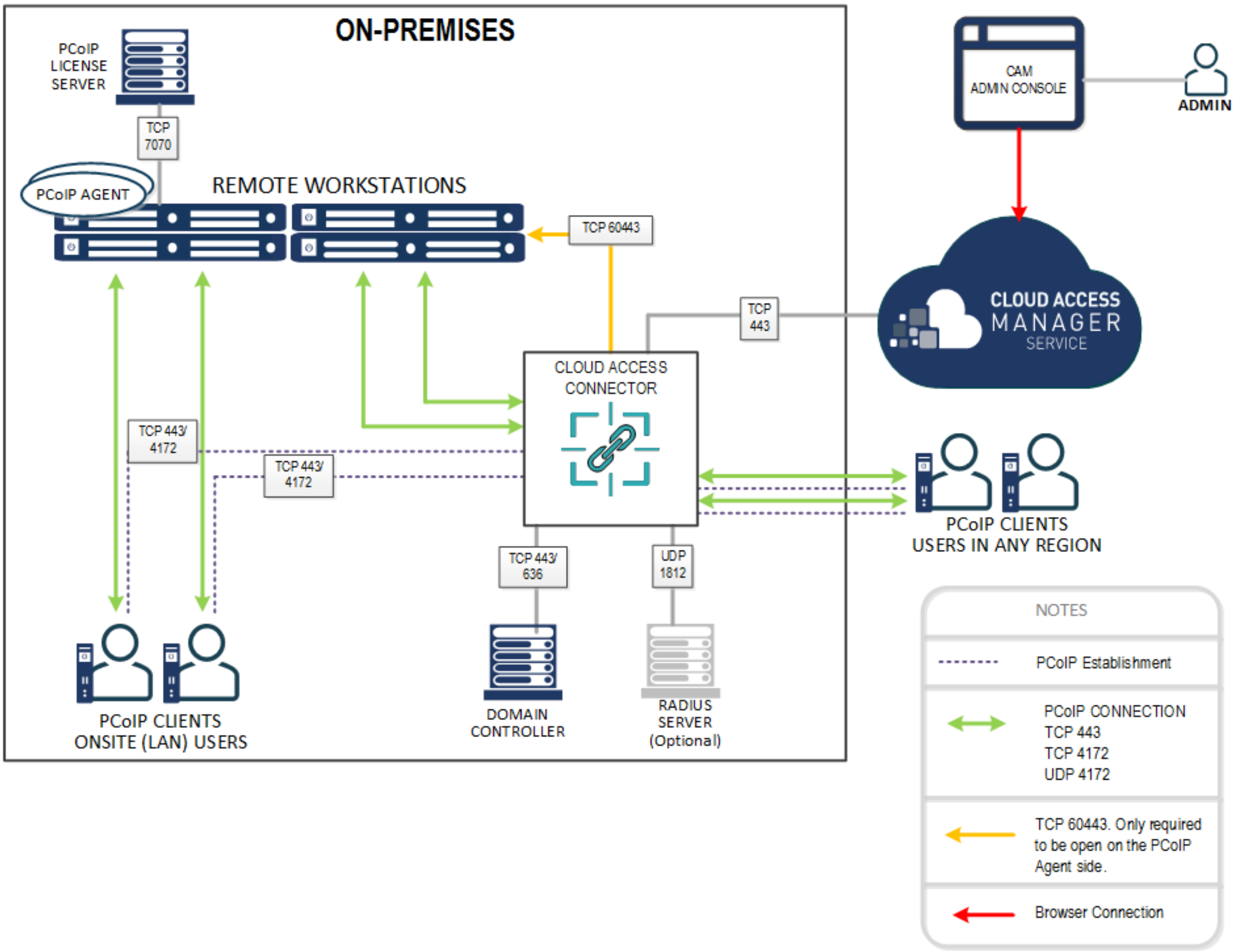
Cloud Access Manager

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

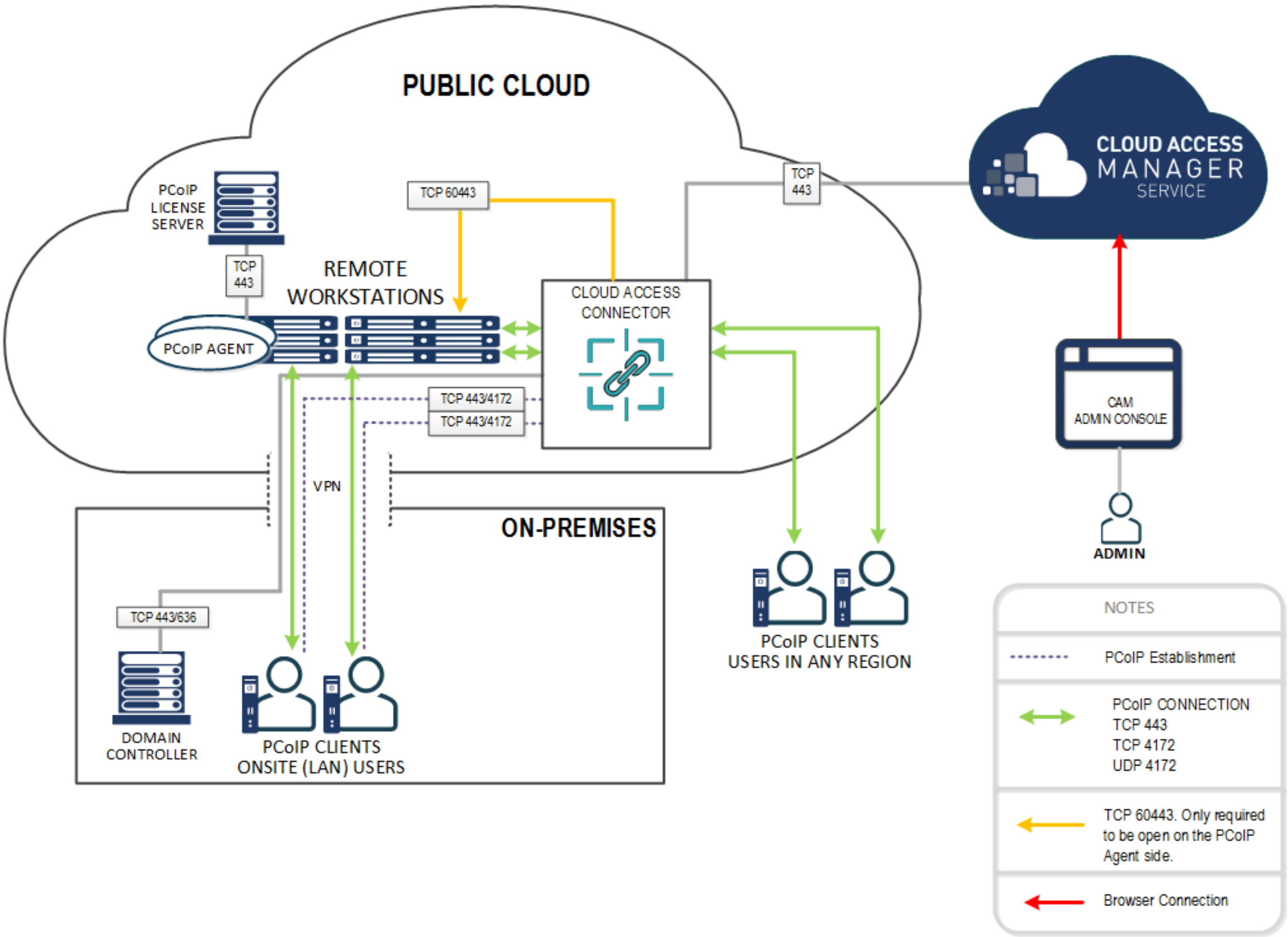
What is Cloud Access Manager?

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.

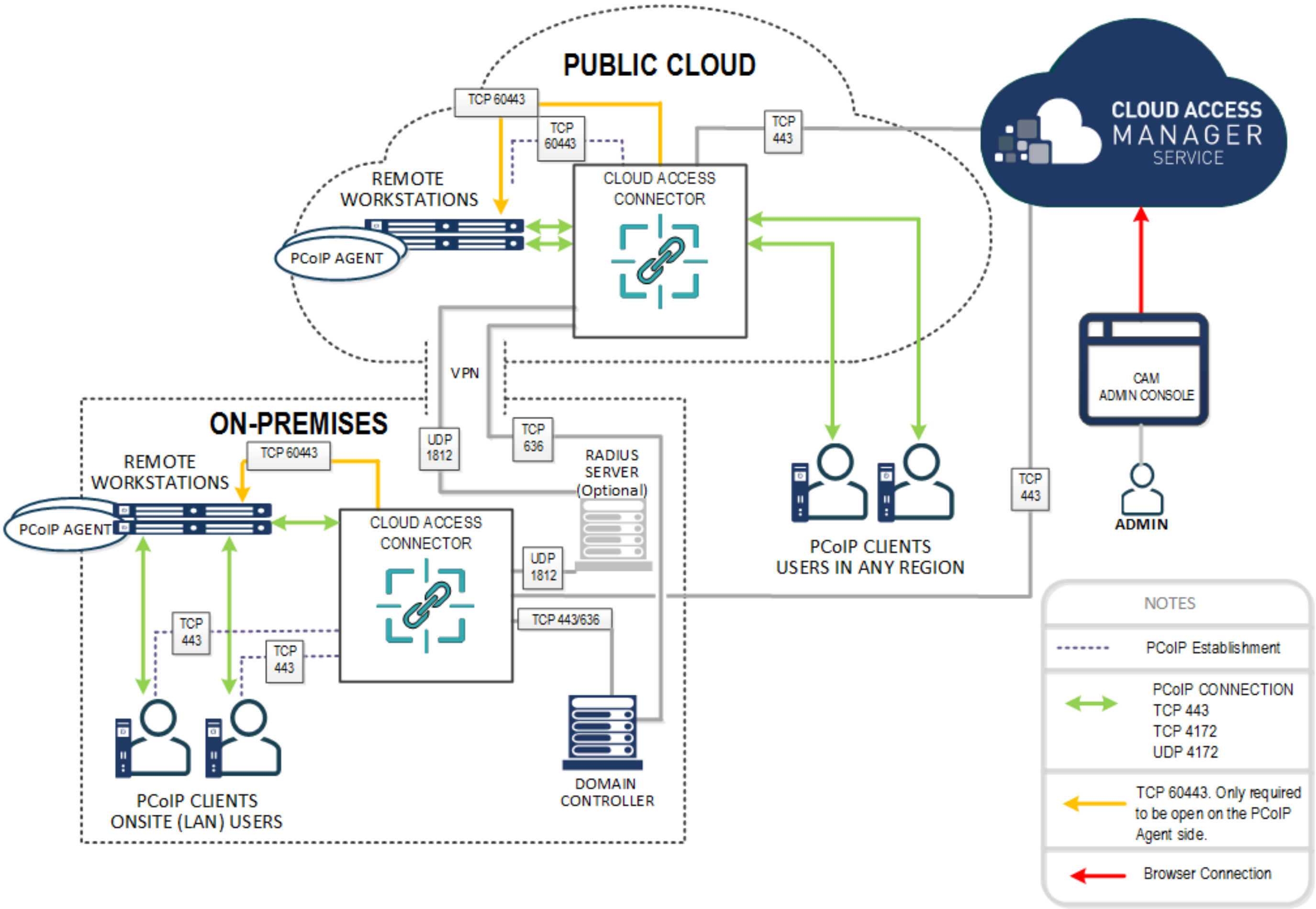
The following image outlines the Cloud Access Manager architecture for an on-premises scenario:



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.

Cloud Access Manager and Cloud Access Connector Ports

For a more detailed breakdown of the ports and connection descriptions, see Firewall and Load Balancing Considerations.

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. Each deployment may only have a single AD configuration. For more information on AD configuration with Cloud Access Manager, see here.

- 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. You cannot configure multiple Cloud Access Connector's in the same deployment to different ADs or with different AD configurations. 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 Connector 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/.

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.
- ***At least*** 4GB RAM.
- 20GB 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.

- Windows 2019 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.architve.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.

- docker.cloudsmith.io

  This is used by the installer to download docker containers used by the Cloud Access Connector that are developed and maintained by Teradici.

- dl.teradici.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:

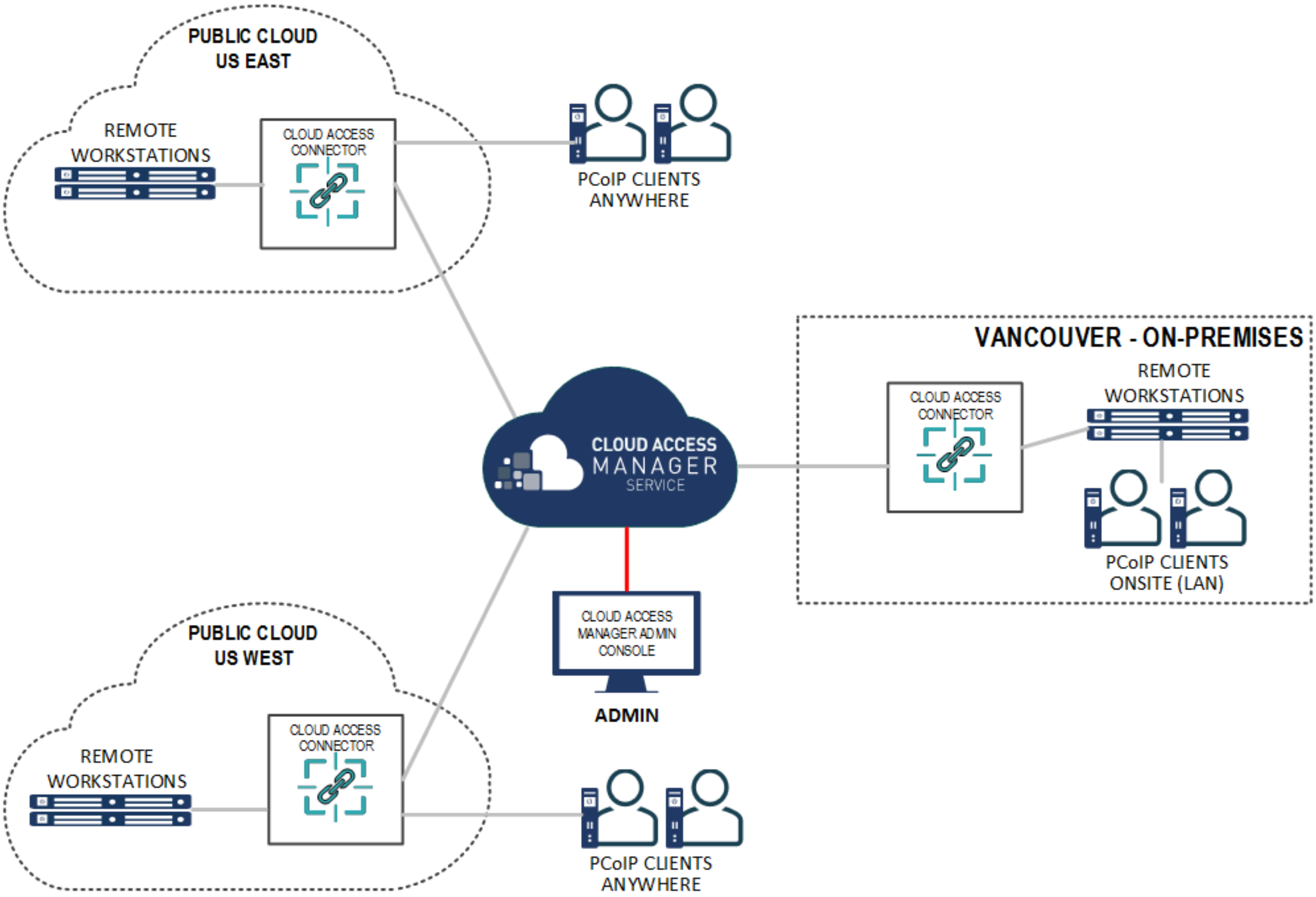
- *teradici.compliance.flexnetoperations.com*: This domain is used by the installer for licensing and validating the registration code. It is the operations website for Flexera.
- *akamai.bintray.com*: This is a Teradici docker container repo.
- *registry-1.docker.io*: This is a public docker repo.
-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

Whitlisting IP Addresses

If you are still having issues with installation after whitelising 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.

Overview

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

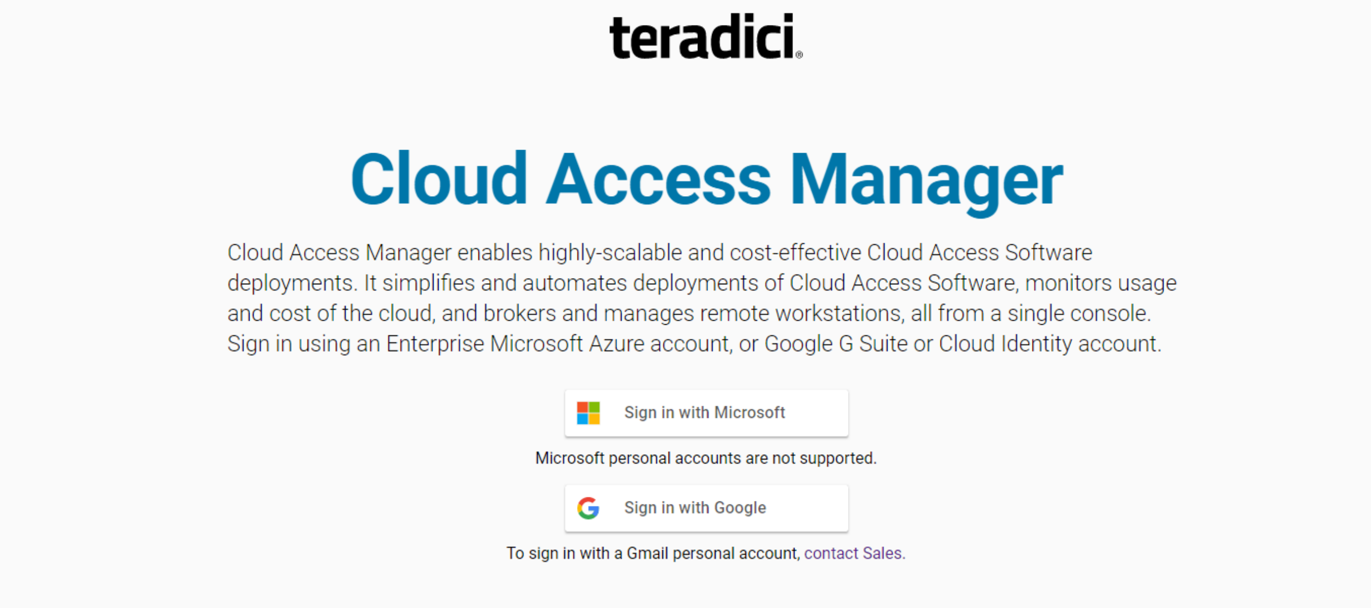
Go to the Cloud Access Manager Admin Console https://cam.teradici.com/ login page and log in with your Enterprise Microsoft Azure account, or if you are logging in through Google, a G Suite or Cloud Identity account. Enter your credentials to access the Admin Console.

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.



teradici

Cloud Access Manager

Cloud Access Manager enables highly-scalable and cost-effective Cloud Access Software deployments. It simplifies and automates deployments of Cloud Access Software, monitors usage and cost of the cloud, and brokers and manages remote workstations, all from a single console. Sign in using an Enterprise Microsoft Azure account, or Google G Suite or Cloud Identity account.

Microsoft personal accounts are not supported.

To sign in with a Gmail personal account, contact Sales.

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/.

