Cloud Access Manager

For a look at Teradici’s Cloud Access Software component downloads and documentation, visit Teradici Cloud Access Software.

What is Cloud Access Manager?

Cloud Access Manager enables highly-scalable and cost-effective Cloud Access Software deployments by managing cloud compute costs and brokering PCoIP connections to remote Windows or Linux workstations. The Cloud Access Manager solution is comprised of two main components – the Cloud Access Manager service, which is a service offered by Teradici to manage Cloud Access Manager deployments, and the Cloud Access Connector, which is the portion of the Cloud Access Manager solution that resides in the customer environment.

The following image outlines the Cloud Access Manager architecture for an on-premises scenario:
The following image outlines the Cloud Access Manager architecture for a public cloud scenario:
The following image outlines the Cloud Access Manager architecture for a multicloud scenario:
You must download, authenticate and then install the Cloud Access Connector. For more information on installing the Cloud Access Connector, see *Installing a Cloud Access Connector*.

---

**Customer Costs**

Customers are responsible for the cloud computing costs associated with the Cloud Access Connector and the remote workstations that they create and run.
Who Should Read This Guide?

This guide provides information for system administrators and IT professionals on using Teradici Cloud Access Manager. This guide provides instructions on how to enable and activate Cloud Access Manager's feature set.

Teradici Glossary

For a glossary of terms and conditions associated with Teradici technology, see Teradici Glossary.
Key Concepts

The following concepts are terms used in the documentation and can be referred to when using Cloud Access Manager (CAM).

**Organization** – A user or group in possession of a valid Cloud Access Software license.

**Organization Administrators** – People who can manage Cloud Access deployments, Cloud Access Connectors, remote workstations within CAM.

**Deployment** – A way to organize the provisioning and power management of remote workstations as well as entitling users, from the Active Directory (AD), to these remote workstations.

- Use case: an IT admin would like to setup a production and a staging (or sandbox) environment. Two Cloud Access deployments would be setup, one called production and the other called staging.
- Use case: a service provider is managing the environment for three customers. Three Cloud Access deployments would be setup: Acme Association, Better Biz, and Cool Company.
- Use case: an IT admin would like to setup a production and a DR (disaster recovery) environment. Two Cloud Access deployments would be setup, one called production and the other called DR.
- Use case: an IT admin wants segregated groupings of remote workstations and access policies.

**Remote Workstation** – A remote desktop running Windows or Linux OS.

**Cloud Access Connector** – Software that is installed in a customer environment, for example Google Cloud Platform (GCP), Amazon Web Services (AWS), Azure or on-premises, that provides connectivity between the PCoIP clients and the remote workstations. The Cloud Access Connector provides a single point of entry into a deployment of remote workstations. It communicates with the CAM Service (SaaS operated by Teradici) and is part of a deployment. A deployment can have one or more Cloud Access Connectors. It includes a NAT function for access through an IP address.

- Use case: an IT admin has a hybrid environment where some remote workstations are on-premises and others are in the cloud (i.e. GCP, AWS, Azure, on-premises). For a given
deployment, a connecter would be installed within the customer’s cloud subscription as well as a connecter would be installed within the customer’s on-prem environment (i.e. a VM running on ESXi). The customer should use the Connecter that is geographically closest to their associated workstation to minimize egress costs and ensure the best performance.

- Use case: an IT admin has three offices (London, San Francisco, and New York) where remote workstations are deployed in the cloud (i.e. GCP, Azure, or AWS) which are closest to these three offices. For a given deployment, three Connectors would be installed within the customer’s cloud subscription in London, WestUS and EastUS.

**Users** – People that are present in the AD. These people are assigned remote workstations to connect to.

**CAM Admin Console** - A web application that can be used by an IT admin to manage and assess their Cloud Access deployments, Connectors and remote workstations. It can be accessed by opening a web browser and connecting to [https://cam.teradici.com/](https://cam.teradici.com/).

**Cloud Access Manager Management Interface** - A legacy web interface that exists within the Cloud Access Connector. It should only be used for Azure deployments. For AWS, Google Cloud and On-Prem deployments we recommend using the CAM Admin Console.

**Private Cloud** - Computing services offered over the internet or a private internal network to select users instead of the general public. Private Cloud is used to define clouds or hypervisors that Cloud Access Manager is unable to directly interact with.

**On-Premises** - Also sometimes shortened to **On-Prem**, this is services and applications that run on a customer’s hardware within their own data centre.
System Requirements

The following section lists the system requirements for Cloud Access Connector, Cloud Access Software, DC servers, authentication service and browsers compatible with the Cloud Access Manager Admin Console.

Cloud Access Connector

- Ubuntu Server 18.04.
- 4GB RAM or more.
- 12GB available storage or more.
- 2 vCPUs or more.

For information on the session establishment and session bandwidth limits when working with external connections, see here.

These environment conditions must be met:

- The server must be able to resolve the AD domain.
- You must be able to access the server using SSH.
- You must have superuser (sudo) privileges on the server.

Supported Browsers for the Admin Console

- Firefox
- Google Chrome

Supported Domain Controller Servers

- Windows 2016 Server with Secure LDAP (LDAPS) enabled.
- Windows 2012 R2 Server with Secure LDAP (LDAPS) enabled.
Authentication Service

Cloud Access Manager Admin Console

• Azure Active Directory organizational email address or a G-Suite or Google Cloud Identity enterprise account.

Remote Workstations and Workstaton users

• Active Directory.

Cloud Identity Accounts

Personal Gmail accounts are not supported by default and need to be whitelisted by Teradici before being used. For access to Cloud Access Manager with a personal Gmail account, contact Teradici sales or open a support case.

Cloud Access Software

• License registration code emailed from Teradici in the form of ABCDEF1234@AB12-C345-D67E-89FG.

• A PCoIP Standard or Graphics agent installed on the remote workstation.

• To connect to remote workstations you require a client. The following are the supported clients with Teradici:
  • Teradici PCoIP Software Clients for Mac, Windows or Chrome OS
  • Teradici PCoIP Mobile Clients for iOS and Android tablets
  • Teradici PCoIP Zero Clients

Required External Connections

The Cloud Access Manager requires certain external connections and sites to be available to enable the Cloud Access Manager Service to function properly. The following sites need to be whitelisted and should be available to access:

• cam.teradici.com
This is Cloud Access Manager. It is required for both API usage and to access the Cloud Access Manager Admin Console user interface.

- **archive.ubuntu.com**
  Source for first-party Ubuntu packages; required so that the OS on the Cloud Access Connector remote workstation can be kept up to date. This address is location dependent, so for example if you are in the USA it would be us.archive.ubuntu.com, or if you were in Canada it would be ca.archive.ubuntu.com.

- **teradici.compliance.flexnet.com**
  Required for license verification when installing the Cloud Access Connector. Required for Cloud Access Software Agent license activation and verification during session establishment.

- **teradici.bintray.com**
  Source for Cloud Access Connector components, configuration files and the Cloud Access Connector installer; required in order for the Cloud Access Connector to be installed, configured and updated over time.

- **download.docker.com**
  Source for Docker; required so that Docker can be installed to run the Cloud Access Connector.

- **sumologic.com**
  Endpoint for log aggregation; logs from the Cloud Access Connector components are sent to Sumo Logic. For more details on the information we collect and how we collect it, please see the Cloud Access Manager Privacy Policy.

- **teradici-docker-registry.bintray.io**
  This is used by the installer to download docker containers used by the Cloud Access Connector that are developed and maintained by Teradici.

- **hub.docker.com**
  This site is used to download the public docker containers. These are not maintained by Teradici.

The following domain networks need to be whitelisted:

- **teradici.compliance.flexnetoperations.com**: This domain is used by the installer for licensing and validating the registration code. It is the operations website for Flexera.
• *akamai.bintray.com*: This is a Teradici docker container repo.
• *registry-1.docker.io*: This is a public docker repo.
• *production.cloudflare.docker.com*: This is a public docker repo.

---

**Whitlisting IP Addresses**

If you are still having issues with installation after whitelisting all the required sites and domains, try to resolve the failing sites by resolving the associated IP addresses. You can also try whitelisting these IPs in your firewall.
The Cloud Access Manager Admin Console enables you to create deployments, connectors and remote workstations all within a single console and from a single interface. You can track all these components from the interface of the console, as well as monitor and manage all aspects of your deployment infrastructure. You can access support, release notes and get service status information from the console also. The diagram below outlines a connection workflow for both cloud and on-premises scenario's using the Cloud Access Manager Admin Console. For further information on the components in this diagram, see Key Concepts.
Connecting to the Admin Console

Go to the Cloud Access Manager Admin Console https://cam.teradici.com/ login page and log in with your Enterprise Microsoft Azure account, or if you are logging in through Google, a G Suite or Cloud Identity account. Enter your credentials to access the Admin Console.

If you encounter issues logging into the Cloud Access Manager Admin Console, it could be for one of the following reasons:

- The account being used is a personal account and has not been white-listed by Teradici.
- Cookies have been blocked on https://cam.teradici.com/.

Email Account Support with Cloud Access Manager

Cloud Access Manager supports two types of email accounts:

- Company email accounts registered with Google G Suite.
- Company email accounts registered with Microsoft Azure Active Directory services. For more information on this account type, see Microsoft Azure Active Directory Authentication.

Personal Gmail accounts are not supported by default and need to be whitelisted by Teradici before being used. For access to Cloud Access Manager with a personal Gmail account, contact Teradici support. Cloud Access Manager does not support Microsoft personal email accounts.
• Pop-ups have been blocked on https://cam.teradici.com/.

If you continue to experience issues logging into the Cloud Access Manager Admin Console, contact Teradici Support.
Cloud Access Manager Admin Console Dashboard

Once you log into the Cloud Access Manager Admin Console you will see the dashboard page. This dashboard acts as a quick-start guide which points to where you can create deployments, create Cloud Access Connectors, add remote workstations as well as provide links to useful information within the Cloud Access Manager documentation.

You can return to the dashboard page at any time by clicking the Dashboard option from the console sidebar.

