploy the components required for the STS host.

   NOTE: The STS host 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.

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

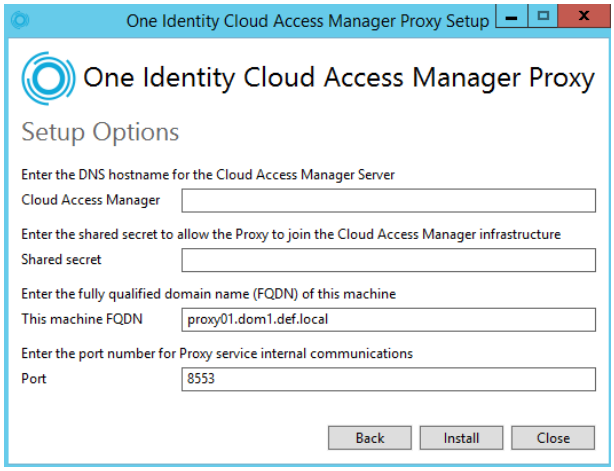
   NOTE: On a Server Core installation you will need to access the configuration wizard from a separate machine. The last page of the Cloud Access Manager install wizard will show the URL for the configuration page.

9. The configuration wizard can take a while to open when accessed for the first time. This is due to Internet Information Services (IIS) initializing and starting the web applications. Please wait while Internet Explorer opens and displays the **Cloud Access Manager Welcome** page.

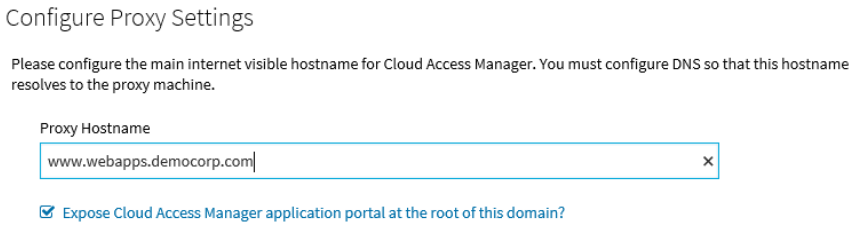


10. When the configuration wizard has loaded, click **Next**.
11. Choose and enter a shared secret and recovery password. You will need to enter the shared secret defined on this page during the installation of the proxy host, you will install the proxy host later in the installation procedure. The recovery password can be used 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**.
12. Enter credentials that have administrative privileges for the MicrosoftSQL Server instance, typically a member of the administrators group, that will be used by Cloud Access Manager. The credentials will be used to create a new database for Cloud Access Manager. Click **Next**.
13. Click **Download Proxy Installer** and save the installer to a temporary location on the STS host. When the download is complete, transfer the installer to the proxy host.
14. Switch to the proxy host and double-click the proxy installer **Cloud Access Manager Proxy Setup.exe** to start the proxy install.

15. Accept the License Agreement and then click **Next**.



16. Enter the hostname of the STS host specified earlier, and the shared secret specified in Step 11. Click **Install**.
17. The proxy installation will now start. When complete, click **Close**.
18. Return to the STS host. In the Cloud Access Manager browser window, click **Next** on the **Install the Proxy** page.



19. Enter a hostname to use for your Cloud Access Manager portal. This should be a hostname within the wildcard DNS subdomain created for the Cloud Access Manager Proxy. For example, if you created a wildcard DNS subdomain called webapps within your domain company.com, then you may want to use www.webapps.company.com or portal.webapps.company.com or any other hostname that ends in .webapps.company.com. This hostname is what your users and administrators will use to access the Cloud Access Manager portal.
20. Click **Next**.
21. Cloud Access Manager will now configure the required components. When the configuration is complete, click **Finish**.

This installation of a typical two host production deployment of Cloud Access Manager is now complete.

Configuring Cloud Access Manager

Now that you have successfully installed Cloud Access Manager, you need to:

- Configure a front-end authentication method to tell Cloud Access Manager how to authenticate and authorize users
- Add a web application
- Manage your SSL certificate.

Please refer to the *One Identity Cloud Access Manager Configuration Guide* for further information.

Cloud Access Manager backup and restore

The following sections describe how to perform a complete backup and restore of Cloud Access Manager.

- Backup
- Restore

Backup

To back up One Identity Cloud Access Manager

1. On the Proxy host, backup the following configuration files:

   <CAM_INSTALL>\bin\svc_in.bat

   <CAM_INSTALL>\conf\server.xml

   Where <CAM_INSTALL> is the location where the Cloud Access Manager Proxy is installed. The default location is C:\Program Files\One Identity\Cloud Access Manager Proxy.

2. On the Database host, backup the following databases used by Cloud Access Manager:

   CTAudit

   CTData

   CTSession

Restore

To restore One Identity Cloud Access Manager from a backup

NOTE: If you are recovering from an OS failure, first restore the full OS backup using the last known good backup.

1. On the proxy host, uninstall the Cloud Access Manager Proxy using the **Uninstall a program** option in the Windows Control Panel.
2. On the Security Token Service (STS) host, uninstall Cloud Access Manager using the **Uninstall a program** option in the Windows Control Panel.
3. On the database host, restore the following databases used by Cloud Access Manager, making sure you use a backup taken from the same version you want to revert to:

   CTAudit

   CTData

   CTSession
4. On the STS host, install the version of Cloud Access Manager you want to revert to, making sure the account name and hostname specified during the installation match those used during the original installation.
5. When the configuration wizard starts, specify the same password for the shared secret and built-in admin account as used during the original configuration.
6. When prompted to setup the database, specify the credentials and optionally the hostname for your existing database.
7. When prompted, install the proxy on the proxy host, ensure:
   - The version of the Cloud Access Manager Proxy matches the Cloud Access Manager version installed on the STS host.
   - You specify the same hostnames and shared secret used during the original installation.
8. On the Proxy host, restore the following configuration files:

   <CAM_INSTALL>\bin\svc_in.bat

   <CAM_INSTALL>\conf\server.xml

   Where <CAM_INSTALL> is the location where the Cloud Access Manager Proxy is installed. The default location is C:\Program Files\One Identity\Cloud Access Manager Proxy.
9. On the Proxy host, run the following commands from a command prompt for the new configuration to take effect:

   <CAM_INSTALL>\bin\svc_out.bat

   <CAM_INSTALL>\bin\svc_in.bat

Where <CAM_INSTALL> is the location where the Cloud Access Manager Proxy is installed. The default location is C:\Program Files\One Identity\Cloud Access Manager Proxy.

10. Return to the STS host and continue with the Cloud Access Manager configuration wizard.
11. Accept your existing proxy hostname and verify that the installation completes successfully.
12. Verify that an admin user and a regular user can both login and use Cloud Access Manager as before.

Upgrading Cloud Access Manager

This section describes how to upgrade previous versions of One Identity Cloud Access Manager.

IMPORTANT: There is no option for upgrading Cloud Access Manager 8.1.2 to 8.1.4. Please contact the One Identity Professional Services team if you wish to migrate your system from 8.1.2 to 8.1.4.

Upgrading Cloud Access Manager

1. Ensure that you take a backup of your entire Cloud Access Manager system. The backup procedure is described in Backup on page 14.
2. Run the new **Cloud Access Manager setup.exe** on all Cloud Access Manager Security Token Service (STS) hosts.
3. Run the new **Cloud Access Manager proxy setup.exe** on all Cloud Access Manager Proxy hosts.

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