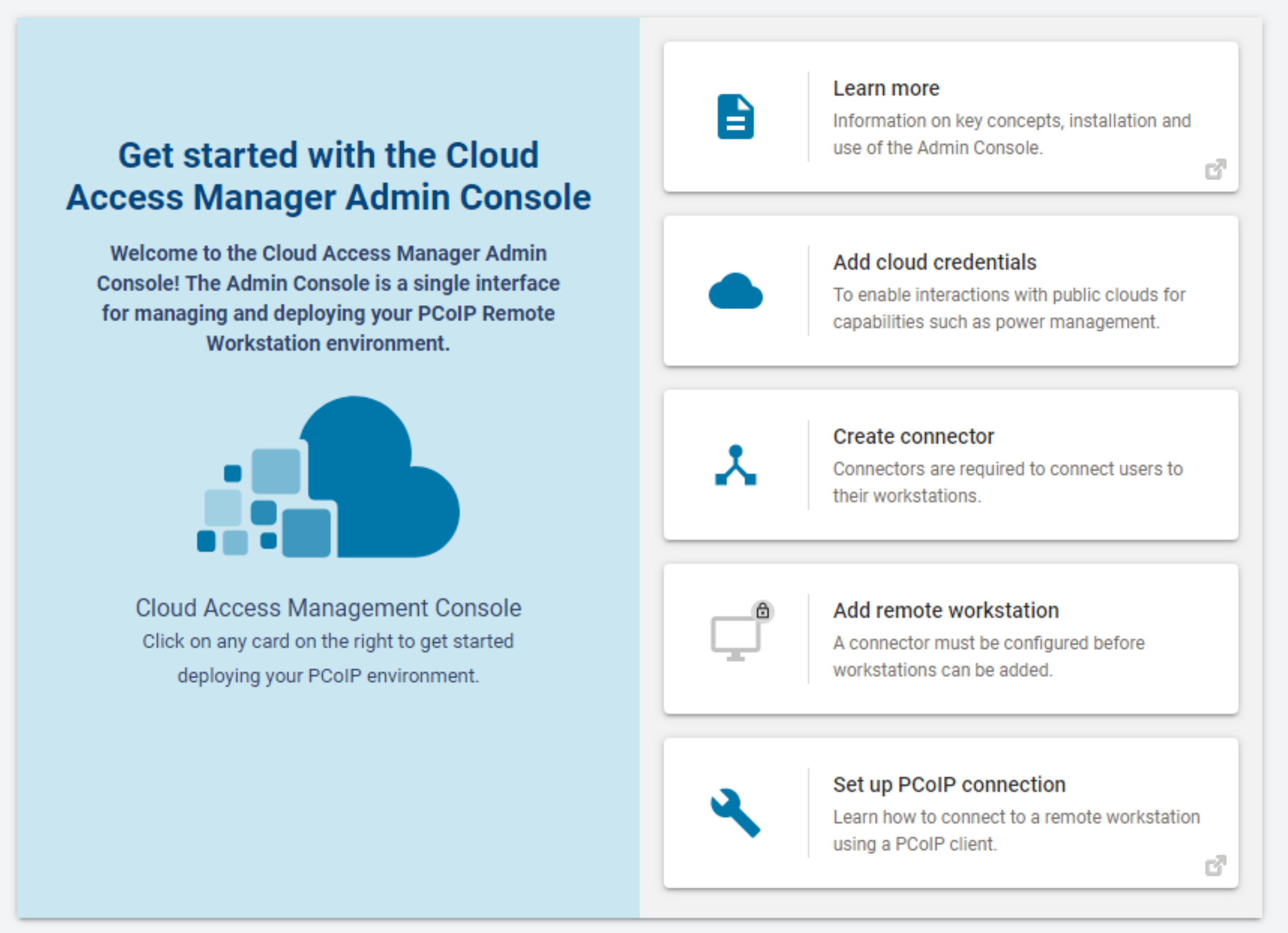
- Pop-ups have been blocked on https://cam.teradici.com/.

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.



Get started with the Cloud Access Manager Admin Console

Welcome to the Cloud Access Manager Admin Console! The Admin Console is a single interface for managing and deploying your PCoIP Remote Workstation environment.

Cloud Access Management Console

Click on any card on the right to get started deploying your PCoIP environment.

Learn more
Information on key concepts, installation and use of the Admin Console.

Add cloud credentials
To enable interactions with public clouds for capabilities such as power management.

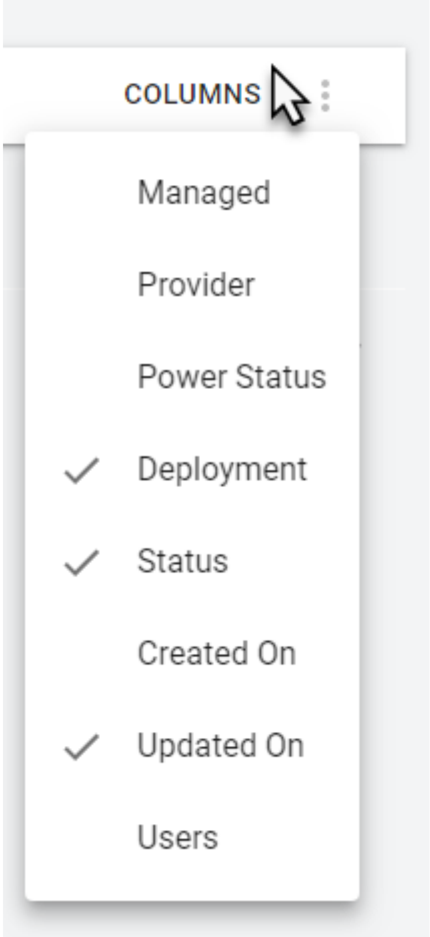
Create connector
Connectors are required to connect users to their workstations.

Add remote workstation
A connector must be configured before workstations can be added.

Set up PCoIP connection
Learn how to connect to a remote workstation using a PCoIP client.

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.

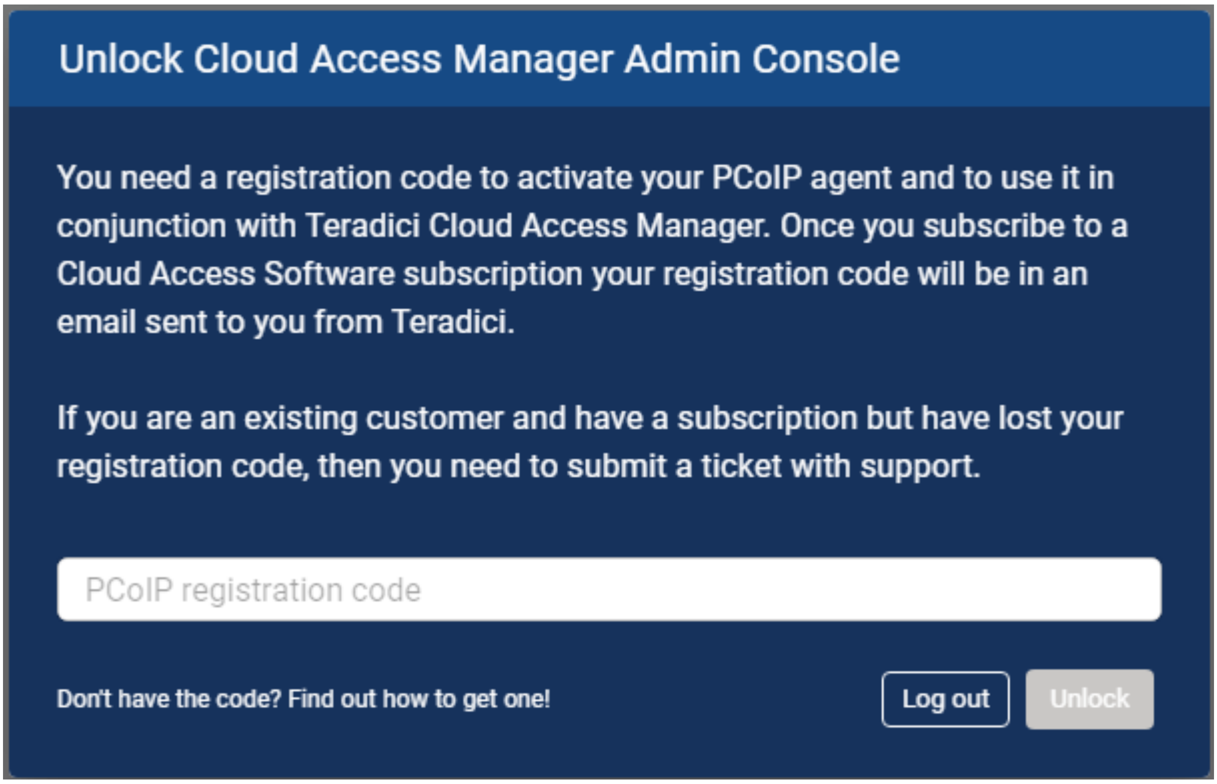


The format you select will be preserved when you log back into the Cloud Access Manager Admin Console.

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.

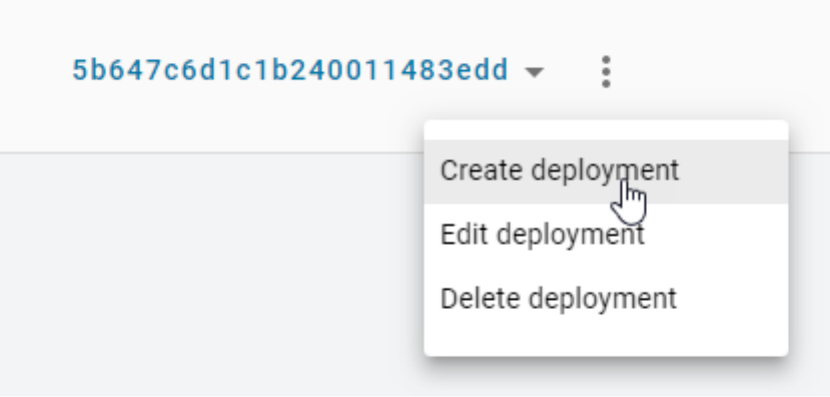


Unlock Cloud Access Manager Admin Console

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.



3. Enter the following information:
    - Enter the deployment name.
    - Enter your Cloud Access Software registration code.
4. You can optionally enter AWS, Azure, and GCP 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 AWS, Azure, and GCP then you do not need to enter this information.

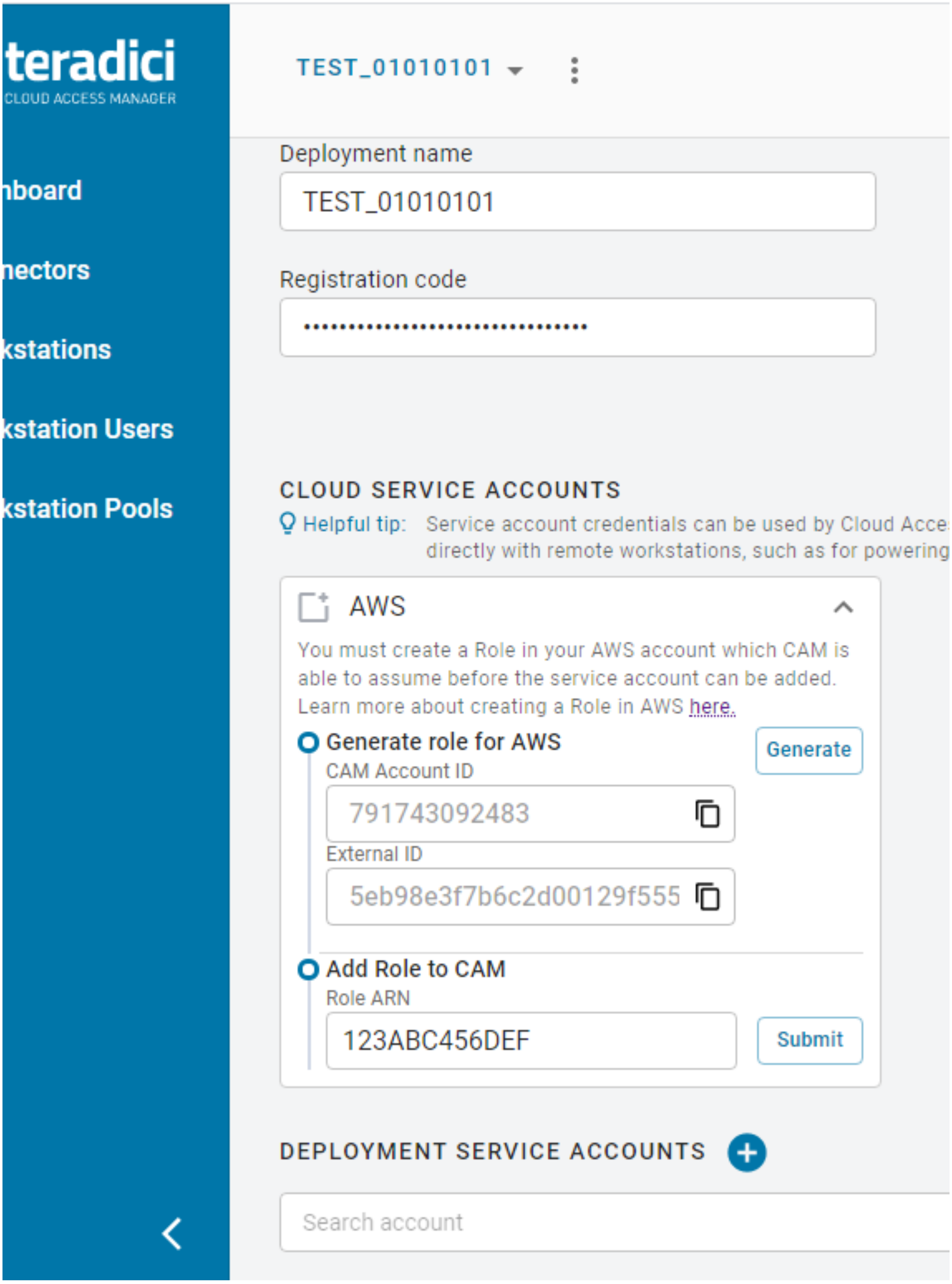
    > **Cloud Service Account Credentials**
    >
    > These credentials are used in places where the Cloud Access Manager interacts with your cloud environment to perform actions such as powering a remote workstation on or off. If credentials are not provided, remote workstations in that cloud can still be added to Cloud Access Manager and users can still be entitled to the remote workstation and start a PCoIP session, but Cloud Access Manager cannot perform functions such as power on and off.

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.

> **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.

AWS Cloud Credentials

Through the Cloud Access Manager Admin Console you can generate a CAM Account ID and Exernal ID that can be used when creating an AWS role through the AWS Management Console.



Deployment name

TEST_01010101

Registration code

••••••••••••••••••••••••••••••••

CLOUD SERVICE ACCOUNTS

Helpful tip: Service account credentials can be used by Cloud Acce
directly with remote workstations, such as for powering

AWS

You must create a Role in your AWS account which CAM is able to assume before the service account can be added. Learn more about creating a Role in AWS here.

Generate role for AWS

CAM Account ID

791743092483

External ID

5eb98e3f7b6c2d00129f555

Add Role to CAM

Role ARN

123ABC456DEF

DEPLOYMENT SERVICE ACCOUNTS

⚠ **AWS Role Creation and Permission Policy**

You must create a role in your AWS account which Cloud Access Manager is able to assume. You must use the Account ID and External IDs when creating the AWS role. For more information on creating roles in AWS, see here.

1. Once you have entered the CAM Account ID and External ID you will need to create a permissions policy for Cloud Access Manager that contains the following permissions:

   - Service: EC2
   - Actions:
     - List: *DescribeInstances*
     - Write: *RebootInstances StartInstances StopInstances TerminateInstances*

   There are additional permissions needed to verify that the role has all the required permissions before being added to a deployment:

   - Service: IAM
   - Actions
     - List: *ListAttachedRolePolicies ListRolePolicies*
     - Read: *GetPolicy GetPolicyVersion GetRolePolicy*