Configuring the Cloud Access Manager Admin Console

On the Deployments, Connectors and Remote Workstations pages you can control which columns are visible and in which order they appear for the listed resources. To change your
column options, select **COLUMNS** from the page heading and select which columns you wish to make visible.

The format you select will be preserved when you log back into the Cloud Access Manager Admin Console.
Creating a Deployment

The following section outlines how to create a deployment using the Cloud Access Manager Admin console:

1. If you do not have any existing deployments (first time log-in) you will be prompted to enter your Cloud Access Software registration code. Once you enter the code it will automatically generate your first deployment and take you to the Edit Deployment page.

![Unlock Cloud Access Manager Admin Console](image)

You need a registration code to activate your PCoIP agent and to use it in conjunction with Teradici Cloud Access Manager. Once you subscribe to a Cloud Access Software subscription your registration code will be in an email sent to you from Teradici.

If you are an existing customer and have a subscription but have lost your registration code, then you need to submit a ticket with support.

2. If you have existing deployments you can click Create deployment from the kebab options at the top of the page to take you to the Create Deployment page.

© 2019 Teradici
3. Enter the following information:
   • Enter the deployment name.
   • Enter your Cloud Access Software registration code.

4. You can optionally enter GCP or Azure credentials if you are working in those environments and want to enable Cloud Access Manager to perform certain functions, such as power management. If you are not using GCP or Azure then you do not need to enter this information.

5. You can enable GCP cloud credentials by entering the GCP client email, Project ID and Private Key and clicking VALIDATE to ensure the GCP account and key are valid. For Azure you need to enter the Tenant ID, Subscription ID, Client ID and Client Secret.

   For information on how to create a new Client Secret from Azure, see here.
Entering these credentials is optional and enables you to access extra functionality and control over the remote workstations within the deployment on the cloud provider of your choice.

6. Click **CREATE**.

The newly created deployment is now listed on the deployments page.

You can delete multiple selected deployments by selecting the check-all box at the top of the page. This enables you to manage your deployments more efficiently.

### Azure Client Secret

Once you generate the client secret you need to copy it straight away as it will not be available again from Microsoft. If you have an expired client secret you need to delete it and then create a new secret and assign it to that deployment.

### Domain Controllers in a Single Deployment

You cannot deploy multiple Cloud Access Connectors against different Domain Controllers within the same deployment. This will cause the Cloud Access Connectors to crash.

---

**Editing an Existing Deployment**

The creation date, computer and users DNs and the interval time in minutes that it syncs with the Active Directory for the deployment are also displayed when you go to edit a specific deployment.

You can search for specific deployments by name by using the search bar in the table toolbar.

You can edit the deployment name, update the registration code and GCP or Azure cloud service account credentials of an existing deployment through the CAM Admin Console. A menu item has been added to the table toolbar that enables you to create, edit, delete and view all existing deployments.

1. Click the dropdown from the top of the page and select the deployment.

2. Select the deployment and click the kebab option under the **ACTIONS** column to edit the deployment.
3. Update the deployment name, registration code, GCP or Azure credentials and then click SAVE.

The updated information and credentials will now be reflected for the deployment.

**Azure Client Secret**

Once you generate the client secret you need to copy it straight away as it will not be available again from Microsoft. If you have an expired client secret you need to delete it and then create a new secret and assign it to that deployment.
Service Account and API Access

Cloud Access Manager provides direct API access in the Cloud Access Manager service. API's are an advanced way of interacting with the service, which enables you to integrate it into your business systems or to automate your use of the service for your specific needs.

Teradici Advantage Partner Program

To access and use the Cloud Access Manager APIs, you must be a member of the Teradici Advantage Partner Program (TAPP) or have been pre-approved by Teradici. Contact Teradici here for more information.

Teradici provide two levels of access:

Service Accounts: There are two types of service accounts that you can create with the Cloud Access Manager Admin Console:

CAM Service Accounts

The CAM service account is an account that is created from the Cloud Access Manager Admin Console for the purpose of creating future deployments and deployment service accounts through the Cloud Access Manager APIs. The CAM service account cannot perform any actions within a deployment, and so further actions to a deployment require the deployment service account, which is outlined below. For information on creating a CAM service account, see here.

Deployment Service Accounts

Deployment service accounts are specific accounts that can only perform actions against the deployment, such as adding remote workstations. The deployment in this case is the deployment the service account is created within. They cannot perform actions against any other deployment. For information on creating a deployment service account, see here.

API Access Token: The API Access Token can be used to enable a user to operate at a level above deployments, such as creating a new deployment. The API Access Token is only valid for a limited period of time.

For more detailed information on accessing the Cloud Access Manager APIs, see https://cam.teradici.com/api/docs.
Creating a CAM Service Account

You can create a CAM service account from within the Cloud Access Manager Admin Console. The following steps outline how to create a CAM service account.

1. Click on your account name and select CAM service account.
2. Click the + icon from the CAM service account page and name your new account.

3. Once you have created the CAM service account download the JSON file or copy the key id. Ensure that you store the file securely as the key cannot be recovered if lost.

4. Go to the Service Account Keys section of the Cloud Access Manager API documentation for the required APIs to use this key to create a deployment.

Creating and Assigning a Deployment Service Account

You can create and assign a deployment service account to a deployment through the Deployments option within the Cloud Access Manager Admin Console. The following steps outline how to add a deployment service account to an existing deployment:

1. Click on your deployment from the console dropdown to display your existing deployments.
2. Click the kebab icon and click Edit deployment to display the deployment properties page.
3. Under the **Deployment Service Accounts** tab click the + sign to create a service account.

4. Once the service account has been created it will return service account information. This information should be saved as a JSON file in a secure location, as it can only be retrieved once. It will return a Cloud Access Manager API token that you can use to query the Cloud Access Manager APIs. This token is only authorized to access resources associated to the deployment that service account is associated with.

All deployment service accounts associated with a specific deployment will be listed on the deployment page. You can delete deployment service accounts from this page. For information on using the deployment service accounts and deployment service keys with the Cloud Access Manager APIs, see [here](#).
Obtaining a Cloud Access Manager API Access Token

API access tokens permit you to enable other tools and applications to interact with Cloud Access Manager through public APIs. The access token has tenant level permissions, which enables you to access all of a user’s resources from any deployment.

To obtain a Cloud Access Manager API Access token:

• Click Get API token from the user account icon within the Cloud Access Manager Admin Console. You will receive the following message:

You need to copy the token as it will expire after a period of time.

You need to copy the token as it will expire after a period of time.

To access and use the Cloud Access Manager APIs, you must be a member of the Teradici Advantage Partner Program or have been pre-approved by Teradici. Contact Teradici here for more information.
Creating and Installing a Cloud Access Connector

Once you have created a deployment you need to download the Cloud Access Connector installer, obtain a Cloud Access Connector token and use this token to install your Cloud Access Connector. For information on how to do carry out these steps, see Cloud Access Connector Installation. When you are creating your Cloud Access Connector through the Cloud Access Manager Admin Console you will be pointed to the relevant content for each step on the Creating a new Connector page.
Editing a Cloud Access Connector

Once you have created a Cloud Access Connector you can edit its name by clicking on the Cloud Access Connector directly from the Connectors page or by clicking on Edit from the kebab associated with it on the Connectors page.

You can search for specific Cloud Access Connectors by name by using the search bar in the table toolbar.

Enter the new name and click Save.

---

Domain Controller Certificates

If all DC certificates have expired, the Cloud Access Connector will stop working. An error indicator will display on the Connectors page when a Cloud Access Connector has a DC with expired certificates.

A warning indicator that details the current state of the DC certs will display on the same page when a Cloud Access Connector has a certificate that less than a week away from expiring.

---

Cloud Access Connector - Troubleshooting

If there is an issue installing the Cloud Access Connector or an existing Connector is failing, please see the troubleshooting section on Cloud Access Connector Connectivity. Within this section there are steps to check the following:

- Remote Workstation connections
- Active Directory connections
- Cloud Access Connector component information
Provisioning a Remote Workstation

The following section outlines how to provision a remote workstation using the Cloud Access Manager Admin Console.

**Pre-Defined Images and Templates**

If you wish to use your own custom images or templates, you must create and manage those outside of Cloud Access Manager and create your remote workstation outside of Cloud Access Manager also. Once you have created a remote workstation you can add it to your deployment in Cloud Access Manager for brokering and management, see here.

**Cloud Service Account Capabilities**

For information on which Cloud Service accounts can perform certain features, please consult the Service Account Requirements section.

You must have a valid cloud service account to enable this feature:

1. Click **Remote Workstations** from the console sidebar.
2. Click **Create new remote workstation** from the add remote workstation icon.
3. Select an existing Cloud Access Connector from the dropdown menu.
4. Select a provisioning template from the dropdown menu and give your remote workstation a machine name. You can also choose whether you want to enable an automatic restart of the workstation. Compute engine can automatically restart remote workstation instances if they are terminated for non- user initiated reasons, such as maintenance events, hardware failures, software failures, etc.
5. Enter the remote workstations network, region and disk properties. An example of what this information may look like is shown below:

![Remote Workstations > Create Remote Workstation]

**SELECT A CONNECTOR**

Connector: test-cn

**DEFINE THE WORKSTATION**

![CentOS 7.5 Graphics Agent - 20190731...]

Machine name: new-machine

Automatic restart: Automatically restart this machine

**MACHINE PROPERTIES**

Region: us-west2

Zone: us-west2-b

Subnetwork: aben-subnet-cac - 10.0.1.0/24

Machine type: n1-highmem-64

GPU type: NVIDIA Tesla P4

Number of GPUs: 1

Disk type: SSD Persistent Disk

Disk size (GB): 50

When deleting this machine: Also delete this boot disk

---

**Public IP or Cloud NAT requirement**

Provisioning will fail unless the machine has a public IP or Cloud NAT.

**Remote Workstation machine name configuration**

Due to NetBIOS and a Windows limitation, the remote workstations machine name must be 15 characters or less. Failure to do this may result in issues with your remote workstation connection.

1. Enter the Active Directory information for the remote workstation. The service account must have permission to join computers to the domain.

2. Once you have entered all required information, click **CREATE**.
The remote workstation will now appear in the table of available machines on the Remote Workstations page.

---

**Active Directory Information**

Active Directory information is only used during provisioning to join the remote workstation in question to the domain. This information is not saved by the Cloud Access Manager. The remote workstation is joined to the active directory domain configured in the Cloud Access Connector.

---

**Metadata Retrieval and Storage Information**

All provisioned remote workstations have `--metadata enable-guest-attributes=TRUE` set. This is set to facilitate the passing of data at provisioning time. For more information, see [https://cloud.google.com/compute/docs/storing-retrieving-metadata](https://cloud.google.com/compute/docs/storing-retrieving-metadata)

---

**IdleShutDown Agent Configuration**

*IdleShutDown Agent* is configured so that the remote workstation will shutdown when it is idle. For more information on installing and configuring this feature, see [Configuring Idle Shutdown](#).

---
Adding an Existing Remote Workstation

You can add an existing remote workstation you created within the Cloud Access Manager Admin Console, or one created in your cloud environment to a deployment. You can also view and add available resource groups if the remote workstation has valid cloud credentials. The remote workstation must have a PCoIP Agent installed on it and be visible to the Cloud Access Connector. You must have a valid Cloud Access Software registration code and the remote workstation, and user, must be part of the deployments active directory domain.

The following section outlines how to add an existing remote workstation to your deployment using the Cloud Access Manager Admin console:

1. Click **Workstations** from the console sidebar.
2. Click the Add Remote Workstation button and click **Add existing remote workstation** to display the Add a Remote Workstation panel.
3. Read the prerequisite information and ensure that you have met all the required needs to add a remote workstation.
4. Select an existing connector.
5. Select a provider for cloud services. If your remote workstation has Microsoft Azure credentials, you can view and select available resource groups from the resource groups tab.

6. Select your remote workstations.

7. Select and assign users.

8. Click **SAVE**.

The remote workstation should now appear on the remote workstations page.

You can stop, start, restart and delete multiple selected remote workstations by selecting the check-all box at the top of the page. This enables you to manage your remote workstations more efficiently.

---

**Remote Workstation machine name configuration**

Due to NetBIOS and a Windows limitation, the remote workstations machine name must be 15 characters or less. Failure to do this may result in issues with your remote workstation connection.
Editing a Remote Workstation

Once you have created a remote workstation within the Cloud Access Manager Admin Console you can manage and reconfigure it directly from the Remote Workstations page.

You can search for specific remote workstations by name by using the search bar in the table toolbar.

Entitling Users

Once you have create a remote workstation you can entitle users from the active directory account to specific remote workstation. The following section outlines how to entitle users:

1. Click the kebab option under the ACTIONS column to edit the desired remote workstation.
2. Click Edit.
3. Select the search bar and select the user you want to entitle:

   ![Manage User Entitlements for Workstation](image)

   - Click Add and then SAVE.

   The user you entitled will appear in the USER column on the Remote Workstations page for that particular remote workstation.
Updating Cloud Provider Information

Once you have created a remote workstation and assigned it cloud provider credentials, you can edit this information from within the Cloud Access Manager Admin Console. You can change the cloud provider for a specific remote workstation once you have valid cloud credentials for the provider.

Editing the cloud provider and zone information will not change the location of the remote workstation. This feature enables Cloud Access Manager to point to a different location to verify the remote workstation exists in the specified zone. If you do not have valid cloud credentials for a cloud provider you will not be able to change the remote workstation cloud provider.

When updating to Azure, your remote workstation must be in the specified subscription and resource group. The Azure deployment must have an Azure service principal that has access to remote workstations within the subscription and resource group.

The following section outlines how to update the cloud provider information:

1. Click the kebab option under the ACTIONS column to edit the desired remote workstation.
2. Click Edit.
3. From the Update Cloud Provider For Workstation tab select the cloud provider you wish to edit.
   - To change the provider in GCP, enter the zone that the remote workstation resides in.
   - To change the provider in Azure, enter the Subscription Id and Resource Group that the remote workstation belongs to.
4. Click SAVE.

If you have entered the correct zone for the remote workstation you will receive a notification that it has been updated. The new zone, cloud provider and information will be listed on this page also.
If you enter an incorrect zone then you will receive an error message stating that the remote workstation does not exist in the entered zone.

Deleting Remote Workstations from the Public Cloud

You can delete existing remote workstations from Azure and GCP from the Cloud Access Manager Admin Console. Only remote workstations that exist in Azure and/or GCP and that have valid cloud credentials can be deleted.

1. Click Workstations from the console sidebar to display your existing remote workstations.
2. Click the kebab option under the ACTIONS column.
3. Click Delete.
4. Click CONFIRM from the resulting pop-up message.

The process for deleting the remote workstation has now begun. It is also possible to bulk delete more than one remote workstation at a time by selecting multiple remote workstations to delete from the Cloud Access Manager Admin Console.

The remote workstation will disappear immediately from the Cloud Access Manager Admin Console and can take 5-10 minutes to be deleted from the CAM Service and public cloud. You should monitor the workstation in your cloud provider to ensure a successful completion. You will be notified in the Cloud Access Manager Admin Console on the whether the deletion was successfull or not.
You can view all available Workstation users in your active directory by selecting the **Workstation Users** page. You can search for specific users by name with the search field in the toolbar. You can obtain the following user information for specific users:

- User Name
- User GUID
- Deployment
- Directory status
- User Groups
- Date of creation

When you select a specific user you will be shown all user groups and entitled workstations associated with this user:

### ACTIVE DIRECTORY USER INFORMATION

<table>
<thead>
<tr>
<th>User Name</th>
<th>User GUID</th>
<th>Created On</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name-587-1561591856</td>
<td>1-587-1561591856</td>
<td>Aug 21, 2019 08:18 AM PDT</td>
</tr>
</tbody>
</table>

**GROUPS**

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owners:CN=Users,DC=example,DC=com</td>
</tr>
<tr>
<td>CN=Domain Admins, CN=Users, DC=example, DC=com</td>
</tr>
<tr>
<td>CN=Enterprise Admins, CN=Users, DC=example, DC=com</td>
</tr>
<tr>
<td>CN=Schema Admins, CN=Users, DC=example, DC=com</td>
</tr>
<tr>
<td>CN=Administrators, CN=BUILTIN, DC=example, DC=com</td>
</tr>
</tbody>
</table>

**ENTITLED WORKSTATIONS**

<table>
<thead>
<tr>
<th>Name</th>
<th>Power State</th>
<th>Assigned On</th>
</tr>
</thead>
<tbody>
<tr>
<td>workstation1</td>
<td>Running</td>
<td>Aug 24, 2019 05:36 PM PDT</td>
</tr>
<tr>
<td>workstation2</td>
<td>Running</td>
<td>Aug 14, 2019 05:36 PM PDT</td>
</tr>
</tbody>
</table>
This gives you an overview of a specific user's entitlements and deployment information and can be useful for troubleshooting issues.
Setting Date and Time Preferences

You can configure the time zone, time format and date format within the Cloud Access Manager Admin Console. This enables you to ensure the time zone is set to your local time zone or else to the time zone into which your remote workstations are deployed. The current date and time format provided by the web browser will be the default preference used.

The following steps outline how to set date and time preferences:

1. Click **Preferences** from the user account icon within the Cloud Access Manager Admin Console.
2. Select the desired Date format, Time zone and Time format.
3. Click **SAVE**.

The new date and time preferences will now be applied globally where applicable across the entire Cloud Access Manager Admin Console.
Cloud Access Connector for On-Premises, AWS, Microsoft Azure and Google Cloud

The Cloud Access Connector enables Cloud Access Manager to broker desktops or workstations located in AWS, Google Cloud, Microsoft Azure and on-premises environments.

The Cloud Access Connector is an access hub installed in the customer environment which facilitates PCoIP Client connections to remote workstations. The Cloud Access Connector operates in conjunction with the Teradici Cloud Access Manager Service to provide user authentication and entitlement for remote workstation access, including MFA. The Cloud Access Connector also eliminates the need for a dedicated VPN by providing NAT services for external users.
You are required to have a valid registration code for Teradici Cloud Access Software to be able to successfully deploy Cloud Access Manager. This code will be sent to you via email from Teradici and looks like ABCDEF1234@AB12-C345-D67E-89FG. For more information on Cloud Access Software, see Cloud Access Software.
Setting up the Cloud Access Connector Server

Cloud Access Connector is software that runs within an Ubuntu server and enables secure connectivity between users and the remote workstations. Cloud Access Connector runs in the customer environment such as on-premises, AWS and Google Cloud. The Connector communicates with the Cloud Access Manager Service (SaaS operated by Teradici) which orchestrates and manages Cloud Access deployments.

Creating the Cloud Access Connector Server

The Cloud Access Connector runs on an Ubuntu server (called the Cloud Access Connector server).

Create a dedicated Ubuntu server with the following specifications:

- Ubuntu Server 18.04
- 4GB RAM or higher
- 12GB available storage or higher
- 2 vCPUs or more

Dedicated instance types are required when using the Connector within a cloud service. Burstable instance types do not offer the consistent performance required for the Connector.

These environment conditions must be met:

- You must have access to the internet.
- You must have an Active Directory (AD) user account located in the designated Cloud Access Connector domain admins group, in order to log into the Management Interface of the Cloud Access Connector.
- The server must be able to resolve the AD domain.
- You must be able to access the server using SSH.
• You must have superuser (sudo) privileges on the server.
• The networking information of the server (including the IP address) must not change while the Cloud Access Connector is operational.
• The server must have a single network interface and IP address. If the server has multiple network interfaces, the Cloud Access Connector will fail to install.

For information on the session establishment and session bandwidth limits when working with external connections, see here.

---

**ESXi deployments need additional tools**

If you are deploying Ubuntu on ESXi, you must install `open-vm-tools` to enable the ESXi host to communicate with the Cloud Access Connector server.