   The following is an example of how the permissions set should look in a JSON format:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:RebootInstances",
                "iam:GetPolicyVersion",
                "ec2:DescribeInstances",
                "ec2:TerminateInstances",
                "iam:GetPolicy",
                "ec2:StartInstances",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "ec2:StopInstances",
                "iam:GetRolePolicy"
            ],
            "Resource": "*"
            }
        ]
}
```

If the user tries to add an AWS role that doesn't have these permissions, Cloud Access Manager will still add the role but will not validate that it has the required permissions.

You can now associate a permissions policy to this role.

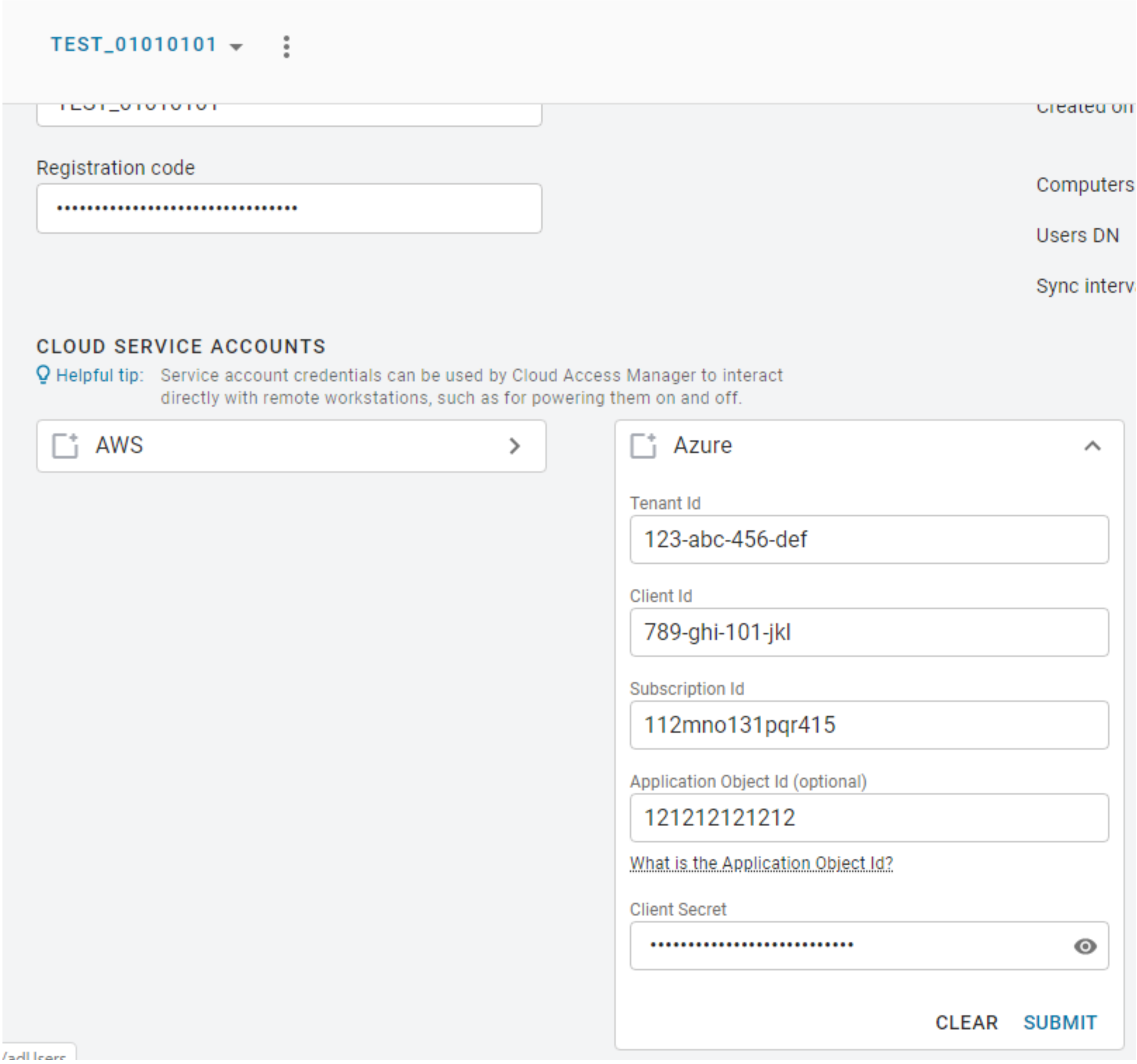
2. Once you have created the role in AWS, copy and paste the role ARN and enter it into the Role ARN field in the Cloud Access Manager Admin Console.
3. Click **Submit**.

For information on the AWS Service Account roles and permission policies with Cloud Access Manager, see here.

Azure Cloud Credentials

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.



TEST_01010101

Registration code

••••••••••••••••••••••••••••••••

Computers

Users DN

Sync interv

CLOUD SERVICE ACCOUNTS

Helpful tip: Service account credentials can be used by Cloud Access Manager to interact directly with remote workstations, such as for powering them on and off.

AWS

Azure

Tenant Id: 123-abc-456-def

Client Id: 789-ghi-101-jkl

Subscription Id: 112mno131pqr415

Application Object Id (optional): 121212121212

What is the Application Object Id?

Client Secret: ••••••••••••••••••••••••••••

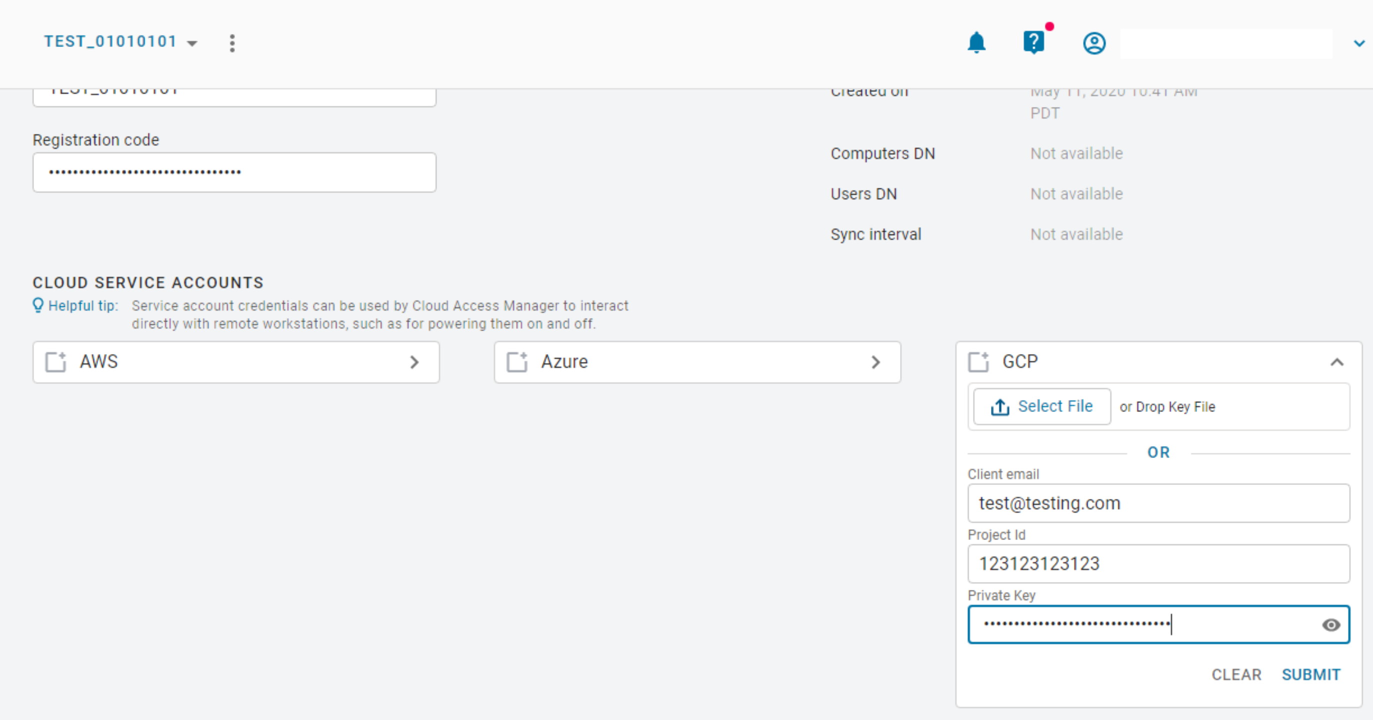
Azure Client Secret

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.

For information on the Azure Service Account and permission requirements with Cloud Access Manager, see here.

GCP Cloud Credentials

You can enable GCP cloud credentials by entering the GCP client email, Project ID and Private Key and clicking **Submit**. You can also upload the JSON Key file with the GCP cloud credentials.



TEST_01010101

Registration code
••••••••••••••••••••••••••••••••

Created on May 11, 2020 10:41 AM PDT

Computers DN Not available

Users DN Not available

Sync interval Not available

CLOUD SERVICE ACCOUNTS

Helpful tip: Service account credentials can be used by Cloud Access Manager to interact directly with remote workstations, such as for powering them on and off.

Client email
test@testing.com

Project Id
123123123123

Private Key
••••••••••••••••••••••••••••••••

For more information on GCP Cloud Service Accounts with Cloud Access Manager, see here.

For information on the GCP Service Account and permission requirements with Cloud Access Manager, see here.

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.

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

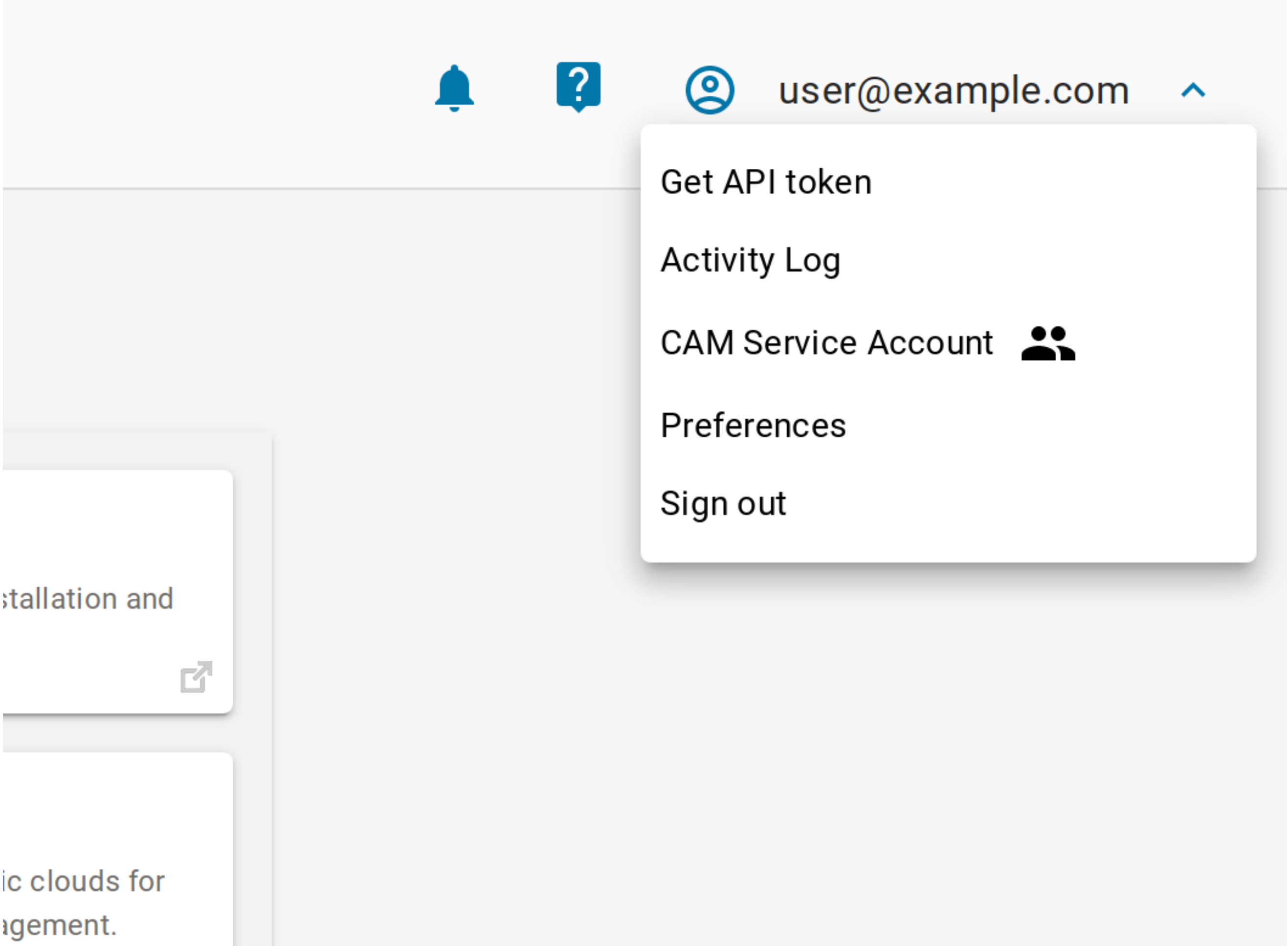
The API Access Token can be used to enable a user to operate at a level above deployments, such as creating a new deployment. The API Access Token is only valid for a limited period of time. This token also acts as an authorization token that can be used when performing an account ownership transfer, as outlined here.

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

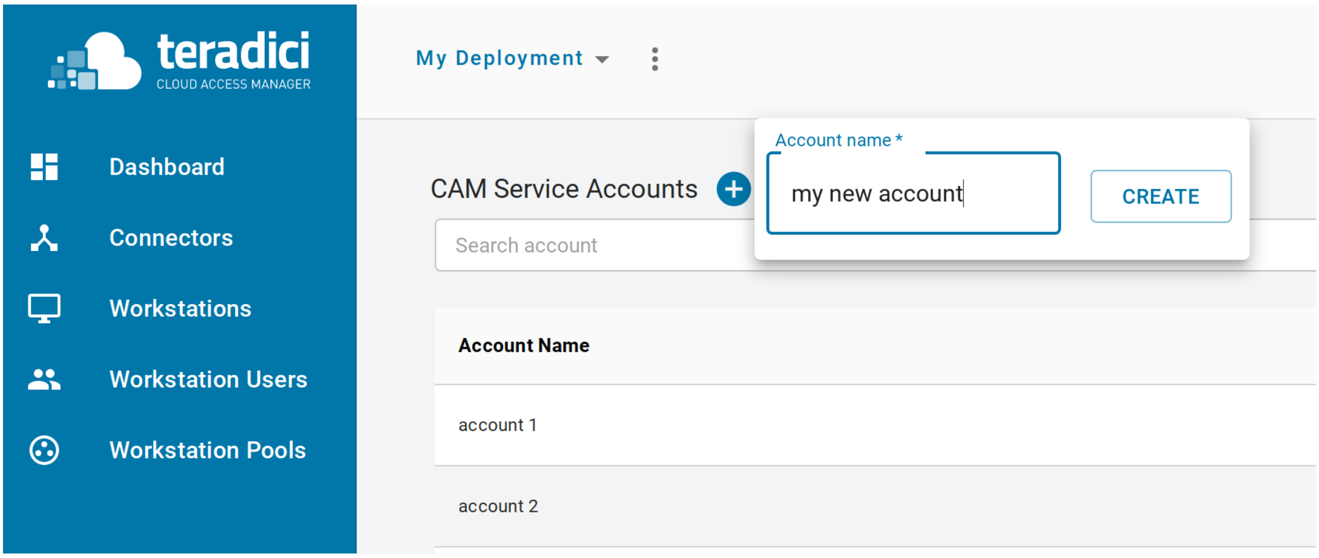
Creating a CAM Service Account

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 this key cannot be recovered if lost.

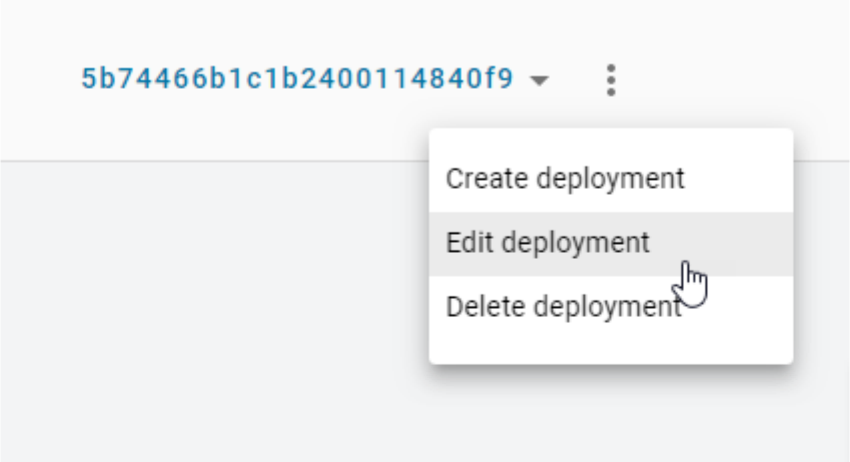
4. Go to the Service Account Keys section of the Cloud Access Manager API documentation for the required APIs to use this key to create a deployment.

Creating and Assigning a Deployment Service Account

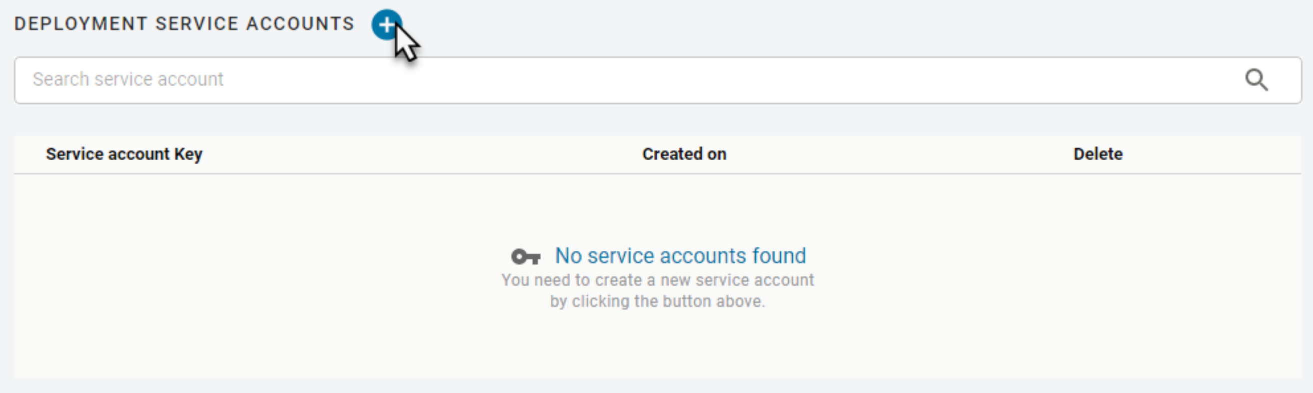
You can create and assign a deployment service account to a deployment through the **Deployments** option within the Cloud Access Manager Admin Console. The following steps outline how to add a deployment service account to an existing deployment:

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.



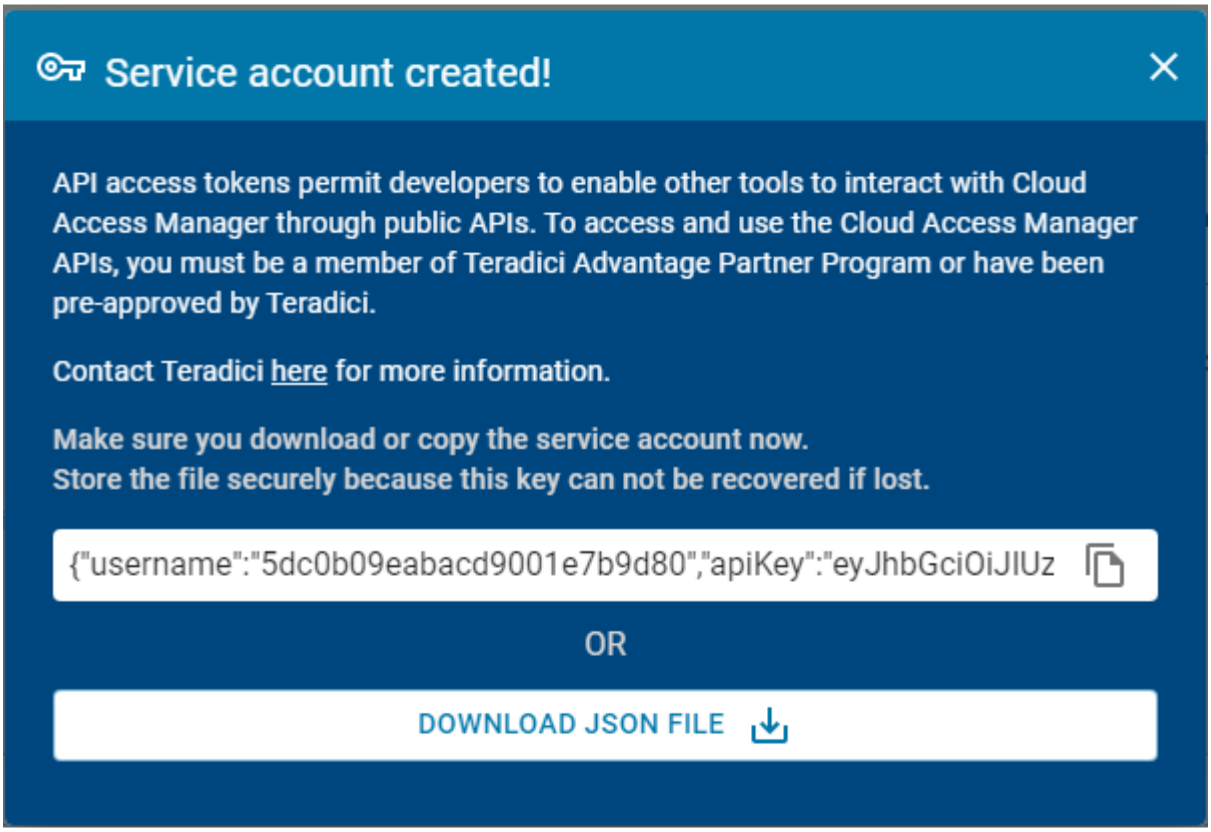
DEPLOYMENT SERVICE ACCOUNTS

Search service account

Service account Key	Created on	Delete

No service accounts found
You need to create a new service account
by clicking the button above.

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.



Service account created!

API access tokens permit developers to enable other tools to interact with Cloud Access Manager through public APIs. To access and use the Cloud Access Manager APIs, you must be a member of Teradici Advantage Partner Program or have been pre-approved by Teradici.

Contact Teradici here for more information.

Make sure you download or copy the service account now.
Store the file securely because this key can not be recovered if lost.

{"username":"5dc0b09eabacd9001e7b9d80","apiKey":"eyJhbGciOiJIUz

OR

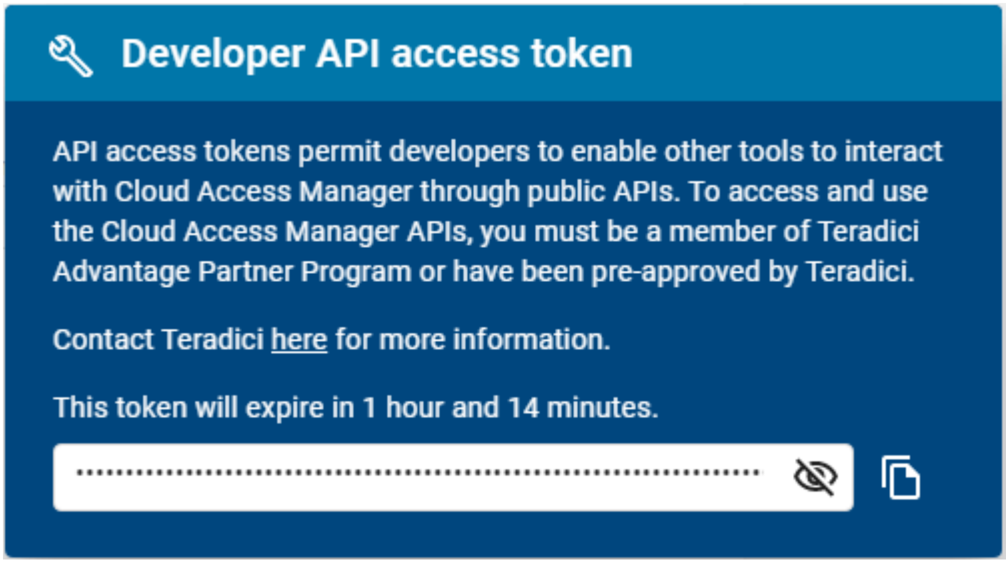
All deployment service accounts associated with a specific deployment will be listed on the deployment page. You can delete deployment service accounts from this page. For information on using the deployment service accounts and deployment service keys with the Cloud Access Manager APIs, see here.

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:



Developer API access token

API access tokens permit developers to enable other tools to interact with Cloud Access Manager through public APIs. To access and use the Cloud Access Manager APIs, you must be a member of Teradici Advantage Partner Program or have been pre-approved by Teradici.

Contact Teradici here for more information.

This token will expire in 1 hour and 14 minutes.

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

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.

Creating and Installing a Cloud Access Connector

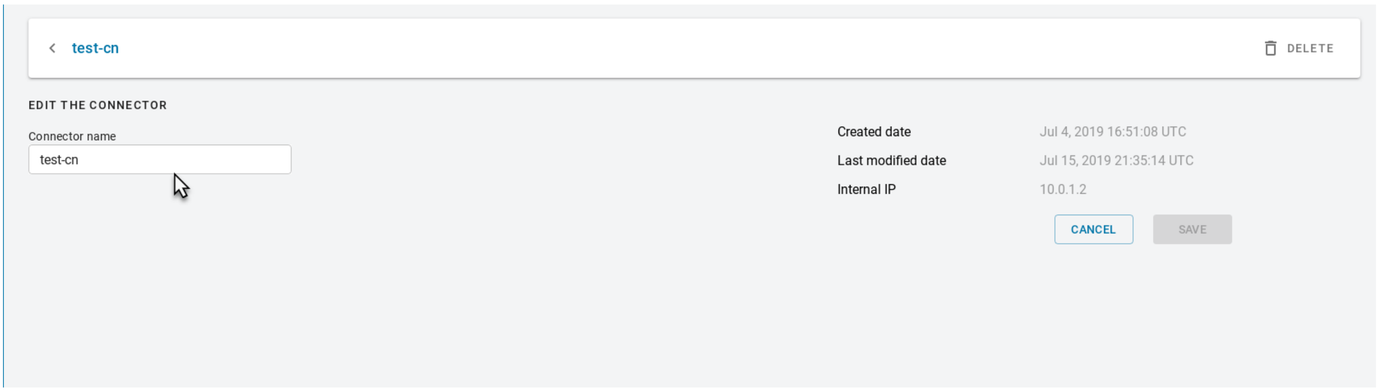
Once you have created a deployment you need to download the Cloud Access Connector installer, obtain a Cloud Access Connector token and use this token to install your Cloud Access Connector. For information on how to do carry out these steps, see Cloud Access Connector Installation. When you are creating 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**.



EDIT THE CONNECTOR

Connector name: test-cn

Created date	Jul 4, 2019 16:51:08 UTC
Last modified date	Jul 15, 2019 21:35:14 UTC
Internal IP	10.0.1.2

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

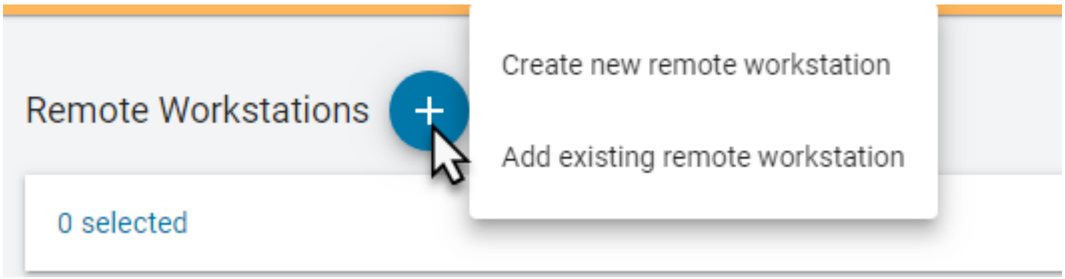
If you wish to use your own custom images or templates, you must create and manage those outside of Cloud Access Manager and create your remote workstation outside of Cloud Access Manager also. Once you have created a remote workstation you can add it to your deployment in Cloud Access Manager for brokering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

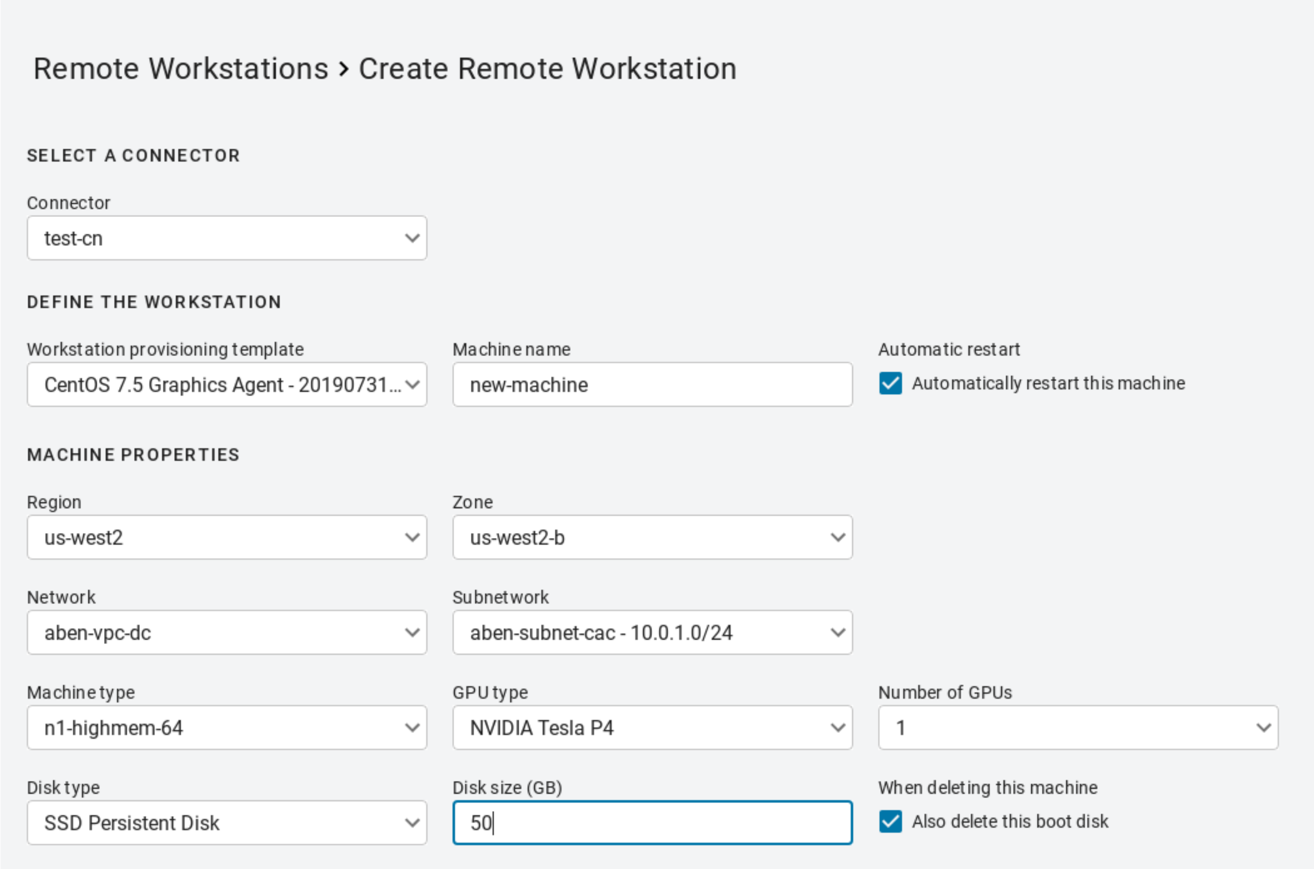
You must have a valid cloud service account to enable this feature:

1. Click **Remote Workstations** from the console sidebar.
2. Click **Create new remote workstation** from the add remote workstation icon.


Remote Workstations
+
Create new remote workstation
Add existing remote workstation
0 selected

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 intitiated 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

Workstation provisioning template: 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

Network: aben-vpc-dc

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.

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

***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.

The remote workstation will now appear in the table of available machines on the **Remote Workstations** page.

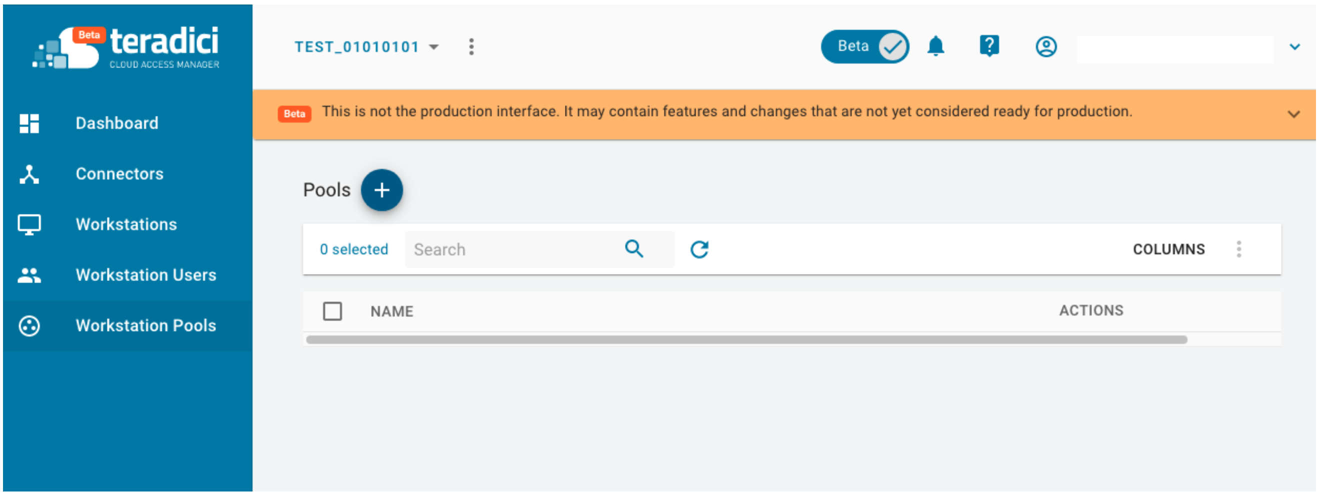
Workstation Pools

You can create workstation pools within the Cloud Access Manager Admin Console. A workstation pool is a group of remote workstations. To simplify user access management, a user group or individual users can simply be assigned to a workstation pool. Once the user logs in, they are automatically and persistently assigned a remote workstation within the pool.

Creating a Workstation Pool

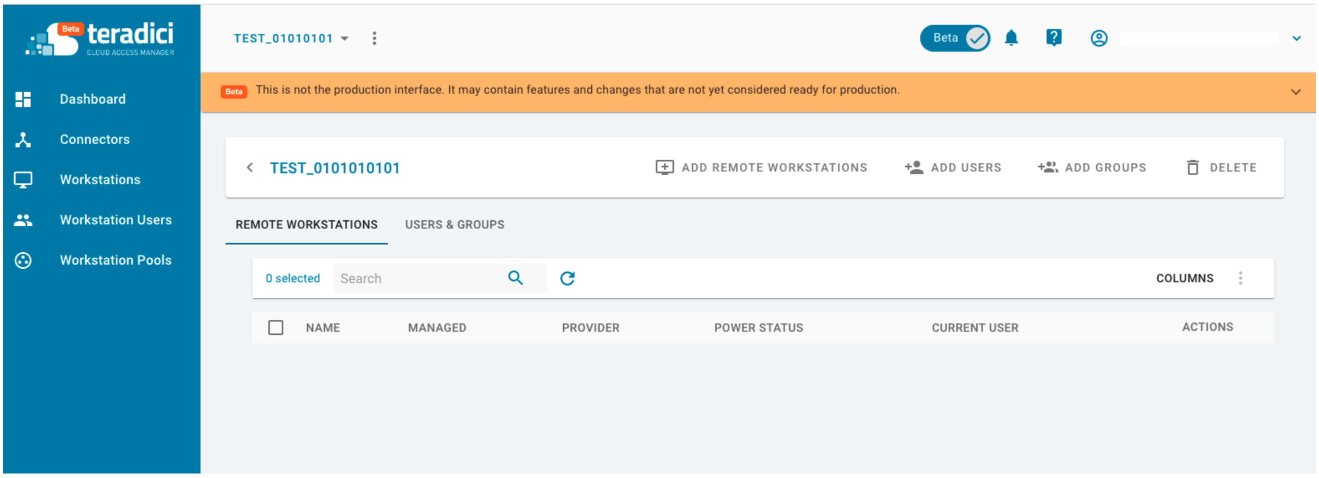
The following steps outline how to create a workstation pool and add remote workstations and users to it:

1. Click on **Workstation Pools** from the Cloud Access Manager Admin Console sidebar.
2. Click the **+** icon to create a new workstation pool.



Beta This is not the production interface. It may contain features and changes that are not yet considered ready for production.

3. Enter a Pool Name and click **Create**. You will now have a workstation pool where you can add remote workstations, users and user groups.



Beta This is not the production interface. It may contain features and changes that are not yet considered ready for production.

☐	NAME	MANAGED	PROVIDER	POWER STATUS	CURRENT USER	ACTIONS

4. From the workstation pool page click ADD REMOTE WORKSTATIONS and search for an available workstation to add to the pool and click SAVE. Remote workstations and users within a workstation pool are a subset of the available remote workstations and users within a specific deployment. As a result of this, you will only be able to add remote workstations and users that have already been created in Cloud Access Manager.
5. From the workstation pool page click ADD USERS and/or ADD GROUPS search for available users and user groups to add to the pool and click SAVE.

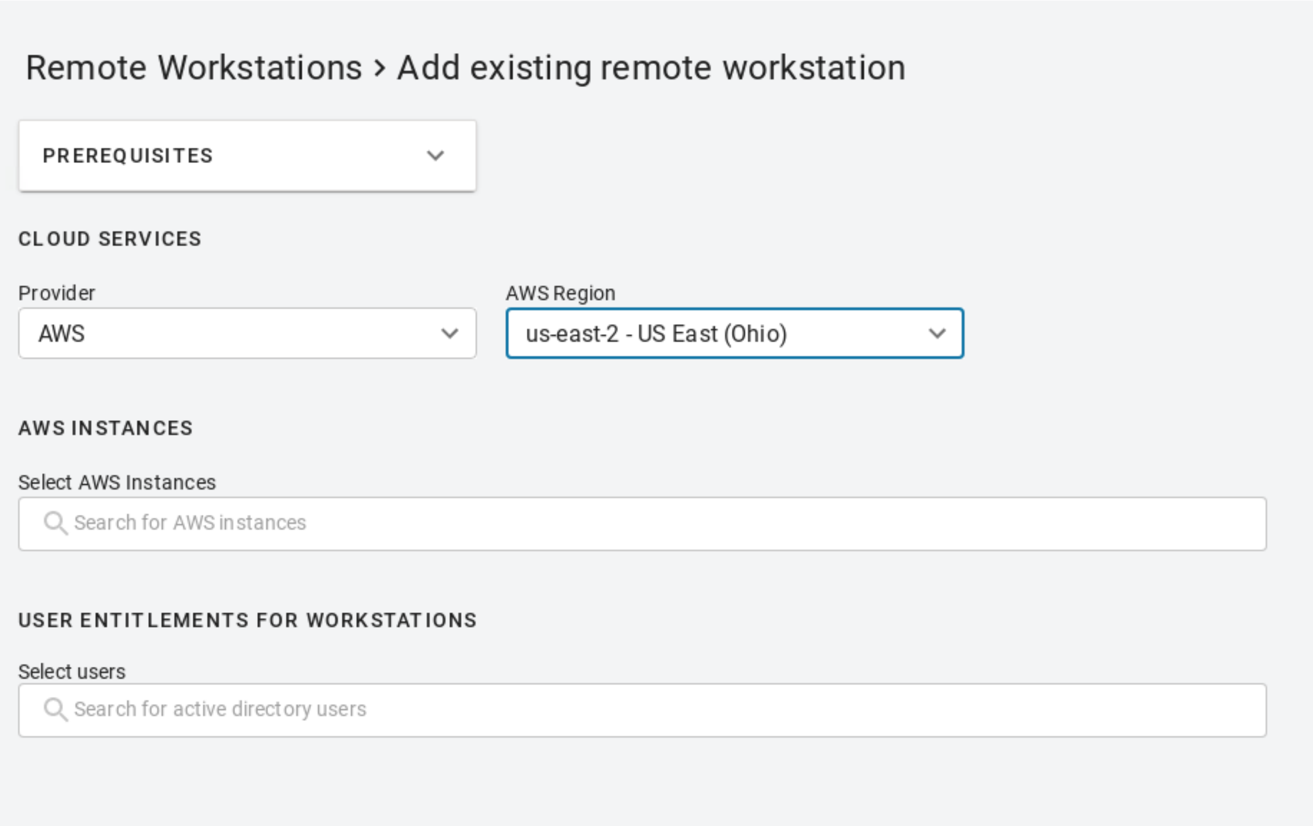
You can add multiple workstation pools to specific deployments. Each workstation pool will list the remote workstations, users and user groups within that pool, as well as component information for these remote workstations and users.

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 Cloud Access Connector.
5. Select a provider for cloud services. If your remote workstation has AWS credentials, select the AWS region and your AWS instances.



Remote Workstations > Add existing remote workstation

CLOUD SERVICES

Provider: AWS

AWS Region: us-east-2 - US East (Ohio)

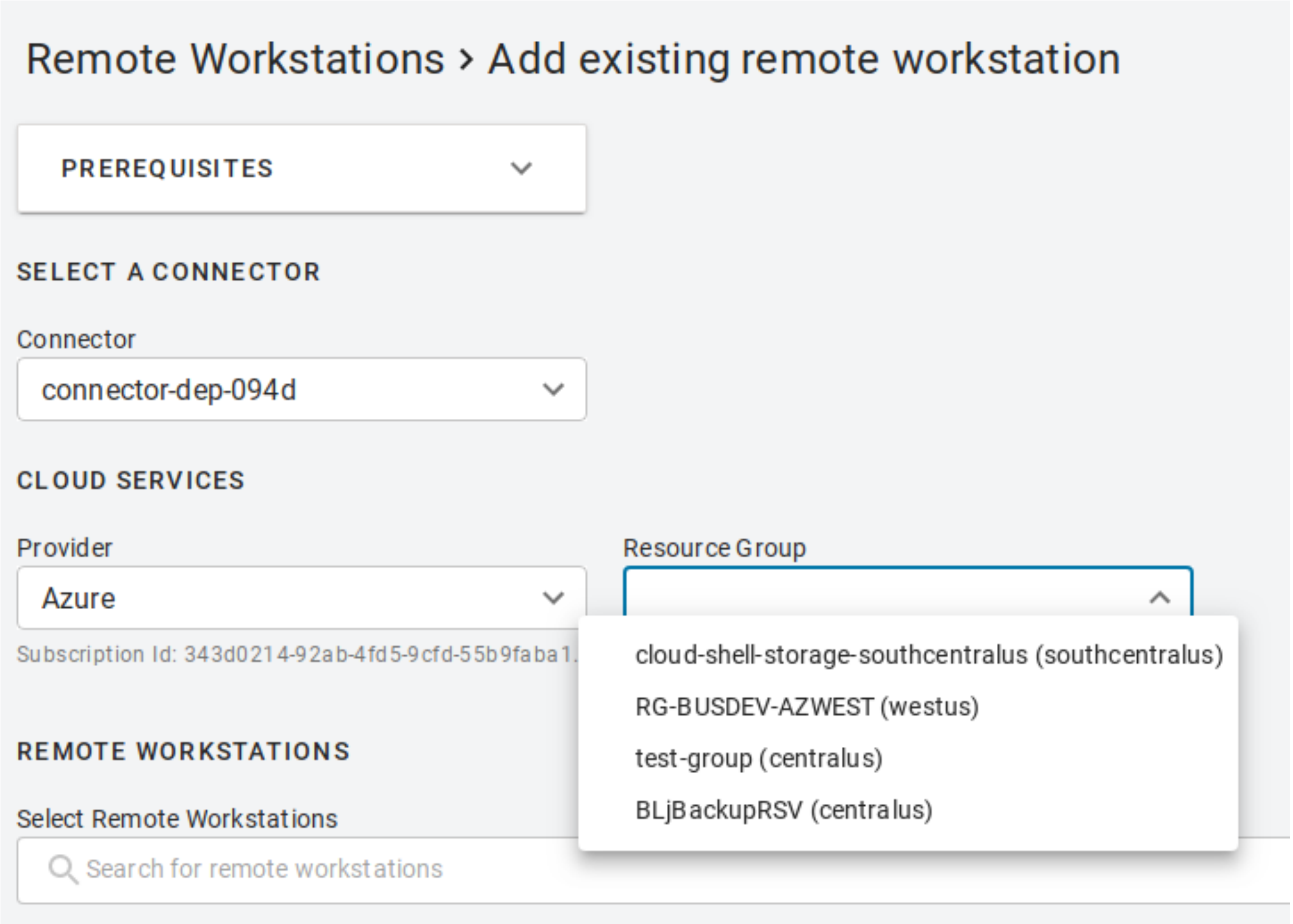
AWS INSTANCES

Select AWS Instances

USER ENTITLEMENTS FOR WORKSTATIONS

Select users

If your remote workstation has Azure credentials, you can view and select available resource groups from the resource groups tab.



Remote Workstations › Add existing remote workstation

PREREQUISITES

SELECT A CONNECTOR

Connector: connector-dep-094d

CLOUD SERVICES

Provider: Azure

Subscription Id: 343d0214-92ab-4fd5-9cfd-55b9faba1

Resource Group:

- cloud-shell-storage-southcentralus (southcentralus)
- RG-BUSDEV-AZWEST (westus)
- test-group (centralus)
- BLjBackupRSV (centralus)

REMOTE WORKSTATIONS

Select Remote Workstations

Search for remote workstations