---

**Creating a DNS record**

If you want to create a DNS record for the Cloud Access Connector, you need to obtain an SSL certificate with its FQDN and provide it (along with the key) when installing the Cloud Access Connector. This will avoid SSL certificate verification warnings.
Verifying the Cloud Access Connector Server

To verify your Cloud Access Connector server network configuration, SSH into the machine and ping the domain and a remote workstation in the domain. You should get a positive response from both attempts:

```
ping <domain FQDN>
ping <remote workstation FQDN>
```

If any of your attempts to verify these components fails, the DNS settings on the Cloud Access Connector server might be misconfigured. For more information on DNS configuration, see Configuring Network Settings in Ubuntu 18.04.
Enabling External Network Access

If the Cloud Access Connector server will be accessed outside the domain, it must be configured for external access (this step is only required if you want to enable remote access to the workstations without requiring a VPN):

- The server must have a public IP address. This can be done via bi-directional NAT mapping.
- The Cloud Access Connector will treat incoming connections from any private IP address range (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) as internal, and any other incoming connections as external.
- Port 443 TCP and 4172 UDP/TCP need to be open. Session set-up is done through port 443 and in-session traffic runs through port 4172.
- The \(--\text{external-pcoip-ip} \) sets the IPv4 address for the Cloud Access Connector for external connections. If this value is not set, the external IPv4 address will be determined automatically. This is an optional setting that can be used when installing the Cloud Access Connector.

For information on the session establishment and session bandwidth limits when working with external connections, see here.

Reboot the server after NAT changes

If the NAT is configured after the Cloud Access Connector has been installed, reboot the Cloud Access Connector server.
Multi-Factor Authentication

When you install the Cloud Access Connector you can specify whether the PCoIP session uses Multi-Factor Authentication (MFA) during authentication or not. The Cloud Access Connector can be integrated with your RADIUS server. To do this you will need to provide the following information during the Cloud Access Connector installation:

- The FQDN or IP address of the RADIUS server.
- The RADIUS server port. If this port is not specified the default port (1812) will be used.
- The shared secret used for configuring RADIUS authentication.

If you do not enable MFA when installing the Cloud Access Connector, you can enable it later when performing an update, see Updating the Cloud Access Connector. For more information on Cloud Access Connector MFA, see Multi-Factor Authentication.
Before installing the Cloud Access Connector you need to create and correctly configure the Active Directory Domain. You need to create an AD service account that has the following permissions to:

- Create Computer Objects
- Delete Computer Objects

The permissions on the Computer Objects must be set to:

- Read All Properties
- Write All Properties
- Read Permissions
- Modify Permissions
- Change Passwords
- Reset User Passwords
- Validated write to DNS host name
- Validated write to service principal name

For information on how to create and install a self-signed certificate on a Windows 2016 AD server to test LDAP connections, see KB 1707.

For information on creating these computer objects and configuring their associated parameters, see Service Account Permissions.

---

Domain Controller Certificates

If all DC certificates have expired, the Cloud Access Connector will stop working. An error indicator will display on the Connectors page when a Cloud Access Connector has a DC with expired certificates.

A warning indicator that details the current state of the DC certs will display on the same page when a Cloud Access Connector has a certificate that less than a week away from expiring.
Service Account Permissions

The following section outlines the steps to enable permissions to create and delete computer objects, permissions on these objects, and permissions to change and reset user credentials. These permissions are the minimum level of permissions required for a service account in a Cloud Access Manager deployment.

Permissions to Create and Delete Computer Objects

The following section outlines how to add permissions to create and delete computer objects through the OU permissions dialog:

1. Go to the security tab of the OU you want to give permissions to.
2. Right-click the relevant OU and click Properties.
3. Go to the security tab and click Advanced.
4. Click Add and browse to your user account. As stated above you need to add the user account to the OU.
5. Select This object and all descendant objects and select the following permissions:
   • Create Computer Objects
   • Delete Computer Objects
6. Click OK.

Permissions on the Computer Objects

The following section outlines how to select permissions on the computer objects through the OU permissions dialog:

1. Go to the security tab of the OU you want to give permissions to.
2. Right-click the relevant OU and click Properties.
3. Go to the security tab and click Advanced.

4. Click Add and browse to your user account. As stated above you need to add the user account to the OU.

5. Limit the Apply Onto scope to Descendant Computer objects and select the following settings:
   - Read All Properties
   - Write All Properties
   - Read Permissions
   - Modify Permissions
   - Validated write to DNS host name
   - Validated write to service principal name

6. Click OK.

DNS and service principal name permissions

The validated write to DNS host and service principal name permissions are required so that the DNS record for a remote workstation can be created after it is domain joined.

Permissions to Change and Reset User Passwords

The following section outlines how to select permissions to change and reset user passwords applicable to the desired user OU:

1. Go to the security tab of the OU you want to give permissions to.

2. Right-click the relevant OU and click Properties.

3. Go to the security tab and click Advanced.

4. Click Add and browse to your user account. As stated above you need to add the user account to the OU.

5. Select This object and all descendant objects and select the following permissions:
   - Change Password
   - Reset Password
6. Click **OK**

### Role-based access control with Active Directory

For more information on role-based access control with Active Directory accounts, see [Best Practices for Securing Active Directory](#).

## During Installation

When the Cloud Access Connector is installed, you will be prompted for the following information:

- The AD domain that the remote workstations should be joined to.
- The AD Service Account username.
- The AD Service Account password.
- AD user group for users that are permitted to log into the legacy Management Interface on the Cloud Access Connector.
Assigning a Certificate to the Cloud Access Connector

You can assign an SSL certificate to the Cloud Access Connector during installation. This will prevent certificate verification errors when connecting to the Cloud Access Manager Interface through your browser. It will also prevent the PCoIP client from reporting an insecure connection when establishing a PCoIP session.

The certificate you provide must be signed and validated by a root certificate that the client trusts. The certificate must be combined or bundled with the intermediate certificates in PEM format and copied, along with the key, to the Cloud Access Connector server prior to installation.

For an example of how to create a self-signed certificate, see Creating a self-signed certificate on a Windows 2016 Active Directory Server. For an example of a method to install a certificate on your Active Directory, see Installing a certificate on your Active Directory server to enable LDAPS.

The DNS needs to be setup so that ‘cam.test.com’ for example, is registered to the public IP address of the application gateway.

When the Cloud Access Connector is installed, you will be prompted for the following information:

- The full path and filename of the SSL key
- The full path and filename of the SSL certificate

If you do not wish to specify a certificate when installing the Cloud Access Connector, you can bypass this by entering the command line option `--self-signed` (which is recommended strictly for testing purposes). If you decide to use a certificate later, Teradici recommends creating a new Cloud Access Connector and deleting the old one. For information on updating SSL certificates, see Updating SSL Certificates.
Downloading the Cloud Access Connector

First, connect to the machine and download the Connector files. The commands below will create the required directory, download the Connector archive file, and extract the archive into it.

1. SSH into the machine:

   ```
   ssh <username>@<server-ip-address>
   ```

2. Download the component files from Teradici:

   ```
   mkdir ~/v2connector && cd ~/v2connector
curl -LO https://teradici.bintray.com/cloud-access-connector/cloud-access-connector-0.1.1.tar.gz
tar xzvf cloud-access-connector-0.1.1.tar.gz
   ```

---

*Copying commands*

If you copy and paste the above sequence into the console, the first two commands will execute immediately. Press [Enter] to execute the final command.
You are required to have a Connector token when installing the connector. You need to create or have created a deployment prior to obtaining a token. For information on how to log into the Cloud Access Manager Admin Console, see here. The following section outlines how to obtain a Cloud Access Connector token using the Admin console:

1. Click **Connectors** from the console sidebar.

2. Click the add connector button (+ sign located beside **Connectors** heading) to display the connector creation panel.

3. Enter the following information:
   - Select the deployment you want to add the Connector to. If you do not have an existing deployment you need to **create one**.
   - Enter the name of the Connector.
Follow the step by step instructions outlined below.

4. Click **GENERATE**.

5. Copy the Connector token by clicking the copy icon.

6. Click **CLOSE** to exit the panel.
You can now use this Connector token when prompted during installation.
Installing the Cloud Access Connector

Once the files are downloaded and the access token is set, you can install the Cloud Access Connector. If you are not already connected, connect to the machine via SSH and navigate to the `~/v2connector` directory.

**Latest Installer Version**

Ensure that you are using the latest installer prior to installing or upgrading the Cloud Access Connector.

Install the Cloud Access Connector by running the following command:

```
./cloud-access-connector install
```

Ensure that you use the options best suited to your system architecture and requirements. If required values are not provided on the command line, you will be prompted for them.

You need to obtain a Cloud Access Connector token prior to installation. For information on how to obtain this token, see [Obtaining a Cloud Access Connector Token](#). Once you have the token you can run the following command and enter it:

```
sudo ./cloud-access-connector install -t "token obtained in previous section" [options]
```

When installed with no options, the Connector will not use MFA, and will use your SSL key and certificate.

The available options are:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-t</code></td>
<td>Required. The token generated for Cloud Access Manager.</td>
</tr>
<tr>
<td><code>--enable-mfa</code></td>
<td>Installs with multi-factor authentication enabled.</td>
</tr>
</tbody>
</table>
The following flags can be used to provide values at the command line. If they are omitted from
the command and are required, you will be prompted for them:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--self-signed</td>
<td>String</td>
<td>Installs the Cloud Access Connector with self-signed certificates. This mode is not secure and is intended for testing. The --insecure flag is still supported.</td>
</tr>
<tr>
<td>--force-install</td>
<td></td>
<td>Replaces any existing Cloud Access Connector installation.</td>
</tr>
<tr>
<td>--debug</td>
<td></td>
<td>This flag can be run if you initial install of the Cloud Access Connector fails. It provides a detailed output of the Cloud Access Connector installation. This is useful for self-troubleshooting or to provide to the Teradici support team when logging a support ticket.</td>
</tr>
</tbody>
</table>

The following flags can be used to provide values at the command line. If they are omitted from the command and are required, you will be prompted for them:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--reg-code</td>
<td>String</td>
<td>Cloud Access Software registration code, provided by Teradici.</td>
</tr>
<tr>
<td>--domain</td>
<td>String</td>
<td>The AD domain that remote workstations will join.</td>
</tr>
<tr>
<td>--domain-group</td>
<td></td>
<td>The Distinguished Name of the user group you want to use to log into the legacy Cloud Access Manager management interface. This option can be used when you install a Cloud Access Connector or update an existing Cloud Access Connector. The default is Domain Admins (eg. CN=CAM Admins,CN=Users,DC=example,DC=com).</td>
</tr>
<tr>
<td>--sa-user</td>
<td>String</td>
<td>The Active Directory service account username.</td>
</tr>
<tr>
<td>--sa-password</td>
<td>String</td>
<td>The Active Directory service account password.</td>
</tr>
<tr>
<td>--radius-server</td>
<td></td>
<td>The FQDN or IP address of the RADIUS server to use for MFA. This flag is optional.</td>
</tr>
<tr>
<td>--radius-port</td>
<td>String</td>
<td>The RADIUS server port. If not specified, the default port (1812) is used. If --radius-server is specified then this flag is optional.</td>
</tr>
<tr>
<td>Flag</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>--radius-secret</td>
<td>String</td>
<td>The shared secret used for configuring RADIUS authentication. If --radius-server is specified then this flag is required.</td>
</tr>
<tr>
<td>--ssl-key</td>
<td>String</td>
<td>The full path and filename of the SSL key to use. The --self-signed flag overrides this flag.</td>
</tr>
<tr>
<td>--ssl-cert</td>
<td>String</td>
<td>The full path and filename of the SSL certificate (in PEM format) to use. The --self-signed flag overrides this flag.</td>
</tr>
<tr>
<td>--https-proxy</td>
<td>String</td>
<td>Specify the URL for a HTTPS proxy (overrides related proxy settings in environment variables)</td>
</tr>
<tr>
<td>--accept-policies</td>
<td>Boolean</td>
<td>Automatically accept the EULA and Privacy Policy.</td>
</tr>
<tr>
<td>--retrieve-agent-state</td>
<td>Boolean</td>
<td>Enables the broker to retrieve the agent state for unmanaged and managed remote workstations. The default value for this flag is false.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The available states are <em>In Session</em>, <em>Ready</em>, <em>Starting</em>, <em>Stopping</em>, <em>Stopped</em> and <em>Unknown</em>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The value of this flag can either be true or false.</td>
</tr>
<tr>
<td>--show-agent-state</td>
<td>Boolean</td>
<td>Controls if the agent state is displayed as part of the remote workstation name in the PCoIP Client. The default value for this flag is true.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Setting the value of this flag to true and the --retrieve-agent-state flag to false will result in no agent state displaying.</td>
</tr>
<tr>
<td>--domain-controller</td>
<td>String</td>
<td>Specifies one or more domain controllers to use with the Cloud Access Connector. For more information, see Specifying Domain Controllers.</td>
</tr>
<tr>
<td>--external-pcoip-ip</td>
<td>String</td>
<td>Sets the IPv4 address for the Cloud Access Connector for external connections. If this value is not set, the external IPv4 address will be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>determined automatically. For more information on external network access, see Enabling External Network Access.</td>
</tr>
</tbody>
</table>
Certificate Information

For an example of how to create a self-signed certificate, see Creating a self-signed certificate on a Windows 2016 Active Directory Server. For an example of a method to install a certificate on your Active Directory, see Installing a certificate on your Active Directory server to enable LDAPS.

Configuring User and Computer Active Directory Distinguished Names

The Cloud Access Connector can optionally be configured to use specific Distinguished Names (DNs) when querying Active Directory for users and computers has been extended to be available when running the `update` command in addition to the `install` command. The following is an example of the DN string format: `CN=CAM Admins,CN=Users,DC=example,DC=com`. You can also configure the frequency at which the Cloud Access Connector syncs this data with the CAM service, as outlined in the following table:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--users-dn</code></td>
<td>String</td>
<td>The base DN to search for users within Active Directory. This option may be specified multiple times to provide multiple DNs.</td>
</tr>
<tr>
<td><code>--computers-dn</code></td>
<td>String</td>
<td>The base DN to search for computers within Active Directory. This option may be specified multiple times to provide multiple DNs.</td>
</tr>
<tr>
<td><code>--sync-interval</code></td>
<td>String</td>
<td>The interval time in minutes for how often to sync Active Directory users and computers with the CAM service. It must be at least five minutes.</td>
</tr>
</tbody>
</table>

These flags outlined are optional and may be provided with the `install` or `update` commands. If you are updating a Cloud Access Connector you only need to provide these flags if you want to...
changing the DN settings associated with that Cloud Access Connector. If you do not add these flags when performing an update then the Cloud Access Connector will retain the same settings.

You can reset user or computer DNs to their default values by providing an explicit DN with a wider scope than the original DN used.

If you want to have multiple connectors with different Active Directory settings then you need to ensure that each Cloud Access Connector belongs to a separate deployment. If you create two Cloud Access Connectors that are associated with the same deployment then both will use the same Active Directory sync settings, and the configuration of the last Cloud Access Connector created will take precedence.

**Installing the Cloud Access Connector for Testing**

To install the Cloud Access Connector with MFA enabled and in insecure mode for testing, you would run this command (note that we are providing the `--enable-mfa` flag but not the RADIUS server information, so prompts will appear to collect it):

```
sudo ./cloud-access-connector install -t $token --enable-mfa --self-signed
```

When the installer completes, the IP address of the Cloud Access Connector will be displayed and you will be directed to go to [https://cam.teradici.com](https://cam.teradici.com) to begin managing your deployments, connectors and remote workstations.

**Cloud Access Connector - Troubleshooting**

If there is an issue installing the Cloud Access Connector or an existing Connector is failing, please see the troubleshooting section on Cloud Access Connector Connectivity. Within this section there are steps to check the following:

- Remote Workstation connections
- Active Directory connections
- Cloud Access Connector component information
Updating and Reconfiguring the Cloud Access Connector

To update a previously installed Cloud Access Connector to the latest versions, navigate to the `~/v2connector` directory and run the `cloud-access-connector update` command.

### Latest Installer Version

Ensure that you are using the latest installer prior to installing or upgrading the Cloud Access Connector. See [Installing a Cloud Access Connector](#).

### Update options

For a complete list of command flags and options, invoke `update` with `--help` to view the help file:

```
sudo ./cloud-access-connector update --help
```

The following table outlines the available update options that you can run when reconfiguring the Cloud Access Connector:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--enable-mfa</code></td>
<td>String</td>
<td>Enable MFA/2FA.</td>
</tr>
<tr>
<td><code>--radius-server</code></td>
<td>String</td>
<td>The FQDN or IP address of the RADIUS server to use for MFA. This flag is optional.</td>
</tr>
<tr>
<td><code>--radius-port</code></td>
<td>String</td>
<td>The RADIUS server port. If not specified, the default port (1812) is used. If <code>--radius-server</code> is specified then this flag is optional.</td>
</tr>
<tr>
<td><code>--radius-secret</code></td>
<td>String</td>
<td>The shared secret used for configuring RADIUS authentication. If <code>--radius-server</code> is specified then this flag is required.</td>
</tr>
<tr>
<td><code>--disable-mfa</code></td>
<td>String</td>
<td>Disable MFA/2FA (all RADIUS options are ignored if specified.</td>
</tr>
<tr>
<td>Flag</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>--domain-group</td>
<td>String</td>
<td>The DN for the AD domain group that manages users and remote workstations in the Management Interface.</td>
</tr>
<tr>
<td>--users-dn</td>
<td>StringArray</td>
<td>The base DN to search for users within AD. Specify multiple DNs with multiple options. Newly provided base DN(s) will automatically replace previous base DN(s).</td>
</tr>
<tr>
<td>--computers-dn</td>
<td>StringArray</td>
<td>The base DN to search for computers within AD. Specify multiple DNs with multiple options. Newly provided base DN(s) will automatically replace previous base DN(s).</td>
</tr>
<tr>
<td>--sync-interval</td>
<td>Unit8</td>
<td>The interval (in minutes) for how often to sync AD users and computers with the CAM Service.</td>
</tr>
<tr>
<td>--self-signed</td>
<td>String</td>
<td>Automatically generate self-signed SSL cert and key for testing purposes. If specified, --ssl-key and --ssl-cert options are ignored.</td>
</tr>
<tr>
<td>--ssl-key</td>
<td>String</td>
<td>The full path and filename of the SSL key to use with the CA connector gateway.</td>
</tr>
<tr>
<td>--ssl-cert</td>
<td>String</td>
<td>The full path and filename of the SSL certificate to use with the CA connector gateway.</td>
</tr>
<tr>
<td>--show-agent-state</td>
<td>Boolean</td>
<td>Show/hide PCoIP agent state (showing requires retrieve-agent-state to be true).</td>
</tr>
<tr>
<td>--retrieve-agent-state</td>
<td>Boolean</td>
<td>Enable/disable retrieving PCoIP agent state.</td>
</tr>
<tr>
<td>--domain-controller</td>
<td>StringArray</td>
<td>Specify a domain controller FQDN to use. May be specified multiple times for more than one DC.</td>
</tr>
<tr>
<td>--external-pcoip-ip</td>
<td>String</td>
<td>Sets the IPv4 address for the Cloud Access Connector for external connections. If this value is not set it will be determined automatically. An empty string will clear the setting, (i.e. --external-pcoip-ip &quot;).</td>
</tr>
</tbody>
</table>
Enabling MFA While Updating

You can enable MFA to the Cloud Access Connector with the `--enable-mfa` flag when performing an update. You need to have the following information:

- RADIUS server IP address or FQDN.
- RADIUS shared secret for configuring RADIUS authentication.

```
sudo ./cloud-access-connector update --enable-mfa
```

If you do not provide the locations of your RADIUS server and RADIUS shared secret, you will be prompted to do so.