If your remote workstation has GCP credentials select the GCP zone where your remote workstation resides and add it from that zone.

6. Select your remote workstations.
7. Select and assign users.
8. Click **SAVE**.

The remote workstation should now appear on the 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

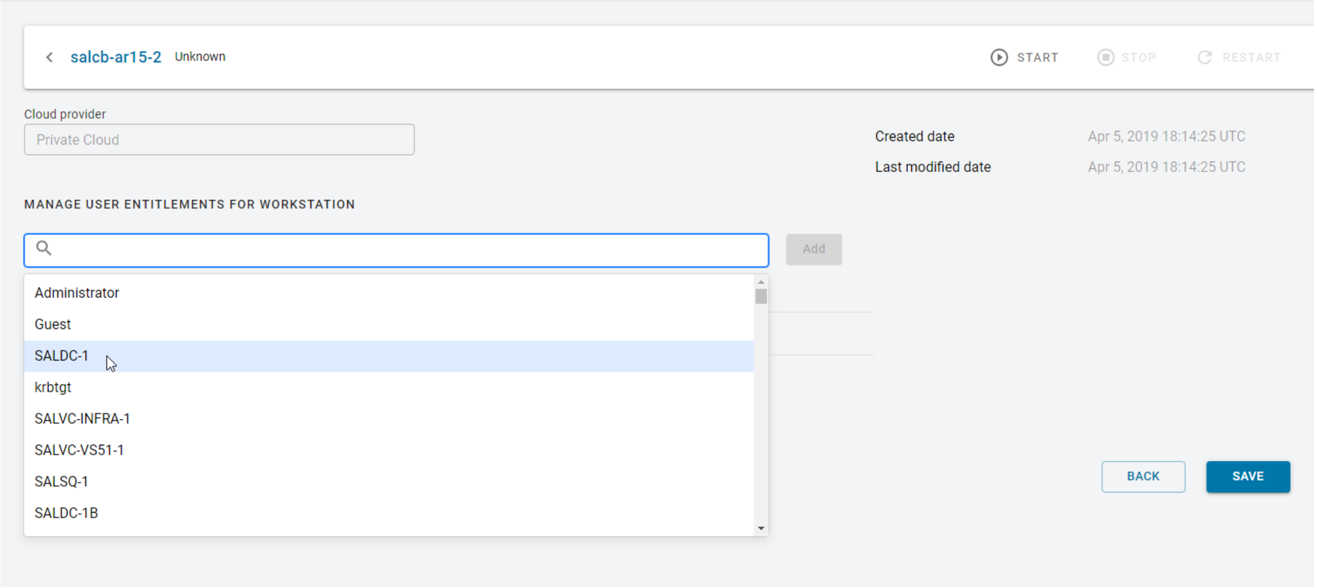
Once you have created a remote workstation within the Cloud Access Manager Admin Console you can manage and reconfigure it directly from the **Remote Workstations** page.

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

Entitling Users

Once you have created a remote workstation you can entitle users from the active directory account to specific remote workstations. 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:



salcb-ar15-2 Unknown

Cloud provider: Private Cloud

Created date: Apr 5, 2019 18:14:25 UTC

Last modified date: Apr 5, 2019 18:14:25 UTC

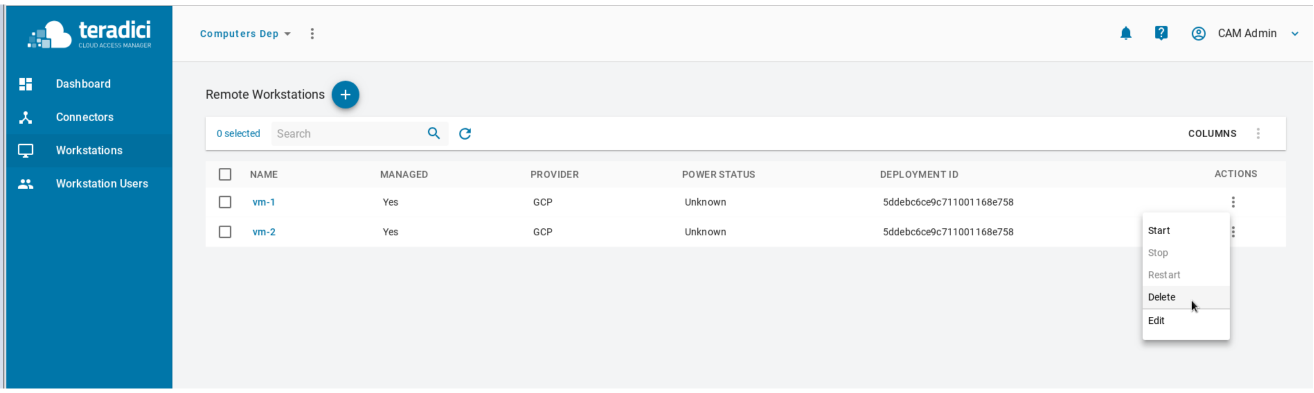
4. Click **Add** and then **SAVE**.

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

Deleting Remote Workstations from the Public Cloud

You can delete existing remote workstations from AWS, Azure, and GCP from the Cloud Access Manager Admin Console. Only remote workstations that exist in AWS, Azure, and GCP and are part of deployments 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**.



□	NAME	MANAGED	PROVIDER	POWER STATUS	DEPLOYMENT ID	ACTIONS
□	vm-1	Yes	GCP	Unknown	5ddebc6ce9c711001168e758	⋮
□	vm-2	Yes	GCP	Unknown	5ddebc6ce9c711001168e758	⋮

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.

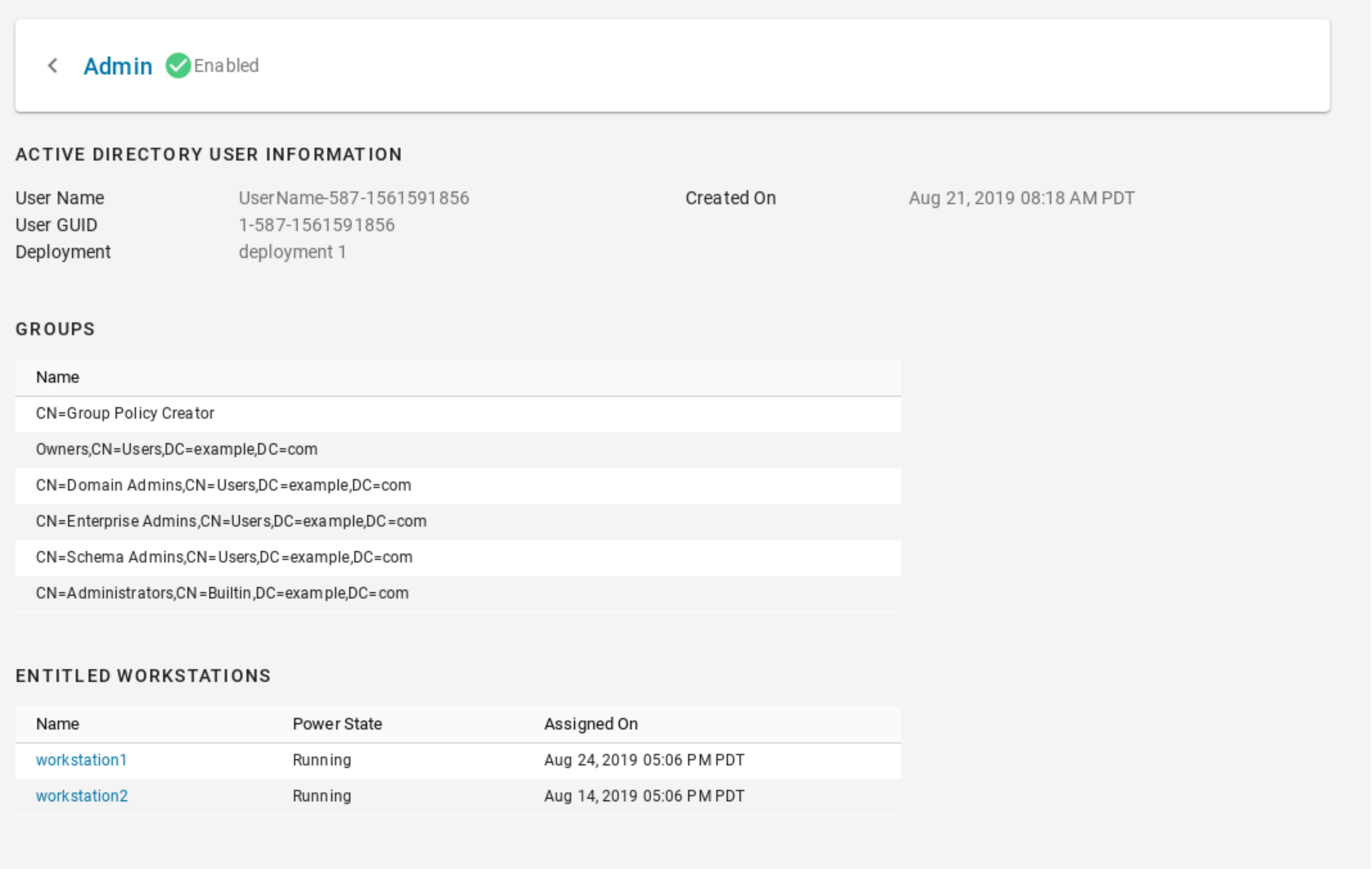
The remote workstation will disappear immediately from the Cloud Access Manager Admin Console and can take 5-10 minutes to be deleted from the CAM Service and public cloud. You should monitor the workstation in your cloud provider to ensure a successful completion. You will be notified in the Cloud Access Manager Admin Console on the whether the deletion was successfull or not.

Viewing Workstation Users

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:



< Admin ✓ Enabled

ACTIVE DIRECTORY USER INFORMATION

User Name	UserName-587-1561591856	Created On	Aug 21, 2019 08:18 AM PDT
User GUID	1-587-1561591856		
Deployment	deployment 1		

GROUPS

Name
CN=Group Policy Creator
Owners,CN=Users,DC=example,DC=com
CN=Domain Admins,CN=Users,DC=example,DC=com
CN=Enterprise Admins,CN=Users,DC=example,DC=com
CN=Schema Admins,CN=Users,DC=example,DC=com
CN=Administrators,CN=Builtin,DC=example,DC=com

ENTITLED WORKSTATIONS

Name	Power State	Assigned On
workstation1	Running	Aug 24, 2019 05:06 PM PDT
workstation2	Running	Aug 14, 2019 05:06 PM PDT

This gives you an overview of a specific user's entitlements and deployment information and can be useful for troubleshooting issues.

Updating Cloud Provider Information

Remote workstations that have been added into Cloud Access Manager, or created by Cloud Access Manager, can be associated to a cloud provider. This enables Cloud Access Manager to use the credentials for that cloud provider to access the remote workstation and enable power management. The cloud provider in which the remote workstation resides in can be changed. This can be done if either the remote workstation has been moved, or if the workstation was set to the Private Cloud, and you want to update it and assign it to the actual cloud 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.

The following section outlines how to update a remote workstation on the private cloud and associate it to a workstation in a public cloud:

1. Click the kebab option under the ACTIONS column to edit the desired remote workstation.
2. Click Edit.
3. From the CLOUD INFORMATION panel click EDIT PROVIDER.
4. Select the cloud provider the remote workstation belongs to.
5. Select the region, resource group and zone, depending on the cloud provider, the remote workstation resides in.
6. Select the remote workstation and update the provider.

If you enter the correct cloud provider and 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.

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 Manager Activity Log

The Cloud Access Manager activity log enables you to view a record of all activity and operations performed in your Cloud Access Manager environment. You can choose whether to show all records or just the records from a selected deployment. To view the activity log from the Cloud Access Manager Admin Console:

1. Click the user account icon within the Cloud Access Manager Admin Console.
2. Click **Activity Log** to display the activity log for that deployment.

The logs will show the date, user account, source and activity details.

You can search for logs based on specific operations that occured. You can download all the logs available in Cloud Access Manager by clicking the **Download CSV** button. For information on Cloud Access Manager service levels and how they impact the activity log, see Cloud Access Manager Service Level Objectives.

> **Activity Log Expiration Timeframe**
>
> The Activity Log in the Cloud Access Manager Admin Console contains short-term data, up to 7 days. After 7 days the log data expires. To maintain your long term storage Teradici recommends downloading the .csv file regularly.

Accessing the Activity Log through Cloud Access Manager APIs

Cloud Access Manager offers a RESTful API as an alternative to using the Cloud Access Manager Admin Console. It allows for programmatic management and automation of resources in Cloud Access Manager deployments.

The following API page details how you can obtain these Activity Logs using the Cloud Access Manager APIs: https://cam.teradici.com/api/docs#tag/Activity-Logs

The `Get activity logs` and `Download activity logs` API calls enable users to get the logs and download them as a .csv file.

SAML Configuration

A system administrator can implement SAML configuration through the Cloud Access Manager Admin Console and can specify which users are allowed to authenticate and access Cloud Access Manager. SAML configuration defines the IDP settings and trust. These settings control which users can authenticate from that IDP.

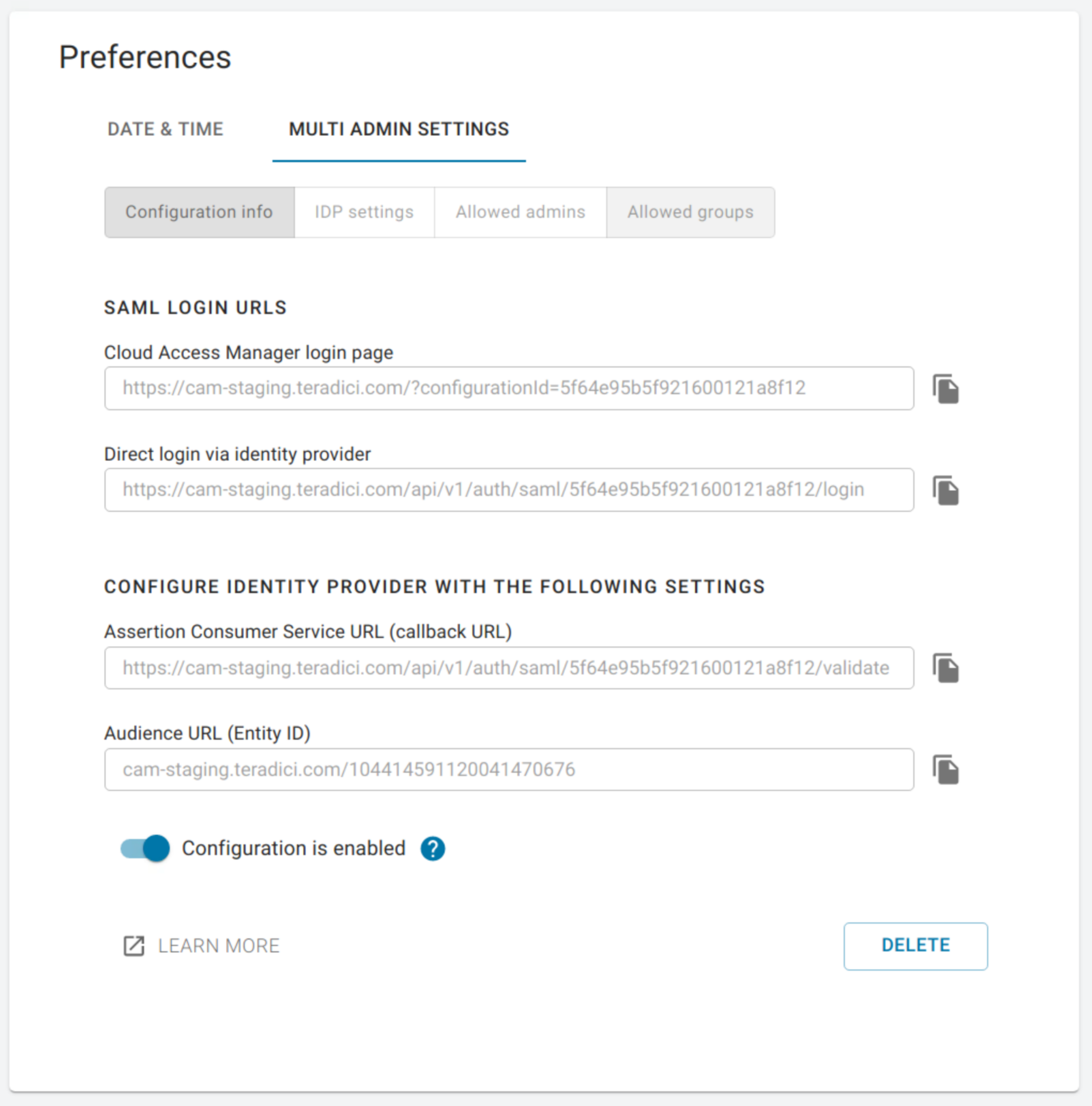
Supported Identity Providers

Teradici has tested SAML authentication with Okta and ADFS. Other SAML providers should work but have not yet been tested.

The following steps outline how to enable SAML authentication through the Cloud Access Manager Admin Console:

1. From the account icon click **Multi Admin Settings**.
2. Click the **Create SAML Configuration** button to initialize a default multi-administrator configuration.

The resulting configuration has 4 sections, each containing settings for the SAML configuration.



Preferences

SAML LOGIN URLS

Cloud Access Manager login page
https://cam-staging.teradici.com/?configurationId=5f64e95b5f921600121a8f12

Direct login via identity provider
https://cam-staging.teradici.com/api/v1/auth/saml/5f64e95b5f921600121a8f12/login

CONFIGURE IDENTITY PROVIDER WITH THE FOLLOWING SETTINGS

Assertion Consumer Service URL (callback URL)
https://cam-staging.teradici.com/api/v1/auth/saml/5f64e95b5f921600121a8f12/validate

Audience URL (Entity ID)
cam-staging.teradici.com/104414591120041470676

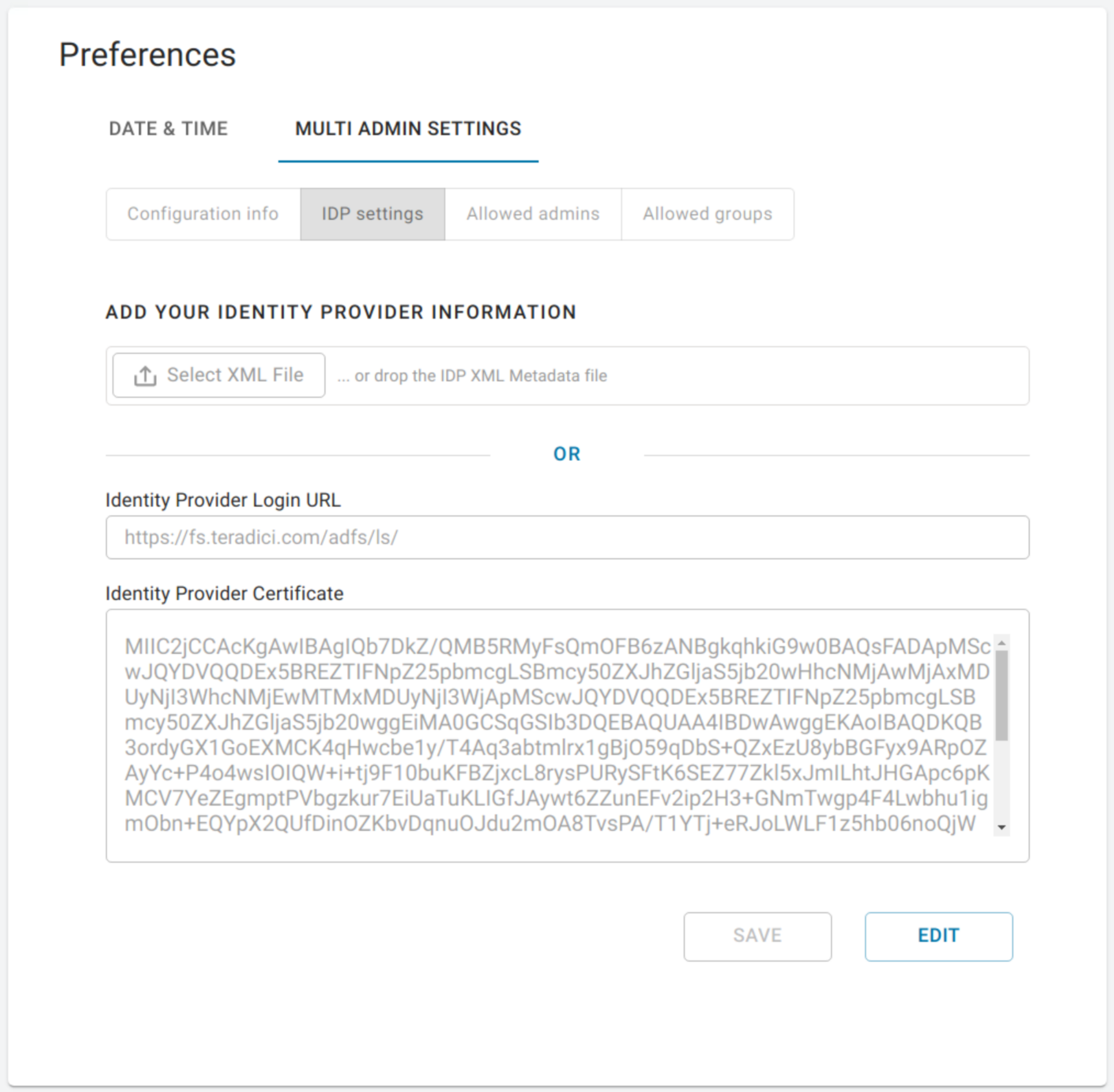
Configuration is enabled

The first section contains auto-generated information about the login URLs and IDP:

- **Cloud Access Manager login page**: A link to the page for multi-administrator login to the Cloud Access Manager Admin Console
- **Direct login via identity provider**: An endpoint to which multi-admin sign-in requests can be sent

- **Assertion Consumer Service URL**: The callback URL provided to the IDP to which user information is sent once the IDP has authorized the user
- **Audience URL**: The entity ID that the IDP can use to identify the Cloud Access Manager Admin Console

The second section contains settings that can be updated to manage the SAML configuration within the Cloud Access Manager:



ADD YOUR IDENTITY PROVIDER INFORMATION

Identity Provider Login URL

https://fs.teradici.com/adfs/ls/

Identity Provider Certificate

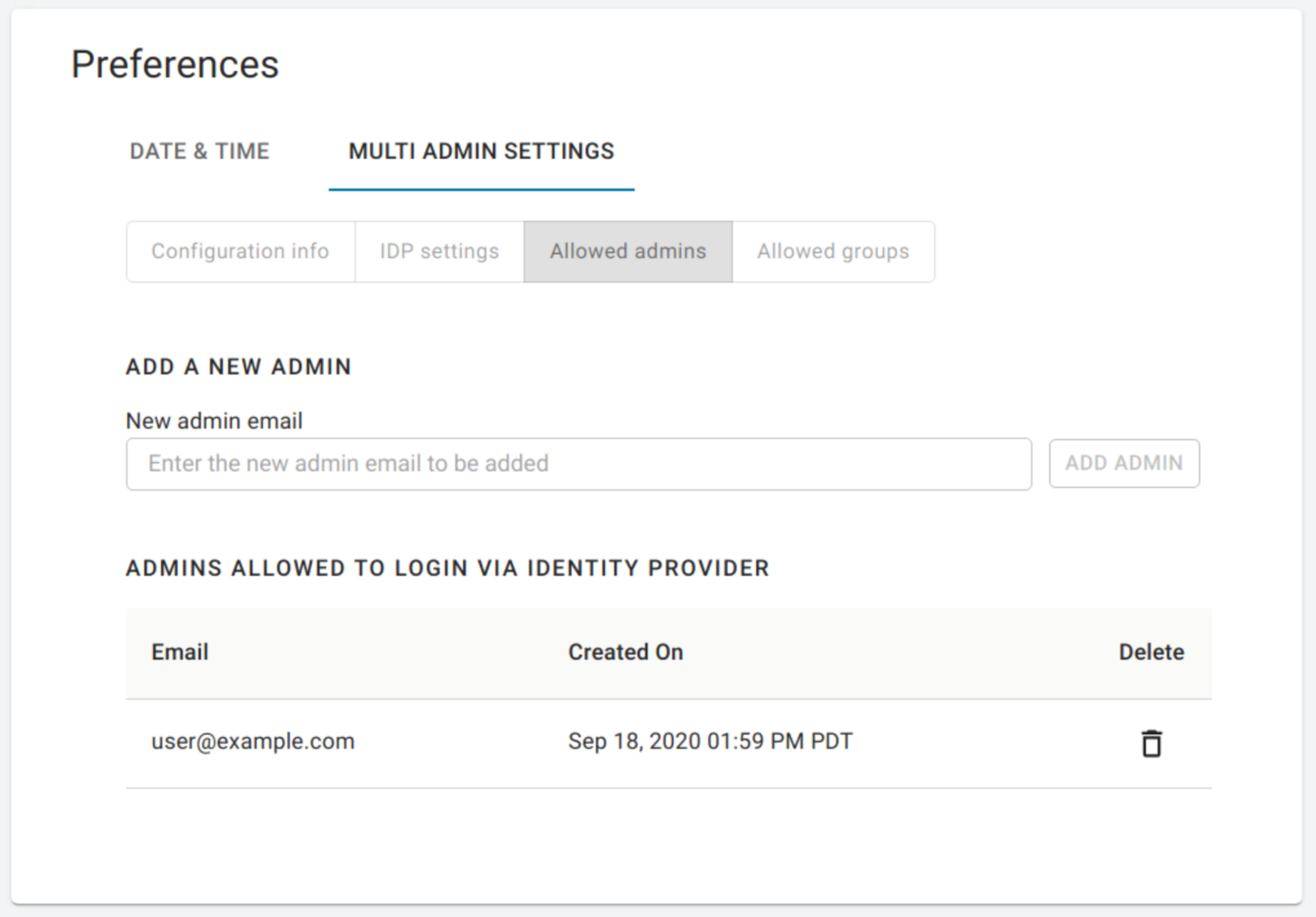
MIIC2jCCAcKgAwIBAgIQb7DkZ/QMB5RMyFsQmOFB6zANBgkqhkiG9w0BAQsFADApMSc
wJQYDVQQDEx5BREZTIFNpZ25pbmcgLSBmcy50ZXJhZGljaS5jb20wHhcNMjAwMjAxMD
UyNjI3WhcNMjEwMTMxMDUyNjI3WjApMScwJQYDVQQDEx5BREZTIFNpZ25pbmcgLSB
mcy50ZXJhZGljaS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDKQB
3ordyGX1GoEXMCK4qHwcbe1y/T4Aq3abtmlrx1gBjO59qDbS+QZxEzU8ybBGFyx9ARpOZ
AyYc+P4o4wsIOIQW+i+tj9F10buKFBZjxcL8rysPURySFtK6SEZ77Zkl5xJmILhtJHGApc6pK
MCV7YeZEgmptPVbgzkur7EiUaTuKLIGfJAywt6ZZunEFv2ip2H3+GNmTwgp4F4Lwbhu1ig
mObn+EQYpX2QUfDinOZKbvDqnuOJdu2mOA8TvsPA/T1YTj+eRJoLWLF1z5hb06noQjW

- **Identity Provider Login URL**: The IDP endpoint to which SAML authentication requests are sent

- **Identity Provider Certificate**: The public certificate of the IDP used to verify the signature of the IDP.

You can also upload a .xml file that contains your IDP information.

The third section enables you to add new admins as well as displaying all existing admins that are allowed to login via an IDP. To enable the access for a single user, visit the **Allowed admins** tab, enter their e-mail, and click the **Add Admin** button.



Email	Created On	Delete
user@example.com	Sep 18, 2020 01:59 PM PDT	🗑

The fourth section enables you to add new groups as well as displaying all existing groups that are allowed to login via an IDP.

To enable the access for a group of users, visit the **Allowed groups** tab, enter the claim type and group claim and click **Add Group**. The claim type informs Cloud Access Manager how the group is returned in the SAML assertion by your IDP. The group claim matches against the group either in the Group Name claim or in the Group ID claim returned in the SAML assertion for a user based on the claim type defined for the group.

A user's access via SAML can be enabled or disabled on either the **Allowed admins** or **Allowed groups** tabs.

Cloud Access Connector

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.

Teradici Cloud Access Software Registration Code

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.
- ***At least*** 4GB RAM.
- 20GB available storage ***or more***.
- 2 vCPUs ***or more***.

Dedicated instance types required

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 `--external-client-cidr` flag takes priority over the `--internal-client-cidr`. The default for the `--internal-client-cidr` is 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16. Any source that does not match to a `--internal-client-cidr` will default to an external connection.

  For example `--external-client-cidr 0.0.0.0/0` will treat everything as an external connection, to reset to the default behaviour you would need to enter the following command and flag parameters:

  ```
  ./cloud-access-connector update --internal-client-cidr 10.0.0.0/8 --internal-client-cidr 172.16.0.0/12 --internal-client-cidr 192.168.0.0/16
  ```

  When setting connections from a firewall or security gateway to be external, the internal CIDR will treat connections under a certain range as internal. For example the following example will treat connections originating from under the 10.11.12.0/24 CIDR except 10.11.12.1 as internal:

  ```
  ./cloud-access-connector update --internal-client-cidr 10.11.12.0/24 --external-client-cidr 10.11.12.1/32
  ```

- 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 `--external-pcoip-ip` flag 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.

Active Directory Domain Prerequisites

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.

> **Organisational Unit [OU] Permissions Dialog**
>
> Permissions are being assigned to the service account through the OU permissions dialog.

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 download the Cloud Access Connector archive, and extract it.

You need to ensure that you have a customer account created on teradici.com to access the download information.

⚠ **Teradici Distribution System**

Teradici is moving to a new distribution system. The URLs to download the Cloud Access Connector installation files are changing. Any automation, scripts or instructions downloading the installer from https://teradici.bintray.com/ should be updated to use the instructions outlined below. The download URL at https://teradici.bintray.com/ is deprecated and will be removed entirely in the near future. If your download fails please ensure that you have provided the correct network access, for more information on this, see Required External Connections.

Downloading the Installer from teradici.com

The following steps outline the current process that enables you to download the installer directly from teradici.com as a tar.gz file or else run the shell script from teradici.com:

1. SSH into the machine:

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

2. Download the installer from Teradici:
   - Open a web browser and navigate to https://docs.teradici.com/find/product/cloud-access-software/current/cloud-access-connector.
   - Download the installer and upload it to the machine or run the shell script provided to download the installer to the machine.

3. Unpackage the installer:
   - Previously the installer was extracted into the `~/v2connector` directory. This location has now changed. Run the following command to extract the installer to `/usr/sbin/` :