Removing MFA While Updating

You can disable MFA from the Cloud Access Connector with the `--disable-mfa` flag when performing an update.

```
sudo ./cloud-access-connector update --disable-mfa
```

Updating SSL Certificates

Before updating SSL certificates, ensure that you aware of the requirments for creating and updating certificates, see Assigning a Certificate to the Cloud Access Connector. You can update your Cloud Access Connectors SSL certificate and key by running the following command and specifying your SSL certificate and SSL key information:

```
sudo ./cloud-access-connector update --ssl-cert path/to/cert --ssl-key path/to/key
```

Certificate format

The SSL certificate must be a PEM file. A CRT formatted file will not work with the update command above.
This command will enable you update your SSL certificate information without having to re-install the Cloud Access Connector. This command also enables you to change your self-signed certificate to a signed certificate.

### Domain Controller Certificates

If all DC certificates have expired, the Cloud Access Connector will stop working. An error indicator will display on the Connectors page when a Cloud Access Connector has a DC with expired certificates.

A warning indicator that details the current state of the DC certs will display on the same page when a Cloud Access Connector has a certificate that less than a week away from expiring.
Multi-Factor Authentication

Cloud Access Manager supports Multi-Factor Authentication (MFA) for PCoIP client sessions. The Cloud Access Manager MFA implementation is based on the RADIUS protocol. Customers can leverage their existing RADIUS server installation to enable MFA for Cloud Access Manager deployments. The following MFA scenario's have been tested with specific versions of the MFA software in question. Different versions may not yield the same results and may lead to different behavior.

Multi-Factor Authentication with Duo

Duo Authentication Version

The Cloud Access Connector was tested with Duo version 2.4.21.

In regards Duo authentication, the following information is configured in the authproxy.cfg file. When installing the Cloud Access Connector it will require the following information to configure the Duo Radius server:

• Radius Client IP (Cloud Access Connector IP)
• Radius Server Port
• Radius Shared Secret
• Duo authentication settings (ikey, skey and api host)

Multi-Factor Authentication PCoIP Client Support

Android PCoIP clients do not presently support RADIUS MFA.

For information on enabling Duo authentication with Cloud Access Manager, see Cloud Access Manager Duo MFA.

© 2019 Teradici
Multi-Factor Authentication with Azure

Microsoft Azure MFA Component Versions

Teradici tested the Cloud Access Connector with Microsoft Azure MFA on November 15th, 2019 with the following components.

Teradici component versions:

- PCoIP Software Client for Windows 19.11.
- Cloud Access Connector with MFA flag enabled.
- PCoIP Standard/graphics Agent 19.11.

3rd party component versions:

- Azure Active Directory Premium or Microsoft 365 Business offering to use Azure MFA.
- Network Policy Server (NPS) acting as the RADIUS server.
- NPS extension 1.0.1.32.
- Microsoft Authenticator App 1911.7724 (Android/iOS).

Using different versions may result in different behavior and has not been tested by Teradici.

Azure MFA can successfully be used as a 2nd factor tool for authenticating into the Cloud Access Connector. The following components are required to enable this MFA set-up:

- Azure Active Directory Premium or Microsoft 365 Business offering to use Azure MFA.
- Network Policy Server (NPS) acting as the RADIUS server.
- NPS extension 1.0.1.32 for Azure MFA sending requests from NPS to Azure MFA cloud service.
- Microsoft Authenticator App 1911.7724 (Android/iOS) to receive Push or to generate a Passcode.

Generated Passcode is not usable with Cloud Access Connector and Azure MFA

Only Microsoft Authenticator App Push Notification is supported due to Azure MFA using Modern Authentication. Selecting Send Me a Push or Submit Passcode triggers a push notification on your Microsoft Authenticator App. You will successfully connect to your PCoIP Session once you approve the push on your Android/iOS device.
For further information on configuring the required 3rd party components to enable Azure MFA with Cloud Access Connector, see Cloud Access Manager Azure MFA.
Assigning Permissions to Active Directory Service Accounts

The following section outlines the steps to enable permissions to create and delete computer objects, permissions on these objects, and permissions to change and reset user credentials. These permissions are the minimum level of permissions required for a service account when installing the Cloud Access Connector.

Permissions to Create and Delete Computer Objects

The following section outlines how to add permissions to create and delete computer objects through the OU permissions dialog:

1. Go to the security tab of the OU you want to give permissions to.
2. Right-click the relevant OU and click Properties.
3. Go to the security tab and click Advanced.
4. Click Add and browse to your user account. As stated above you need to add the user account to the OU.
5. Select This object and all descendant objects and select the following permissions:
   - Create Computer Objects
   - Delete Computer Objects
6. Click OK.
Permissions on the Computer Objects

The following section outlines how to select permissions on the computer objects through the OU permissions dialog:

1. Go to the security tab of the OU you want to give permissions to.
2. Right-click the relevant OU and click Properties.
3. Go to the security tab and click Advanced.
4. Click Add and browse to your user account. As stated above you need to add the user account to the OU.
5. Limit the Apply Onto scope to Descendant Computer objects and select the following settings:
   - Read All Properties
   - Write All Properties
   - Read Permissions
   - Modify Permissions
   - Validated write to DNS host name
   - Validated write to service principal name
6. Click OK.
Duo Authentication

If you wish to use Duo authentication with Cloud Access Manager you will be required to setup an authentication server provided by Duo. For more information on this, see Duo Authentication Proxy - Reference.

The Cloud Access Connector was tested with Duo version 2.4.21.

The following are key items in the authproxy.cfg file that are relevant for the Cloud Access Manager configuration:

```
[duo_only_client]
[radius_server_duo_only]
   ikey=<integration key for duo>
   skey=<secret key for duo>
   api_host=<host used for duo>
   radius_ip_1=<cac connection server ip>
   radius_secret_1=<shared secret for above>
   radius_ip_2=<cac connection server ip2>
   radius_secret_2=<shared secret for above>
   port=1812
```

For further information on the above integration, see RADIUS Duo Only.
Azure MFA Authentication

Microsoft Azure MFA Component Versions

Teradici tested the Cloud Access Connector with Microsoft Azure MFA on November 15th 2019 with the following components.

Teradici component versions:

- PCoIP Software Client for Windows 19.11.
- Cloud Access Connector with MFA flag enabled.
- PCoIP Standard/Graphics Agent 19.11.

3rd party component versions:

- Azure Active Directory Premium or Microsoft 365 Business offering to use Azure MFA.
- Network Policy Server (NPS) acting as the RADIUS server.
- NPS extension 1.0.1.32.
- Microsoft Authenticator App 1911.7724 (Android/iOS).

Using different versions may result in different behavior and has not been tested by Teradici.

Azure MFA Configuration

If you wish to use Azure MFA with the Cloud Access Connector you need to configure a number of 3rd party components. The following steps outline this process:

1. From within the Azure portal click Azure AD.
2. Click Enable MFA for target users.
3. Install the Microsoft Authenticator App on an Android or iOS mobile device.
4. Ensure that if the users requiring MFA are not yet populated in Azure AD, that you setup Azure AD Connect to sync On-Premises users to Azure.
6. Install Network Policy Server (NPS) extension for Azure MFA.
7. Register NPS to Active Directory to enable it to query the list of users.

© 2019 Teradici
Once you have registered the NPS you need to configure the server. The following steps outline the NPS configuration:

1. From within the NPS console click **RADIUS Clients**.
2. Add the Cloud Access Connector IP address and Shared Secret and click **OK**.
3. Click **Policies > Connection Request Policies** and add a new policy name and click **OK**.

4. From the **Conditions** tab add the Client IPv4 Address of the Cloud Access Connector and click **OK**.

5. From the **Settings** tab under **Authentication** click **Accept users without validating credentials**.

6. Restart NPS services to enable these changes to take effect.
Using the Cloud Access Connector with a Web Proxy

If web access is being blocked to the machines in your environment the Cloud Access Connector will not work. In order to give the Cloud Access Connector machine access to the required resources from the internet, a web proxy server is required. The web proxy server must support the HTTP Connect method and it must be enabled. Both HTTP and HTTPS traffic will be proxied through the same proxy server.

Using the Cloud Access Connector with a Web Proxy

The following steps outline how to use the Cloud Access Connector with a web proxy:

1. Set up a web proxy with access to the Internet, for example Squid.
2. Ensure that HTTP Connect is enabled on the web proxy. For Squid for example, the config file may look like this:

```
# Allowed Source IPs (ie, machines with 10.xxx.xxx.xxx IPs)
acl localnet src 10.0.0.0/8 # RFC1918 possible internal network

# Allowed ports to proxy traffic (Default)
acl SSL_ports port 443
acl Safe_ports port 80    # http
acl Safe_ports port 21    # ftp
acl Safe_ports port 443   # https
acl Safe_ports port 70    # gopher
acl Safe_ports port 210   # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280   # http-mgmt
acl Safe_ports port 488   # gss-http
acl Safe_ports port 591   # filemaker
acl Safe_ports port 777   # multiling http

# Enable HTTP Connect
acl CONNECT method CONNECT

# Default Squid http_access settings
# Deny requests to certain unsafe ports
http_access deny !Safe_ports
```

© 2019 Teradici
3. To test that the proxy is working correctly, using SSH, open a terminal on the Cloud Access Connector host machine and run the following set of commands:

```bash
# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports
# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 3128
# Leave coredumps in the first cache dir (Default)
coredump_dir /var/spool/squid
# Default Refresh patterns
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i /cgi-bin/|\? 0 0% 0
refresh_pattern (Release|Packages(.gz)*)$ 0 20% 2880
refresh_pattern . 0 20% 4320
```

Running curl to cam should time out since the host should not be able to route to the internet

```bash
$ curl cam.teradici.com
curl: (7) Failed to connect to cam.teradici.com port 80: Connection timed out
$ curl https://cam.teradici.com
curl: (7) Failed to connect to cam.teradici.com port 443: Connection timed out
```

Setting the proxy settings in the environment for curl to test that it works for HTTP and HTTPS traffic

```bash
$ export http_proxy=http://<ip-of-proxy-server>:<proxy-port (default 3128)>
$ curl cam.teradici.com
<html>
<head><title>308 Permanent Redirect</title></head>
<body bgcolor="white">
<center><h1>308 Permanent Redirect</h1></center>
<hr><center>nginx</center>
```
4. To run the installer with the proxy settings, you can apply them in the environment:

   ```
   # Installer will read proxy setting from environment if http_proxy, https_proxy, HTTP_PROXY, or HTTPS_PROXY are set
   $ export https_proxy=http://<ip-of-proxy-server>:<proxy-port (default 3128)>
   $ ./cloud-access-connector install ...
   ```

   or through the command line option:

   ```
   $ ./cloud-access-connector install --https-proxy http://<ip-of-proxy-server>:<proxy-port (default 3128)>
   ```

5. The installer should run as normal and configure the containers with the web proxy settings provided.

   ```
   Proxy Passwords are not Supported
   ```
   Proxy passwords are not supported with the Cloud Access Connector at this time.
Specifying Domain Controllers

You can optionally specify one or more domain controllers to use with the Cloud Access Connector by providing the `--domain-controller` option with the `install` or `update` commands. The following is an example of how this command might look (other required options excluded):

```
sudo ./cloud-access-connector install --domain-controller dc1.domain.com [--domain-controller dc2.domain.com]
```

Multiple domain controllers can be specified by providing multiple `--domain-controller` options. If you explicitly provide domain controllers the Cloud Access Connector will only use these domain controllers when authenticating or syncing users and computer information to the CAM service, regardless of whether other domain controllers are available.

---

**FQDN Specification**

The domain controller you provide must be specified as an FQDN, and not an IP address.
Cloud Service Account Requirements

Cloud Access Manager’s capabilities are enhanced if you provide service account credentials for your specific cloud environment. This section describes which capabilities are enabled by providing service account access, and what levels of access are required to restrict accounts.

Service Account Permission Requirements - Google Cloud Platform

You need a service account that has adequate permissions and can manage compute instances to provision a remote workstation in Google Cloud Platform (GCP) with Cloud Access Manager.

The table below outlines the default roles that are required for the service account on GCP, and which features they are required for.

**Default Roles and Feature Requirements - GCP**

<table>
<thead>
<tr>
<th>Default Roles</th>
<th>Workstation Provisioning</th>
<th>Power Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment Manager Editor</td>
<td>Required</td>
<td>-</td>
</tr>
<tr>
<td>Compute Admin</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Cloud KMS Admin</td>
<td>Required</td>
<td>-</td>
</tr>
<tr>
<td>Cloud KMS CryptoKey Encrypter/Decrypter</td>
<td>Required</td>
<td>-</td>
</tr>
</tbody>
</table>

For GCP the service account requires access to the following APIs:

- Service Usage API
- Cloud Resource Manager API
- Cloud Deployment Manager V2 API
- Cloud Key Management Service (KMS)
- Compute Engine API
The following links have more information on GCP service accounts:

- GCP - Getting Started
- GCP - Access Information
- Managing Service Account Keys
- Enabling GCP API for Projects

Service Account Permission Requirements - Microsoft Azure

You need a service account that has adequate permissions and can manage compute instances to power manage a remote workstation in Microsoft Azure with Cloud Access Manager. The following roles are required:

- Reader
- Virtual Machine Contributor

For information on how to create a new Client Secret from Azure, see here.

Azure Client Secret

Once you generate the client secret you need to copy it straight away as it will not be available again from Microsoft. If you have an expired client secret you need to delete it and then create a new secret and assign it to that deployment.
Providing Service Account Credentials

Service account credentials can be provided as part of the Cloud Access Manager deployment. These credentials can be manually entered, or for GCP deployments a key file can be provided that can be used to populate the fields. For more information on creating a deployment, see Creating a Deployment.

The table below outlines the features supported by the different Cloud Access Connector versions, and the cloud providers that work with the Cloud Access Manager Service.

### Cloud Access Manager Features enabled by Cloud Service Accounts

<table>
<thead>
<tr>
<th>Feature</th>
<th>Azure (CACv1)</th>
<th>Azure</th>
<th>GCP</th>
<th>AWS</th>
<th>ESX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deallocation*</td>
<td>Supported</td>
<td>Supported</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Power Management</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Workstation Provisioning</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
</tbody>
</table>

*Deallocation is a power state within Microsoft Azure. When a remote workstation is powered off by a user, it will be shutdown and the account will still be billed. Cloud Access Manager can deallocate remote workstations that have been shutdown in order to stop them being billed.*
Installing and Configuring Cloud Access Manager Idle Shutdown

The following section outlines how to install and configure idle shutdown on remote workstations not provisioned by Cloud Access Manager on Windows and Linux.

Any remote workstations provisioned by Cloud Access Manager will have this feature installed and configured by default. If idle shutdown has been installed and configured on remote workstations that were not provisioned by Cloud Access Manager and are not managed by Cloud Access Manager, then the administrator may be required to log into their cloud environment to reboot these remote workstations whenever the idle shutdown powers them off.

This setting may not suit all customers' needs and can be customized to suit.

---

**Service Account and Access Prerequisites**

Powering the remote workstation on or off from the Cloud Access Manager at session start, or from the web interface, requires that the remote workstation exists in a cloud environment with appropriate service account credentials that supports power management with Cloud Access Manager.

---

### Installing on Windows

After installing the PCoIP Agent, run the following commands in PowerShell:

```powershell
$idleTimerRegKeyValue = <idle-time-in-minutes>
$enableAutoShutdown = <$true-or-$false>

# Detect agent type
$is64 = $false
$serviceName = "CAMIdleShutdown"
$path = "C:\Program Files (x86)\Teradici\PCoIP Agent\bin"
if (!((Test-Path -path $path)) {  
  $path = "C:\Program Files\Teradici\PCoIP Agent\bin"
  $is64 = $true
}
  cd $path
```

© 2019 Teradici
# Install Service

```
$ret = .\IdleShutdownAgent.exe -install
```

# Check for success

```
if ( ! $? ) {
    $msg = "Failed to install {0} because: {1}" -f $serviceName, $ret
    Write-Host $msg
    throw $msg
}
```

# Configure Service

```
$idleTimerRegKeyPath = "HKLM:SOFTWARE\WOW6432Node\Teradici\CAMShutdownIdleMachineAgent"
if ( $is64 ) {
    $idleTimerRegKeyPath = "HKLM:SOFTWARE\Teradici\CAMShutdownIdleMachineAgent"
}
$idleTimerRegKeyName = "MinutesIdleBeforeShutdown"
if ( !(Test-Path $idleTimerRegKeyPath) ) {
    New-Item -Path $idleTimerRegKeyPath -Force
}
New-ItemProperty -Path $idleTimerRegKeyPath -Name $idleTimerRegKeyName -Value $idleTimerRegKeyValue -PropertyType DWORD -Force
```

# Disable service if desired

```
$svc = Get-Service -Name $serviceName
if ( !$enableAutoShutdown ) {
    $msg = "Attempting to disable {0} service" -f $serviceName
    Write-Host $msg
    try {
        if ( ($svc.Status -ne "Stopped") ) {
            Start-Sleep -s 15
            $svc.Stop()
            $svc.WaitForStatus("Stopped", 180)
        }
        Set-Service -InputObject $svc -StartupType "Disabled"
        $status = if ( $? ) { "succeeded" } else { "failed" }
        $msg = "Disabling {0} service {1}" -f $svc.ServiceName, $status
        Write-Host $msg
    }
    catch {
        throw "Failed to disable CAMIdleShutdown service."
    }
}
```
Configuring on Windows

For the PCoIP Agent for Windows the settings must be retrieved from the registry. The following steps outline how to configure these settings for Windows:

- For PCoIP Agent versions 2.15 and earlier, the settings are stored in:
  HKLM\SOFTWARE\WOW6432Node\Teradici\CAMShutdownIdleMachineAgent
- PCoIP Agent version 19.05 and later, the settings are stored in:
  HKLM\SOFTWARE\Teradici\CAMShutdownIdleMachineAgent

The table below outlines the settings and defaults:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DWORD</td>
<td>PollingIntervalMinutes</td>
<td>15</td>
<td>Polling interval in minutes for checking the CPU utilization. Must be between 1 and 60.</td>
</tr>
<tr>
<td>DWORD</td>
<td>MinutesIdleBeforeShutdown</td>
<td>240</td>
<td>Number of minutes the machine must be considered idle before it can be shutdown. The timer starts only when all active users have disconnected (or logged off), and is reset if any user connects. Must be between 5 and 10000.</td>
</tr>
<tr>
<td>DWORD</td>
<td>CPUUtilizationLimit</td>
<td>20%</td>
<td>Value between 0 and 100 representing CPU utilization percentage. If CPU utilization is below this value the machine is considered idle and will shutdown if maintained for MinutesIdleBeforeShutdown.</td>
</tr>
<tr>
<td>DWORD</td>
<td>EnableCAMDebug</td>
<td>0</td>
<td>Additional debugging messages to the event log when this value is non-zero.</td>
</tr>
</tbody>
</table>

1. After installation the service will be enabled by default. To enable or disable the service explicitly, run:

   Set-Service CAMIdleShutdown -StartupType "Automatic"
or

Set-Service CAMIdleShutdown -StartupType "Disabled"

2. **MinutesIdleBeforeShutdown** can be configured through the Microsoft Azure ARM provisioning template as the **autoShutdownIdleTime** setting in the parameters file. Once the **autoShutdownIdleTime** setting is installed on a remote workstation, you can configure the setting by pushing the desired registry key settings directly to the specific remote workstation.

**Installing on Linux**

After installing the PCoIP Agent, run the following commands in the command line:

```bash
AUTO_SHUTDOWN_IDLE_TIMER=<Desired-Idle-Time>
ENABLE_AUTO_SHUTDOWN=<true-or-false>
mkdir /tmp/idleShutdown
awk '{ sub("\r$", ""); print }' /tmp/idleShutdown/Install-Idle-Shutdown-raw.sh > /tmp/idleShutdown/Install-Idle-Shutdown.sh && sudo chmod +x /tmp/idleShutdown/Install-Idle-Shutdown.sh
INSTALL_OPTS="--idle-timer ${AUTO_SHUTDOWN_IDLE_TIMER}"
if [ [ "$ENABLE_AUTO_SHUTDOWN" = "false" ] ]; then
  INSTALL_OPTS="${INSTALL_OPTS} --disabled"
fi
sudo /tmp/idleShutdown/Install-Idle-Shutdown.sh "${INSTALL_OPTS}"
```

**Configuring on Linux**

For the PCoIP Agent for Linux, the idle shutdown is configured through a system service and can be configured through the accompanying service and timer .conf and files.