```
sudo tar xzvf <PATH TO FILE>/cloud-access-connector-
<version>_Linux.tar.gz -C /
```

Legacy Download Instructions

> ⚠ **Legacy Distribution System**
>
> The following steps are for the legacy distribution system which is **deprecated and will be removed entirely in the future**.

1. SSH into the machine:

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

   > **Copying Commands**
   >
   > If you copy and paste the sequence below into the console, the first two commands will execute immediately. Press `Enter` to execute the final command.

2. Download the component files from Teradici:

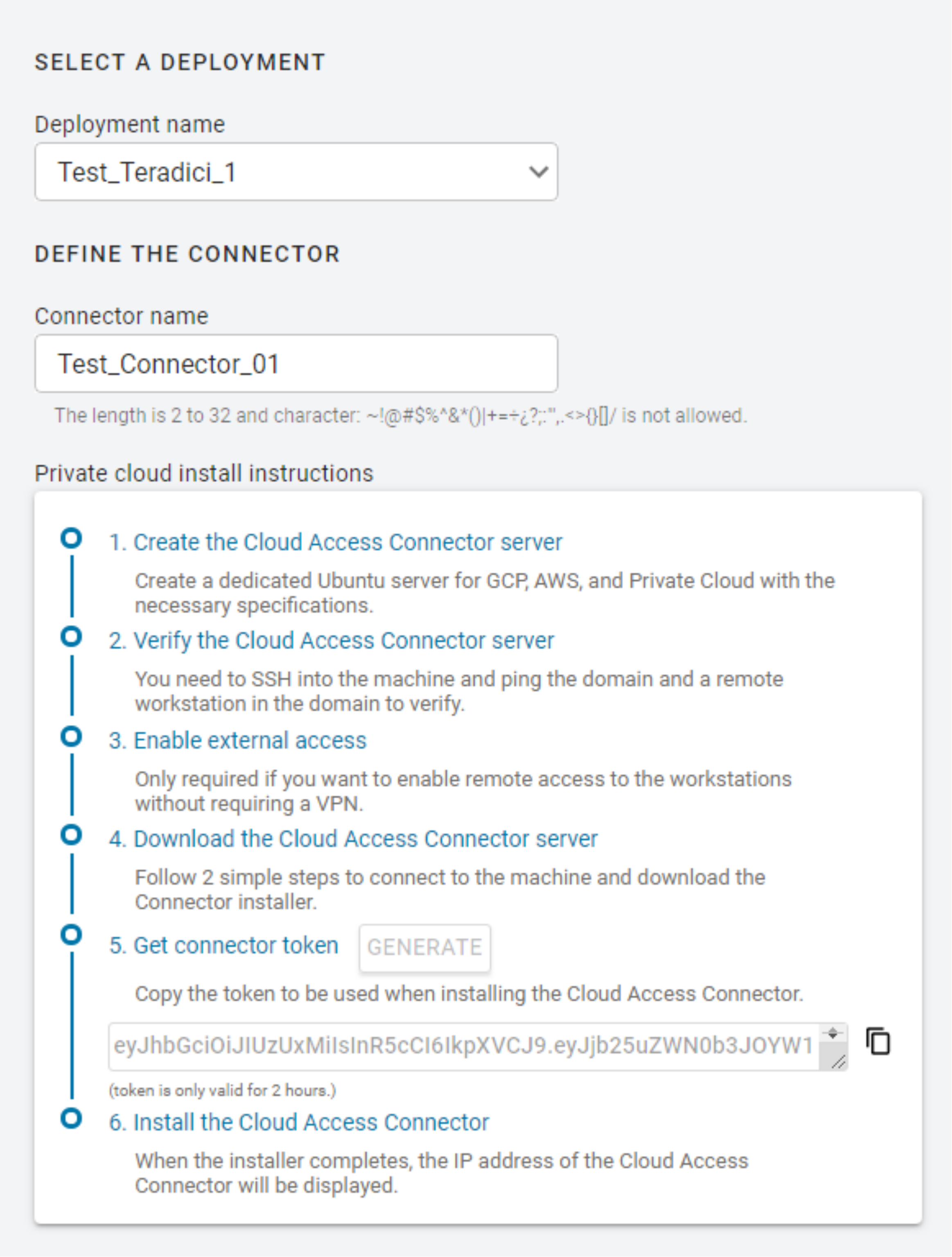
   ```
   mkdir ~/v2connector && cd ~/v2connector
   curl -LO https://teradici.bintray.com/cloud-access-connector/cloud-access-
   connector-0.1.1.tar.gz
   tar xzvf cloud-access-connector-0.1.1.tar.gz
   ```

Obtaining a Cloud Access Connector Token

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.



SELECT A DEPLOYMENT

Deployment name

Test_Teradici_1

DEFINE THE CONNECTOR

Connector name

Test_Connector_01

The length is 2 to 32 and character: ~!@#$%^&*()|+=÷¿?;:'",.<>{}[]/ is not allowed.

Private cloud install instructions

1. Create the Cloud Access Connector server

   Create a dedicated Ubuntu server for GCP, AWS, and Private Cloud with the necessary specifications.

2. Verify the Cloud Access Connector server

   You need to SSH into the machine and ping the domain and a remote workstation in the domain to verify.

3. Enable external access

   Only required if you want to enable remote access to the workstations without requiring a VPN.

4. Download the Cloud Access Connector server

   Follow 2 simple steps to connect to the machine and download the Connector installer.

5. Get connector token GENERATE

   Copy the token to be used when installing the Cloud Access Connector.

   eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJjb25uZWN0b3JOYW1

   (token is only valid for 2 hours.)

6. Install the Cloud Access Connector

   When the installer completes, the IP address of the Cloud Access Connector will be displayed.

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 `/usr/sbin` directory. Previously the directory used was `~/v2connector`. All new and recent installs and updates should use `/usr/sbin` but older installs and updates may still be using the legacy directory.

Latest Installer Version

Ensure that you are using the latest installer prior to installing or upgrading the Cloud Access Connector. If you are not using the latest installer, you may see one of the following errors:

- The installer is out of date. Please obtain the latest version and try again. See https://teradici.com/downloadcac for instructions.
- The installer is out of date. Please download the latest version from https://teradici.bintray.com/cloud-access-connector/cloud-access-connector-0.1.1.tar.gz and try again.

Install the Cloud Access Connector by running the following command:

```
cd /usr/sbin
sudo ./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 Cloud Access Connector will not use MFA, and will use your SSL key and certificate.

The available options are:

Flag	Description
`--token` (`-t`)	Required. The token generated for Cloud Access Manager.
`--enable-mfa`	Installs with multi-factor authentication enabled.
`--self-signed`	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.
`--force-install`	Replaces any existing Cloud Access Connector installation.
`--debug`	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.

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:

Flag	Type	Description
`--reg-code`	String	Cloud Access Software registration code, provided by Teradici. Cloud License registration code, provided by Teradici.
`--domain`	String	The AD domain that remote workstations will join.
`--domain-group`	String	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`).

Flag	Type	Description
`--users-dn`	StringArray	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). This field is looking for user's within the user-defined DN and SGs.
`--computers-dn`	StringArray	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).
`--sync-interval`	uint8	The interval (in minutes) for how often to sync AD users and computers with the CAM Service.
`--sa-user`	String	The Active Directory service account username.
`--sa-password`	String	The Active Directory service account password.
`--radius-server`	String	The FQDN or IP address of the RADIUS server to use for MFA. This flag is optional.
`--radius-port`	String	The RADIUS server port. If not specified, the default port (1812) is used. If `--radius-server` is specifed then this flag is optional.
`--radius-secret`	String	The shared secret used for configuring RADIUS authentication. If `--radius-server` is specifed then this flag is required.
`--ssl-key`	String	The full path and filename of the SSL key to use. The `--self-signed` flag overrides this flag.
`--ssl-cert`	String	The full path and filename of the SSL certificate (in PEM format) to use. The `--self-signed` flag overrides this flag.
`--https-proxy`	String	Specify the URL for a HTTPS proxy (overrides related proxy settings in environment variables)

Flag	Type	Description
`--accept-policies`	—	Automatically accept the EULA and Privacy Policy.
`--retrieve-agent-state`	Boolean	Enables the broker to retrieve the agent state for unmanaged and managed remote workstations. The default value for this flag is false. The available states are ***In Session***, ***Ready***, ***Starting***, ***Stopping***, ***Stopped*** and ***Unknown***. The value of this flag can either be true or false.
`--show-agent-state`	Boolean	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. Setting the value of this flag to true and the `--retrieve-agent-state` flag to false will result in no agent state displaying.
`--domain-controller`	String	Specifies one or more domain controllers to use with the Cloud Access Connector. For more information, see Specifing Domain Controllers.
`--external-pcoip-ip`	String	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. For more information on external network access, see Enabling External Network Access.
`--connector-network-cidr`	String	This is the CIDR to use for the Cloud Access Connector's docker network. The default docker network subnet is 10.101.0.0/16.
`--local-license-server-url`	String	Sets the URL for PCoIP License Server to be used for PCoIP Sessions. If this is not provided, ensure that the Cloud License Server is registered on the PCoIP Agent. Example: *--local-license-server-url* *http://10.10.10.10:7070/request*. For more information on the PCoIP License Server, see here.

Flag	Type	Description
`--add-pool-group`	String	Specifies one or more Active Directory groups, by entering the distinguished name (DN), to be assigned to pools for remote workstation management (eg, --pool-group 'CN=GroupPool1,CN=Users,DC=sample,DC=com' --pool-group 'CN=GroupPool2,CN=Users,DC=sample,DC=com'). By providing all the existing pools groups in the Cloud Access Connector settings would get replaced by the user specified ones. When running this command you need to run it with **adconfig**. Example: ***sudo ./cloud-access-connector adconfig --add-pool-group***.
`--users-filter`	String	The filter to search for users within Active Directory. Specify multiple filters with multiple options. Default user filter: (&(objectCategory=person)(objectClass=user)).
`--computers-filter`	String	The filter to search for computers within Active Directory. Specify multiple filters with multiple options. Default computer filter: (&(primaryGroupID=515)(objectCategory=computer)).
`--internal-client-cidr`	String	The CIDR for PCoIP Clients that connect to remote workstations directly.
`--external-client-cidr`	String	The CIDR for PCoIP Clients that connect to remote workstations through the Security Gateway. If external CIDRs settings are set, internal settings must be explicitly set.
`--setup-docker-image`	String	Specifies the docker image to be used from the setup container. This is intended to be used for debugging purposes and is not recommended to be used without guidance from Teradici support. Usage without guidance could result in failed installations.

Flag	Type	Description
`--docker-registry`	String	This is an optional flag that enables users to specify the docker image registry that they want to use when installing or updating a Cloud Access Connector. If an option is not specified, the default registry ***docker.cloudsmith.io/teradici/cloud-access-connector*** will be used. This is intended to be used for debugging purposes and is not recommended to be used without guidance from Teradici support. Usage without guidance from Teradici could result in failed installations.

Troubleshooting the Cloud Access Connector

If you encounter issues when attempting to install the Cloud Access Connector, please see the Troubleshooting section for information on how to potentially diagnose the specific issue. You can also view the following KB article here which provides a list of troubleshooting steps for common issues related to installing the Cloud Access Connector.

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.

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 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

When updating an installed Cloud Access Connector you must download the latest version of the Cloud Access Connector installer. For information on how to download the Cloud Access Connector installer, see here. Once you have downloaded the latest installer run the following command:

```
cd /usr/sbin
sudo ./cloud-access-connector update
```

Please note that older installs and updates may still be in the legacy directory at `~/v2connector` .

Teradici Distribution System

Teradici is moving to a new distribution system. The URLs to download the Cloud Access Connector installation files are changing. Any automation, scripts or instructions downloading the installer from https://teradici.bintray.com/ should be updated to use the instructions outlined here. The download URL at https://teradici.bintray.com/ is deprecated and will be removed entirely in the near future. You need to ensure that you have a customer account created on help.teradici.com to access the download information.

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. If you are not using the latest installer, you may see one of the following errors:

- The installer is out of date. Please obtain the latest version and try again. See https://teradici.com/downloadcac for instructions.
- The installer is out of date. Please download the latest version from https://teradici.bintray.com/cloud-access-connector/cloud-access-connector-0.1.1.tar.gz and try again.

Update options

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

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

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

Flag	Type	Description
`--enable-mfa`	String	Enable MFA/2FA.
`--radius-server`	String	The FQDN or IP address of the RADIUS server to use for MFA. This flag is optional.
`--radius-port`	String	The RADIUS server port. If not specified, the default port (1812) is used. If `--radius-server` is specifed then this flag is optional.
`--radius-secret`	String	The shared secret used for configuring RADIUS authentication. If `--radius-server` is specifed then this flag is required.
`--disable-mfa`	String	Disable MFA/2FA (all RADIUS options are ignored if specified.
`--domain-group`	String	The DN for the AD domain group that manages users and remote workstations in the Management Interface.
`--users-dn`	StringArray	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). This field is looking for user's within the user-defined DN and SGs.
`--computers-dn`	StringArray	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).

Flag	Type	Description
`--sync-interval`	uint8	The interval (in minutes) for how often to sync AD users and computers with the CAM Service.
`--self-signed`	String	Automatically generate self-signed SSL cert and key for testing purposes. If specified, --ssl-key and --ssl-cert options are ignored.
`--ssl-key`	String	The full path and filename of the SSL key to use with the CA connector gateway.
`--ssl-cert`	String	The full path and filename of the SSL certificate to use with the CA connector gateway.
`--show-agent-state`	Boolean	Show/hide PCoIP agent state (showing requires retrieve-agent-state to be true).
`--retrieve-agent-state`	Boolean	Enable/disable retrieving PCoIP agent state.
`--domain-controller`	StringArray	Specify a domain controller FQDN to use. May be specified multiple times for more than one DC.
`--external-pcoip-ip`	String	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 ").
`--connector-network-cidr`	String	This is the CIDR to use for the Cloud Access Connector's docker network. The default docker network subnet is 10.101.0.0/16.
`--local-license-server-url`	String	Sets the URL for PCoIP License Server to be used for PCoIP Sessions. If this is not provided, ensure that the Cloud License Server is registered on the PCoIP Agent. Example: *--local-license-server-url http://10.10.10.10:7070/request*. For more information on the PCoIP License Server, see here.
`--users-filter`	String	The filter to search for users within Active Directory. Specify multiple filters with multiple options. Default user filter: (&(objectCategory=person)(objectClass=user)).

Flag	Type	Description
`--computers-filter`	String	The filter to search for computers within Active Directory. Specify multiple filters with multiple options. Default computer filter: (&(primaryGroupID=515)(objectCategory=computer)).
`--add-pool-group`	String	Specifies one or more Active Directory groups, by entering the distinguished name (DN), to be assigned to pools for remote workstation management (eg, --pool-group 'CN=GroupPool1,CN=Users,DC=sample,DC=com' --pool-group 'CN=GroupPool2,CN=Users,DC=sample,DC=com'). By providing all the existing pools groups in the Cloud Access Connector settings would get replaced by the user specified ones. When running this command you need to run it with **adconfig**. Example: ***sudo ./cloud-access-connector adconfig --add-pool-group***.
`--internal-client-cidr`	String	The CIDR for PCoIP Clients that connect to remote workstations directly.
`--external-client-cidr`	String	The CIDR for PCoIP Clients that connect to remote workstations through the Security Gateway. If external CIDRs settings are set, internal settings must be explicitly set.
`--setup-docker-image`	String	Specifies the docker image to be used from the setup container. This is intended to be used for debugging purposes and is not recommended to be used without guidance from Teradici support. Usage without guidance could result in failed installations.
`--docker-registry`	String	This is an optional flag that enables users to specify the docker image registry that they want to use when installing or updating a Cloud Access Connector. If an option is not specified, the default registry ***docker.cloudsmith.io/teradici/cloud-access-connector*** will be used. This is intended to be used for debugging purposes and is not recommended to be used without guidance from Teradici support. Usage without guidance from Teradici could result in failed installations.

⚠ **Cloud Access Connector Upgrade and Diagnose Issues**

Several previous versions of Cloud Access Connector installers are no longer compatible with our latest infrastucture upgrades. When you run the update or diagnose commands with these older versions you may receive errors such as "*Error response from daemon: GET https://docker.cloudsmith.io/......: unauthorized*" for example. If this occurs you need to download the latest version of the Cloud Access Connector installer from here.

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 (MFA)

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.

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.

Firewall and Load Balancing Considerations

Cloud Access Manager and the Cloud Access Connector require certain ports to be open to enable connections between the Cloud Access Manager Service, Cloud Access Connector, Remote Workstations, as well as other components.

Ports and Component Connections

Component	Allow	Port/Protocol	Source/ Destination Component	Descriptions
Cloud Access Connector	Inbound	80 TCP	From administrative web browsers.	For accessing the Management Interface, redirects to port 443.
Cloud Access Connector	Inbound	443 TCP	From PCoIP Clients and administrative web browsers.	For users to negotiate connections to their remote workstations. For accessing the Management Interface for (legacy) management of Cloud Access Manager.
Cloud Access Connector	Outbound	443 TCP	To CAM Service, PCoIP Cloud License Server and to SumoLogic.	To sync AD information to the CAM service and call Cloud Access Manager APIs related to negotiating PCoIP sessions. To verify license activation code during the Cloud Access Connector installation. For log aggregation for support purposes.
Cloud Access Connector	Outbound	60443 TCP	To remote workstations.	Prepares PCoIP Agents for a new user session.
Cloud Access Connector	Inbound	4172 TCP/UDP	From PCoIP Clients.	For PCoIP Sessions with users that are outside of the corporate network.

Component	Allow	Port/Protocol	Source/ Destination Component	Descriptions
Cloud Access Connector	Outbound	4172 TCP/UDP	To remote workstations.	For PCoIP Sessions with users that are outside of the corporate network.
Cloud Access Connector	Outbound	636 TCP	To Domain Controllers.	To authenticate users, and query user and computer information.
Cloud Access Connector	Outbound	1812 UDP (This port is configurable)	To RADIUS Server.	For authentication against RADIUS Server.
Cloud Access Connector	Outbound	53 UDP	To DNS.	Domain name resolution.
PCoIP License Server	Inbound	7070 TCP (This port is configurable)	From remote workstations.	For license activation and verification from PCoIP Agent if the PCoIP License Server is used instead of the Cloud License Server.

Port and Component Notes:

- Port **80 TCP** can be blocked and is not required to be open if users all use port 443 instead.
- Port **443 TCP** is not required if the PCoIP License Server is used in place of the Cloud License Server.
- The RADIUS Server is optionally configured.
- See the PCoIP License Server guide for changing port and configuring TLS encryption.

For system diagrams detailing these ports and components, see What is Cloud Access Manager?

Cloud Access Manager Security and Privacy

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.

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.

Cloud Access Manager Multi-Factor Authentication

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.

Duo Authentication Version

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.

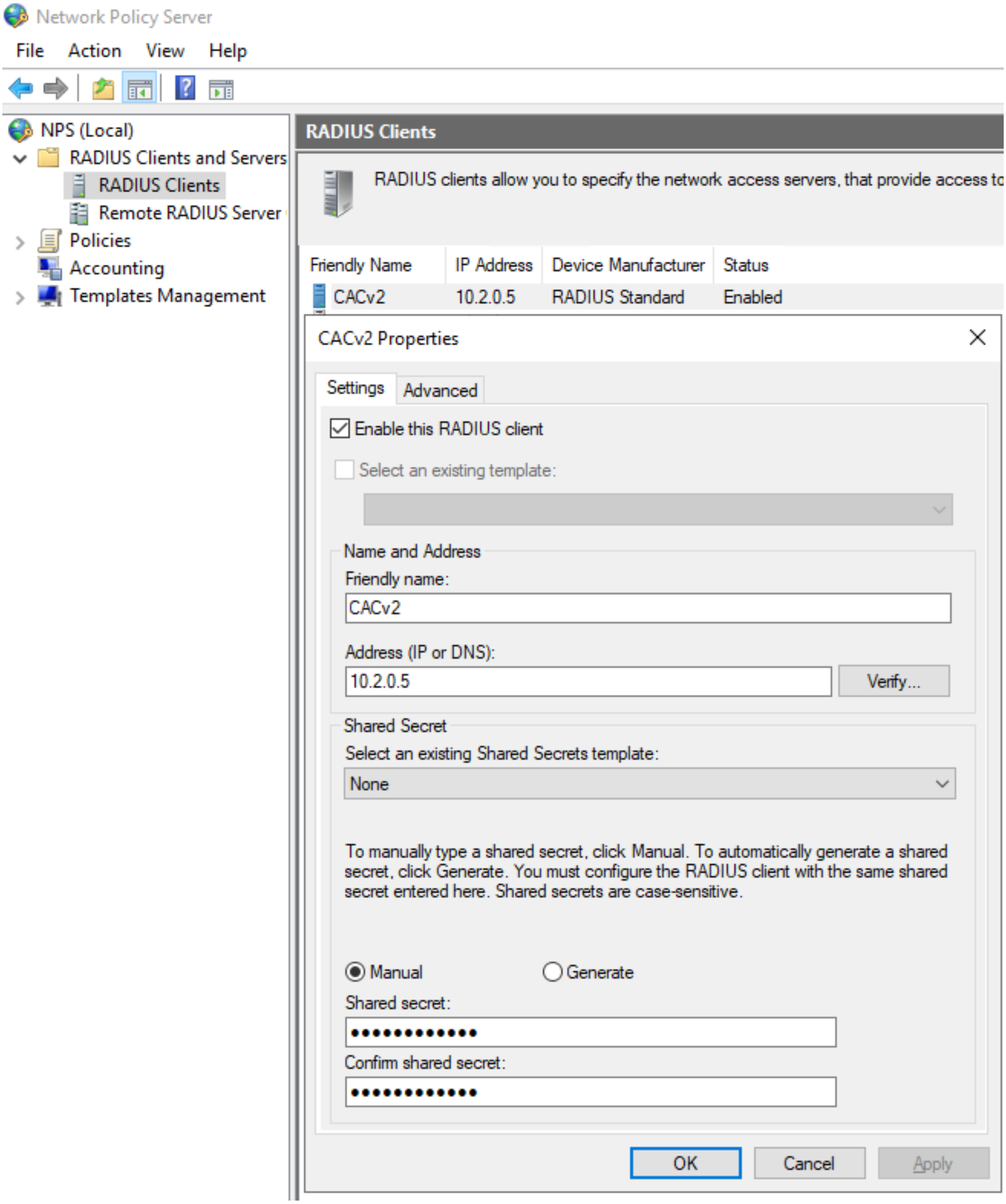
Azure MFA Configuration

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.
5. Install Network Policy and Access role on Windows Server 2016 or 2019.
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.

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**.



RADIUS clients allow you to specify the network access servers, that provide access to

Friendly Name	IP Address	Device Manufacturer	Status
CACv2	10.2.0.5	RADIUS Standard	Enabled

CACv2 Properties

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: CACv2

Address (IP or DNS): 10.2.0.5

Shared Secret

Select an existing Shared Secrets template: None

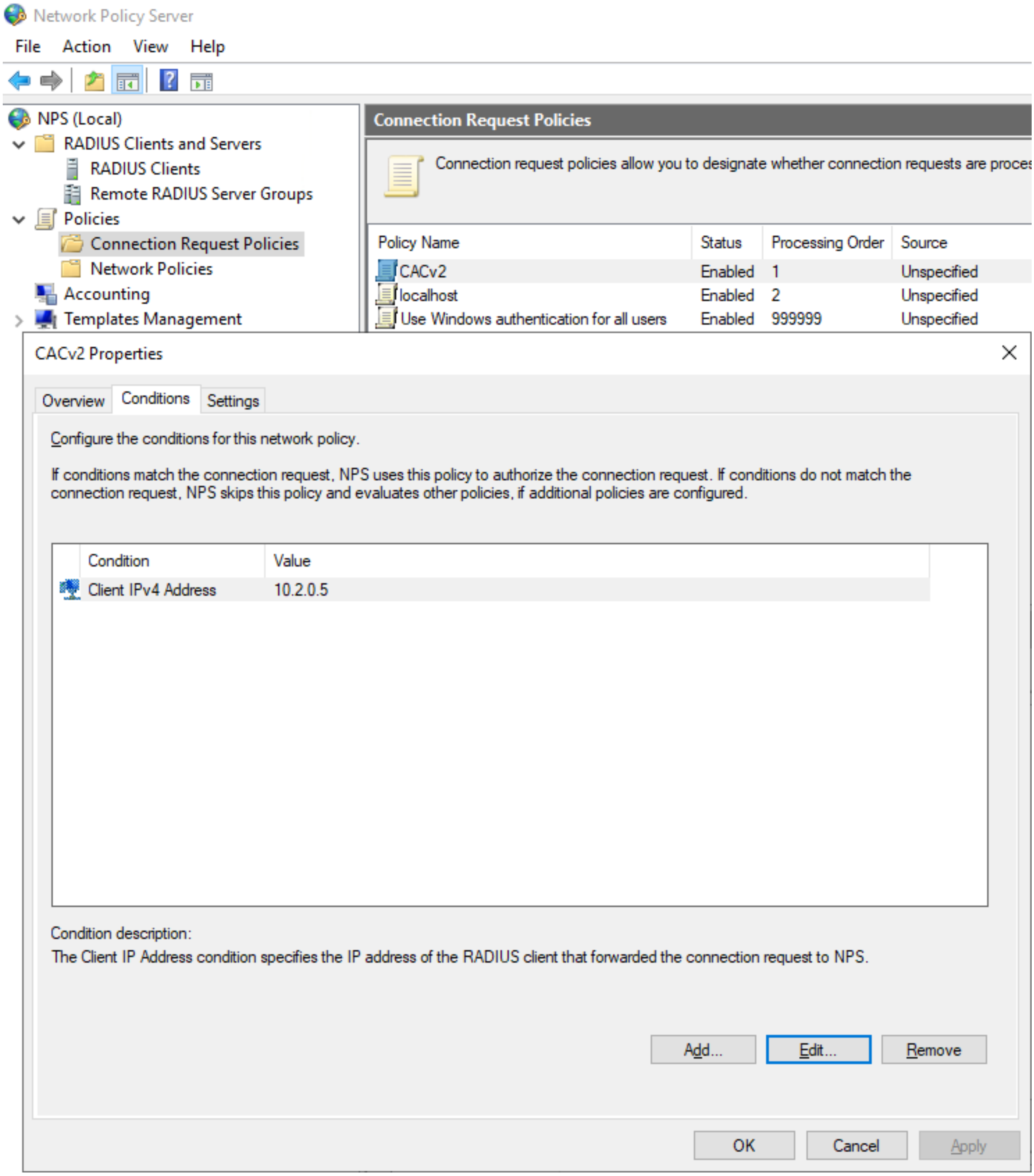
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••••••••

Confirm shared secret: ••••••••••••

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**.