The table below outlines the settings and defaults:
To apply any changes, you need to run the following command:

```bash
systemctl daemon-reload
```

After installation the service will be enabled by default. To enable or disable the service explicitly, run:

```bash
systemctl enable CAMIdleShutdown.timer
systemctl start CAMIdleShutdown.service
systemctl start CAMIdleShutdown.timer

or

systemctl stop CAMIdleShutdown.service
systemctl stop CAMIdleShutdown.timer
systemctl disable CAMIdleShutdown.timer
```

<table>
<thead>
<tr>
<th>Location</th>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/etc/systemd/system/CAMIdleShutdown.service.d/CAMIdleShutdown.conf</code></td>
<td><code>MinutesIdleBeforeShutdown</code></td>
<td>240 minutes</td>
<td>Number of minutes the machine must be considered idle before it can be shutdown. The timer starts only when all active users have disconnected (or logged off), and is reset if any user connects. NOTE: This includes SSH sessions.</td>
</tr>
<tr>
<td><code>/etc/systemd/system/CAMIdleShutdown.service.d/CAMIdleShutdown.conf</code></td>
<td><code>CPUUtilizationLimit</code></td>
<td>20%</td>
<td>Value between 0 and 100 representing CPU utilization percentage. If average CPU utilization is below this value the machine is considered idle and will shutdown if maintained for <code>MinutesIdleBeforeShutdown</code>.</td>
</tr>
<tr>
<td><code>/etc/systemd/system/CAMIdleShutdown.timer.d/CAMIdleShutdown.conf</code></td>
<td><code>OnUnitActiveSec</code></td>
<td>15 minutes</td>
<td>Polling interval in minutes for checking the CPU utilization.</td>
</tr>
</tbody>
</table>
3. *MinutesIdleBeforeShutdown* can be configured through the Microsoft Azure ARM provisioning template as the *autoShutdownIdleTime* setting in the parameters file. Once the *autoShutdownIdleTime* setting is installed on a remote workstation, you can configure the setting by pushing the desired registry key settings directly to the specific remote workstation.
Microsoft Azure Active Directory Authentication

The Cloud Access Manager Admin Console supports Microsoft Azure Active Directory for authentication. All users with a work or school account from Microsoft can sign in to the Cloud Access Manager Admin Console using Azure Active Directory. A work or school account is an account created by an organization's administrator to enable a member of the organization to access Microsoft cloud services, such as Microsoft Azure or Office 365. This account can take the form of a user's organizational email address, such as username@orgname.com for example.

Please check with your organization's administrator to see if you can set up a work or school account. For more information about configuring your organization to use Microsoft's cloud services, view the documentation here: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/sign-up-organization.
The Cloud Access Manager Privacy Statement details information around the collection, use, processing and disclosure of personal information and other information in connection with the Cloud Access Manager service. The statement outlines the information we collect, how and when it is used, as well as other privacy and security information. For privacy information on Teradici's other services and activities, see Teradici Privacy Policy.
Cloud Access Manager Deployment Scripts

Teradici has an open github repository that contains a collection of scripts that simplify the setup, installation and usage of Cloud Access Manager. This repository enables users to set-up the necessary cloud resources (networking, firewalls, NAT gateway, storage buckets, etc.), as well as Domain Controllers, Cloud Access Connectors and remote workstations from scratch to produce a working environment.

⚠️ **Infrastructure Limitations**

The scripts in this repository are suitable for creating reference deployment for demonstration, evaluation or development purposes. The infrastructure created may not meet the reliability, availability or security requirements of your organization.

The tools in this repository are provided as-is, with no expectation of support. Users are encouraged to clone, modify and to submit bug reports in github.

The repository which contains scripts for deploying Cloud Access Connectors is available at https://github.com/teradici/cloud_deployment_scripts.
Scaling and PCoIP Session Limits

When using Cloud Access Manager there are certain session establishment and session bandwidth limits when dealing with external connections.

The following table outlines the RAM, vCPU and correlated estimated bandwidth support:

<table>
<thead>
<tr>
<th>vCPUs</th>
<th>RAM</th>
<th>Estimated Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>2vCPU</td>
<td>7.5 GB RAM</td>
<td>~ 300 Mbit/s</td>
</tr>
<tr>
<td>4vCPU</td>
<td>15 GB RAM</td>
<td>~ 340 Mbit/s</td>
</tr>
<tr>
<td>8vCPU</td>
<td>30 GB RAM</td>
<td>~ 480 Mbit/s</td>
</tr>
</tbody>
</table>

**Estimated Bandwidth**

These are estimated bandwidth levels. The bandwidth can vary based on the host, OS, CSP, etc.

480 Mbit/s is approximately the maximum bandwidth that can be achieved. If you attempt to size larger then this figure then you may only see minimal, if any, further increases to bandwidth.
Getting Support

If you are having trouble, help is available. This section contains information about contacting Teradici support and connecting with the Teradici user community.

Contacting Support

If you encounter problems installing or using Teradici technology, you can:

- Check for updated release notes, which may address the issue you are experiencing. Release notes are published on Teradici Support.
- Browse the Teradici Knowledge Base.
- Submit a Support ticket.

The Teradici Community Forum

The PCoIP Community Forum allows users to have conversations with other IT professionals to learn how they resolved issues, find answers to common questions, have peer group discussions on various topics, and access the Teradici PCoIP Technical Support Service team. Teradici staff are heavily involved in the forums.

To join the Teradici community, visit the Teradici Community Forum.
Getting Your Registration Code

You need a registration code to activate your PCoIP agent and to use it in conjunction with Teradici Cloud Access Manager. Once you subscribe to a Cloud Access Software subscription your registration code will be in an email sent to you from Teradici. If you are an existing customer and have a subscription but have lost your registration code, then you need to submit a ticket with support.

If you do not have a subscription with Teradici then you need to contact sales to find out about our subscriptions, components and solutions.
Cloud Access Manager Service Status

Teradici provides service status at the following site: Cloud Access Manager Service Status. From this site it is possible to view the current status of the Cloud Access Manager Service API's, as well as all recent and upcoming updates.

From this site you can subscribe to be notified via email about upcoming updates. These updates may affect the performance and functionality of the Service API's which will affect your use of the Cloud Access Manager service. To subscribe click on the Subscribe to Updates button at the top right of the screen and enter the email address you wish to be notified on.

An email will be sent to you shortly afterwards indicating that you have successfully subscribed to these updates.
Cloud Access Manager provides some diagnostic checks that can be used to troubleshoot the cause of issues you may be experiencing with your Cloud Access Connector. The command is `. / cloud-access-connector diagnose`. This command can also be used to verify that your Cloud Access Connector has been correctly configured. The diagnostic checks cover Remote Workstation connectivity and Active Directory connectivity.

The following table lists the flags associated with this command:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--rw</td>
<td>The Remote Workstation FQDN</td>
</tr>
<tr>
<td>--ad</td>
<td>Verify connectivity to currently configured Active Directory server</td>
</tr>
<tr>
<td>-h --help</td>
<td>help for diagnose</td>
</tr>
<tr>
<td>-h --debug</td>
<td>This flag can be run if you initial install of the Cloud Access Connector fails. It provides a detailed output of the Cloud Access Connector installation. This is useful for self-troubleshooting or to provide to the Teradici support team when logging a support ticket.</td>
</tr>
</tbody>
</table>

### Common Installation Issues with the Cloud Access Connector

For information on issues relating to failed Cloud Access Connector installations, Teradici has a KB article that details troubleshooting steps for common issues related to installing the Cloud Access Connector, see [here](#).

### Remote Workstation Connectivity Check

This command will attempt to connect to the specified remote workstation on the ports required for establishing a PCoIP session. It checks to ensure that the PCoIP agent is running on the remote workstation.

Example command to diagnose remote workstation connectivity issues:
Check Passes

- Your Cloud Access Connector is able to resolve the FQDN of the remote workstation and connect to it.
- The PCoIP agent is running and responding on the remote workstation.

Check Fails

If the check fails it may be as a result of one or more of the following issues:

- Firewall or network routing rules or restrictions may be in place.
- A failure has occurred and the FQDN of the remote workstation cannot be resolved.
- The PCoIP agent on the remote workstation is not running or is unresponsive.

Active Directory Connectivity Check

This command will attempt to connect to the Active Directory domain controller that was provided during installation using those same credentials.

Example command to diagnose Active Directory connectivity issues:

```
sudo ./cloud-access-connector diagnose --ad
```

Check Passes

- The Cloud Access Connector is able to resolve the FQDN of the domain controller and authenticate to it.

Check Fails

If the check fails it may be as a result of one or more of the following issues:

- Firewall or network routing rules or restrictions may be in place.
- A failure has occurred and the FQDN of the domain controller cannot be resolved.
- The Active Directory server may be unresponsive.
• The check was unable to authenticate to the Active Directory server.
Retrieving Logs from the Cloud Access Connector

The following section outlines how to retrieve the logs and view the status of the Cloud Access Connector services and installer. This information can help troubleshoot issues relating to the Cloud Access Connector.

To view the status of all services in the Cloud Access Connector run the following command:

```
sudo docker service ls
```

To get logs from services run the following command:

```
sudo docker service logs [service]
```

The following list details the important services:

- `connector.activedirectorysync`
- `connector.brokerexternal`
- `connector.brokerinternal`
- `connector.cm`
- `connector.cmsg`
- `connector.connectorgateway`
- `connector.healthcheck`
- `connector.managementinterface`
- `connector.sumologic`

The log files for the installer are located in `/var/log/cloud-access-connector/`. 
Cloud Access Connector and Cloud Access Manager Service

For information on new updates and enhancements around the Cloud Access Connector, as well as issues that have been resolved, go to the following release note page:

- Cloud Access Connector