Connection request policies allow you to designate whether connection requests are proces

Policy Name	Status	Processing Order	Source
CACv2	Enabled	1	Unspecified
localhost	Enabled	2	Unspecified
Use Windows authentication for all users	Enabled	999999	Unspecified

Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
Client IPv4 Address	10.2.0.5

Condition description:
The Client IP Address condition specifies the IP address of the RADIUS client that forwarded the connection request to NPS.

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
```

```
# 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
```

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:

```
# Running curl to cam should time out since the host should not be able to route to the internet
$ 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
$ 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>
```

```
</body>
</html>
$ export https_proxy=$http_proxy
$ curl https://cam.teradici.com
<!doctype html><html lang="en"><head><meta charset="utf-8"><meta
name="viewport" content="width=device-width,initial-scale=1,shrink-to-
fit=no"><meta name="theme-color" content="#000000"><link rel="manifest"
href="/manifest.json"><link rel="shortcut icon" href="/
favicon.ico"><title>Cloud Access Manager</title><link href="/static/css/main.
27391ea7.css" rel="stylesheet"></head><body><noscript>You need to enable
JavaScript to run this app.</noscript><div id="root" class="full-height"></
div><script type="text/javascript" src="/static/js/main.45a05db7.js"></
script></body></html>
# Clear the settings from the environment
$ unset http_proxy
$ unset https_proxy
```

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.

Specifing 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.

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:

```
$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
```

```
# 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`

> **PCoIP Agent Versions**
>
> PCoIP Agent versions 2.15 and earlier are 32-bit, and versions 19.05 and later are 64-bit.

The table below outlines the settings and defaults:

Type	Name	Default	Description
DWORD	*PollingIntervalMinutes*	15 minutes	Polling interval in minutes for checking the CPU utilization. Must be between 1 and 60.
DWORD	*MinutesIdleBeforeShutdown*	240 minutes	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.
DWORD	*CPUUtilizationLimit*	20%	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*.
DWORD	*EnableCAMDebug*	0	Additional debugging messages to the event log when this value is non-zero.

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:

```
AUTO_SHUTDOWN_IDLE_TIMER=<Desired-Idle-Time>
ENABLE_AUTO_SHUTDOWN=<true-or-false>
mkdir /tmp/idleShutdown
wget "https://raw.githubusercontent.com/teradici/deploy/master/remote-
workstations/new-agent-vm/Install-Idle-Shutdown.sh" -O /tmp/idleShutdown/Install-
Idle-Shutdown-raw.sh
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:

Location	Setting	Default	Description
/etc/systemd/system/CAMIdleShutdown.service.d/CAMIdleShutdown.conf	*MinutesIdleBeforeShutdown*	240 minutes	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.
/etc/systemd/system/CAMIdleShutdown.service.d/CAMIdleShutdown.conf	*CPUUtilizationLimit*	20%	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 *MinutesIdleBeforeShutdown*.
/etc/systemd/system/CAMIdleShutdown.timer.d/CAMIdleShutdown.conf	*OnUnitActiveSec*	15 minutes	Polling interval in minutes for checking the CPU utilization.

1. To apply any changes, you need to run the following command:

```
systemctl daemon-reload
```

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

```
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
```

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.

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 nescessary 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:

vCPUs	RAM	Estimated Bandwidth
2vCPU	7.5 GB RAM	~ 300 Mbit/s
4vCPU	15 GB RAM	~ 340 Mbit/s
8vCPU	30 GB RAM	~ 480 Mbit/s

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.

Licensing Options with Cloud Access Manager

With Cloud Access Manager, you can choose to put all your licenses into a single "cloud based" licensing pool or you can setup your own local PCoIP License Server if you require more advanced options.

How to Choose?

Use a Cloud License Server if you not need the advanced features of the local PCoIP License Server and do not want the overhead of deploying and managing the PCoIP License Server.

Use the PCoIP License Server if your use case includes one or more of the following advanced features or scenario's:

- Your remote workstations do not have access to the internet.
- You want to use an offline (dark site) activation process.
- You want to divide your license pool into multiple pools for multiple users.
- You want to actively track license usage.

Cloud License Server

This is a license server managed by Teradici that exists in the cloud. Users must obtain a license key for it and enter it into the Cloud Access Connector during the installation process. You must enter this key in the Cloud Access Manager Admin Console when creating a deployment.

PCoIP License Server

The PCoIP License Server is a standalone software application that runs on a Linux (RHEL or CentOS) machine, and handles both PCoIP session license registrations and PCoIP session request authorization. If you want to use the PCoIP License Server with Cloud Access Manager you need to have a PCoIP License Server activation code.

When a PCoIP Agent attempts to establish a new PCoIP session, it will request authorization from the assigned PCoIP License Server. The PCoIP License Server checks to see if an activated PCoIP session license is available in its trusted storage, and authorizes the session. Each PCoIP session activation consumes one PCoIP session license. For more information on the PCoIP License Server, see here.

⚠ **PCoIP License Server Activation Code**

In order to use Cloud Access Manager with the PCoIP License Server, you will require both a Cloud License Server registration code and a PCoIP License Server activation code. Contact support here to ensure you have both codes available.

You can enter in the FQDN or IP address into the Cloud Access Connector during the installation process using the `--local-license-server-url` flag.

Licensing Features

The following table outlines the features supported for both licensing types

Licensing Features Comparison

Features	Cloud License Server	PCoIP License Server
Online activation supported?	Yes	Yes
Offline (Dark site) activation supported?	No	Yes
Internet proxy supported?	Yes	Yes
High Availability options available?	No	Yes
Ability to track license usage?	No	Yes

For more information on Licensing with Teradici, see here.

Using Cloud Licensing with Cloud Access Manager

If you are using Cloud Access Manager you will need a PCoIP registration code (format: XXXXX@YYYY-YYYY-YYYY-YYYY)

A PCoIP Agent configured for a cloud license server will continue to use the cloud license server even if the PCoIP License Server has been configured in the Cloud Access Connector.

Installation Steps

- When installing the Cloud Access Connector, use your registration code to register with the Teradici licensing system. For more information on installing the Cloud Access Connector, see here.

All PCoIP connections will check the Cloud Licensing service prior to enabling a connection. You will be limited to the amount of sessions you have configured, for example if you are configured to have 5 concurrent sessions, the licensing system will limit you to 5 sessions. If you require more connections, you can scale up or down the cloud-based licensing pool by purchasing additional cloud-based licenses.

Using a PCoIP License Server with Cloud Access Manager

If you have chosen to use a PCoIP License Server, you will need:

- PCoIP registration code
- Activation code(s)

> **Activation and PCoIP Registration Code**
>
> In order to use Cloud Access Manager with the PCoIP License Server, you will require both a Cloud License Server registration code and a PCoIP License Server activation code. Contact support here to ensure you have both codes available.

Installation Steps

1. Install a local PCoIP License Server in your environment. For more information on this, see here.
2. Activate the licenses using your activation codes.
3. Once the PCoIP License Server has been installed, record your FQDN or IP address of the PCoIP License Server.
4. Install the Cloud Access Connector(s), use your registration code to register with the Teradici licensing system. In addition, you will need to enter the FQDN or IP address obtain in the

previous step by entering the `--local-license-server-url` flag at installation. This is an optional flag, so if you do not provide it then the installer will not ask for it.

For more information on installing the Cloud Access Connecter, see here.

All PCoIP connections will check your PCoIP License server prior to enabling a connection. You will be limited to the amount of sessions you have configured, for example if you are configured to have 5 concurrent sessions, the licensing system will limit you to 5 sessions. If you require more connections, you can scale up or down by purchasing additional PCoIP License Server licenses. For each license you purhcase you will receive an activation code. You will be required to manually install these on your PCoIP License Server. It is possible to have licenses both in the cloud and on your local PCoIP License Server. The system will always check the cloud license system first and if there are no available licenses, it will then check with the PCoIP License Server.

Licensing Requirements with Cloud Access Manager

- Cloud Access Manager requires a Cloud License Server registration code to be entered in the Cloud Access Manager Admin Console when creating a deployment.
- The user can install the PCoIP License Server URL directly into the Cloud Access Connector during installation.
- Any remote workstations provisioned by Cloud Access Manager will need to use the Cloud License Server for licensing purposes.
- Any remote workstation without a Cloud License Server license already installed, will need to use the PCoIP License Server URL from the Cloud Access Connector to obtain a license.

Licensing Priority Levels

Licenses will be acquired based on the following priority levels:

- PCoIP License Server address setting from GPO.
- Cloud License Server.
- PCoIP License Server address from the PCoIP Connection Manager.

These priority levels come from the PCoIP Agent, Please check the PCoIP Agent documentation for changes or updates:

- PCoIP Standard Agent for Windows

- PCoIP Standard Agent for Linux
- PCoIP Graphics Agent for Windows
- PCoIP Graphics Agent for Linux

Cloud Access Manager Maintenance

The following page outlines how to perform updates to the OS, Cloud Access Connector(s) and how to clean up unnecessary disk space.

OS Updates

The Cloud Access Connector can run on Ubuntu 18.04. Updates for the OS are pushed for installed packages frequently. In order to ensure the OS is as secure and up to-date as possible, it is important to run OS updates regularly by running the following command:

```
apt update
apt upgrade -y
```

Cloud Access Connector Updates

The Cloud Access Connector needs to be updated as new features are added and/or security updates are required. In order to ensure you are running the latest version of the Cloud Access Connector, it is important to run updates regularly. For more information on how to update the Cloud Access Connector, see here. Teradici recommends updating once a month. Updates can be carried out in place or by deploying a new Cloud Access Connector machine as part of a red-black deployment update.

Disk Space Updates

The Cloud Access Connector uses Docker to run and as a result you may encounter issues with disk space usage after some of the Docker containers have been updated with newer images. If this becomes an issue you can run the following Docker commands to clean up unused docker images that may have been previously downloaded for older versions of the Cloud Access Connector:

```
docker system prune
```

For more information on this, see https://docs.docker.com/config/pruning/.

Cloud Service Account Requirements

Cloud Access Manager's capabilites are enhanced if you provide service account or role 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.

Roles and Permission Policies - AWS

You can use the AWS Management Console to create a role which Cloud Access Manager is able to assume. For more information on creating roles in AWS, see here. You must use the Account ID and External ID that can be generated from the Cloud Access Manager Admin Console, for information on how to generate these credentials, see here.

AWS Permissions Policies

Once you have created the role in the AWS Management Console you can create and assign a permissions policy that contains the following permissions:

- **Service:** EC2
- **Actions:**
  - List: ***DescribeInstances***
  - Write: ***RebootInstances StartInstances StopInstances TerminateInstances***

There are additional permissions needed to verify that the role has all the required permissions before being added to a deployment:

- Actions
  - List: ***ListAttachedRolePolicies ListRolePolicies***
  - Read: ***GetPolicy GetPolicyVersion GetRolePolicy***

If the user tries to add an AWS role that doesn't have these permissions, Cloud Access Manager will still add the role but will not validate that it has the required permissions.

Service Account Permission Requirements - 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.

Service Account Permission Requirements - GCP

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

Default Roles	Workstation Provisioning	Power Management
Deployment Manager Editor	Required	—
Compute Admin	Required	Required
Cloud KMS Admin	Required	—
Cloud KMS CryptoKey Encrypter/Decrypter	Required	—

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

> **Key File Storage**
>
> Cloud Access Manager does not store the key file provided and only extracts the fields that are entered into the dialog.

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

Creating a Cloud IAM Custom Role

Users can create a single custom IAM role by using the following permissions for Cloud Access Manager:

- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.create
- cloudkms.cryptoKeys.get
- cloudkms.keyRings.create
- cloudkms.keyRings.get
- compute.acceleratorTypes.list
- compute.addresses.create

- compute.addresses.delete
- compute.diskTypes.list
- compute.disks.list
- compute.images.list
- compute.instances.create
- compute.instances.delete
- compute.instances.get
- compute.instances.getGuestAttributes
- compute.instances.osLogin
- compute.instances.reset
- compute.instances.setMetadata
- compute.instances.setServiceAccount
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.suspend
- compute.instances.update
- compute.instances.updateNetworkInterface
- compute.instances.use
- compute.machineTypes.list
- compute.networks.create
- compute.networks.list
- compute.regions.list
- compute.subnetworks.list
- compute.zones.get
- compute.zones.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete

- deploymentmanager.deployments.get
- deploymentmanager.resources.list
- resourcemanager.projects.get

Using these permissions you can create a custom IAM role. If you use this single custom role you do not need to use other default roles discussed above. For information how to do this, see Creating and managing custom roles.

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

Feature	Azure (CACv1)	Azure	GCP	AWS	ESX
Deallocation*	Supported	Supported	Not Applicable	Not Applicable	Not Applicable
Power Management	Supported	Supported	Supported	Supported	Not Supported
Workstation Provisioning	Supported	Not Supported	Supported	Not Supported	Not Supported

*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.

Configuring the Active Directory

Teradici recommends having a single AD configuration for a single deployment, which means all Cloud Access Connectors within that deployment should be configured to the same AD. If you want to have multiple Cloud Access 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.

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. This 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:

Flag	Type	Description
`--users-dn`	String	The base DN to search for users within Active Directory. This option may be specified multiple times to provide multiple DNs.
`--computers-dn`	String	The base DN to search for computers within Active Directory. This option may be specified multiple times to provide multiple DNs.
`--sync-interval`	String	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.

Flag	Type	Description
`--users-filter`	String	The filter to search for users within Active Directory. Specify multiple filters with multiple options. Default user filter: (&(objectCategory=person)(objectClass=user)). An example for a user group filter: (&(objectCategory=person)(objectClass=user)(memberOf: 1.2.840.113556.1.4.1941:=CN=PCoIP Users Group,CN=Users,DC=example,DC=com)).
`--computers-filter`	String	The filter to search for computers within Active Directory. Specify multiple filters with multiple options. Default computer filter: (&(primaryGroupID=515)(objectCategory=computer)).

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.

Configuring Active Directory Pool Groups

A set of command line flags enables users to update Active Directory pool groups. These flags apply changes to the Active Directory settings of the Cloud Access Connector.

By providing the following flags the appropriate update gets applied to the Cloud Access Connector settings. If no command-line option is provided, the Cloud Access Connector will display all available options for this operation.

Flag	Type	Description
`--cam-insecure`	String	Skips certificate validation when connecting to Cloud Access Manager. This option should only be used when connecting to Cloud Access Manager deployed with self-signed certificates.

Flag	Type	Description
`--add-pool-group`	String	Adds specified Active Directory group to the existing pool group settings. By providing all the existing pools groups in the Cloud Access Connector, settings would get replaced by the user specified ones.
`--remove-pool-group`	String	Removes specified pool Active Directory group by its DN.
`--clear-pools-groups`	String	Clears all pools Active Directory groups. This operation is exclusive and cannot be combined with `--remove-pool-group` or `--add-pool-group` .
`--get-cam-settings`	String	Prints all Cloud Access Manager settings to Cloud Access Manager Admin console.

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.

Organisational Unit [OU] Permissions Dialog

Permissions are being assigned to the service account through the OU permissions dialog.

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**.

Cloud Access Manager Account Ownership

Cloud Access Manager accounts have a single account owner, and one or more administrators who have the ability to authenticate to the Cloud Access Manager Admin Console and manage Cloud Access Manager deployments and services. The account owner is any user who is able to sign in with a supported identity provider and provide a PCoIP registration code. The following are some important points around the Cloud Access Manager account owner:

- If the account owner password is lost it can only be recovered through the identity provider. Teradici does not store any of the passwords. It is the customer's responsibility to maintain access to their account owner's password and if necessary securely store the account information.
- As the account owner account is provided by an identity provider such as Google or Microsoft, Teradici does not have the ability to recover account owner's account and is unable to transfer data to a new account if there is no access to the old account.
- Teradici can transfer a Cloud Access Manager account to another account owner provided the old and new owner accounts are accessible by the system administrator. In order to perform an account transfer see below.
- Both Microsoft and Google support transferring accounts from one organization to another. The process for doing this differs between the providers and in order to initiate this account transfer the user must work with the indentity provider in question. Once the account has been transferred through the identity provider, the user will be able access Cloud Access Manager but they will not see any of their old data as Cloud Access Manager recognized this as a different account.

Account Ownership Transfers

- If a Cloud Access Manager account needs to be transferred to a different account, the owner will need to open a support case and upon request from Teradici, provide the following information:
    - **Cloud Access Manager Authorization token from the old account:** This needs to be provided by the user.

    - **Cloud Access Manager Authorization token from the new account:** This needs to be provided by the user.
    - **Cloud Access Manager Authorization token from Cloud Access Manager support :** This needs to be provided by Teradici Global Support Services group.

For information on how to obtain a Cloud Access Manager authorization token from the Cloud Access Manager Admin Console, see here.

All the tokens are acquired by authenticating the identity provider and as a result must have specific permissions in order to succeed.

The two general use-cases for requiring an account ownership transfer are:

Owner account is disabled and access to the old account is possible

In the scenario where the account owner leaves the organization and their account is permanently disabled but it is possible to access the old account, an account transfer can be undertaken. The following steps need to be followed:

1. The user's IT organization needs to reactivate the account and sign into Cloud Access Manager Admin Console.
2. Create a support ticket. See here for information on creating a support ticket with Teradici.
3. Provide an authorization token from the old account.
4. Provide an authorization token from the new account. Cloud Access Manager operations uses the above information to migrate the accounts.
5. Disable the old account once more.

Owner account is disabled and access to the old account is not possible

In the scenario where the account is permanently disabled and access to old account is not possible then there is no way to validate the authenticity of the request and requester. An account transfer cannot be completed.

Performing an Account Ownership Transfer

The following steps outline how to transfer a Cloud Access Manager user account:

1. Sign into the Cloud Access Manager Admin Console with the old account.
2. Click the user account icon and click on the **Get API token**.
3. Copy the token and sign out of the Cloud Access Manager Admin Console.
4. Do the same process with the new account and copy the token again.
5. Send the old account and new account tokens to Teradici and the transfer needs to be processed within 2 hours of receiving the tokens.

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 Connector Connectivity Issues

Cloud Access Manager provides some diagnosic checks that can be used to troubleshoot the cause of issues you may be experiencing with your Cloud Access Connector. Run the following command:

```
cd /usr/sbin
sudo ./cloud-access-connector diagnose
```

Please note that older installs and updates may still be in the legacy directory at `~/v2connector` .

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:

Flag	Description
`--rw`	The Remote Workstation FQDN
`--ad`	Verify connectivity to currently configured Active Directory server
`-h` `--help`	help for diagnose
`--debug`	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.

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.

⚠ **Cloud Access Connector Upgrade and Diagnose Issues**

Several previous versions of Cloud Access Connector installers are no longer compatible with our latest infrastucture upgrades. When you run the update or diagnose commands with these older versions you may receive errors such as "*Error response from daemon: GET https://docker.cloudsmith.io/......: unauthorized*" for example. If this occurs you need to download the latest version of the Cloud Access Connector installer from 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:

```
sudo ./cloud-access-connector diagnose --rw fqdn.of.my.rw
```

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 occured 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 occured 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.

Viewing Logs from the Cloud Access Connector

The following section outlines how to view 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 installer and update logs are saved for the installer 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