What is CAS Manager as a Service?

CAS Manager is a Teradici management plane enabling users to configure, manage and monitor brokering of remote workstations. CAS Manager enables highly-scalable and cost-effective Cloud Access Software deployments by managing cloud compute costs by brokering PCoIP connections to remote Windows or Linux workstations.

CAS Manager as a Service is a service that is managed by Teradici that enables CAS users to securely access the cloud-based version of CAS Manager. CAS Manager as a Service also requires an external component called CAS Connector that resides in the users environment. Connector is a access hub that facilitates PCoIP connections to remote desktops and workstations by providing user authentication, entitlement and security gateway services. In all deployment environments, CAS Manager as a Service interacts seamlessly with Connectors to access and manage your remote desktops and workstations.

Once CAS Manager as a Service has been enabled, all configurations and deployment management will be carried out in the Admin Console.

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

---

**CAS Manager as a Service and 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 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 CAS Manager as a Service. This guide provides instructions on how to enable and activate CAS Manager as a Service'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 CAS Manager as a Service.

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

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

**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 CAS Manager as a Service, 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.

**CAS 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 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
Connectors. You cannot configure multiple 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.

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/.

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

For information on the system requirements for the Connector, see the System Requirements section in the CAS Manager guide.

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

Admin Console

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

<table>
<thead>
<tr>
<th>Cloud Identity Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Gmail accounts are not supported by default and need to be whitelisted by Teradici before being used. For access to CAS Manager as a Service with a personal Gmail account, contact Teradici sales or open a support case.</td>
</tr>
</tbody>
</table>

Remote Workstations and Workstation users

- Active Directory permissions set to List contents and Read all properties. If you do not set these permissions you will be unable to connect to specific remote workstations.

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 Connector requires certain external connections and sites to be available to enable the Connector to function properly. The following table outlines the sites that need to be whitelisted and should be available to access:

<table>
<thead>
<tr>
<th>Description</th>
<th>Destination</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Apt Rep for Ubuntu 18.04.</td>
<td>security.ubuntu.com</td>
<td>TCP</td>
<td>80</td>
</tr>
<tr>
<td>Source for first-party Ubuntu packages; required so that the OS on the Connector remote workstation can be kept up to date. This address is location dependent, so for example, if you are in the USA, it would be us.archive.ubuntu.com, or if you were in Canada it would be ca.archive.ubuntu.com.</td>
<td>*.archive.ubuntu.com</td>
<td>TCP</td>
<td>80</td>
</tr>
<tr>
<td>This is CAS Manager as a Service. It is required for both API usage, and to access the Admin Console.</td>
<td>cas.teradici.com</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>Source for Connector components, configuration files and the Cloud Access Connector installer. It is required in order for the Connector to be installed, configured and updated over time.</td>
<td>dl.teradici.com</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>Description</td>
<td>Destination</td>
<td>Protocol</td>
<td>Port</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>This is used by the installer to download docker containers used by the Connector that are developed and maintained by Teradici.</td>
<td>docker.cloudsmith.io</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>This domain is used by the installer for licensing and validating the registration code. It is the operations website for Flexera.</td>
<td>teradici.compliance.flexnetoperations.com</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>Source for Docker. It is required so that Docker can be installed to run the Connector.</td>
<td>download.docker.com</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>This site is used to download the public docker containers. These are not maintained by Teradici.</td>
<td>hub.docker.com</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>This is a public docker repo.</td>
<td>registry-1.docker.io</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>This is a public docker repo.</td>
<td>production.cloudflare.docker.com</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>SumoLogic log collection. Logs from the Connector components are sent to SumoLogic. For sumologic, multiple FQDNs may need to be whitelisted, see <a href="https://help.sumologic.com/APIs/General-API-Information/Sumo-Logic-Endpoints-and-Firewall-Security">https://help.sumologic.com/APIs/General-API-Information/Sumo-Logic-Endpoints-and-Firewall-Security</a> for full list. For more details on the information we collect, and how we collect it, please see the CAS Manager as a Service Privacy Policy.</td>
<td>*.sumologic.com</td>
<td>TCP</td>
<td>443</td>
</tr>
</tbody>
</table>

*These URLs are location dependent.*

---

**Whitelisting IP Addresses**

If you are still having issues with installation after whitelisting all the required sites and domains, try to resolve the failing sites by resolving the associated IP addresses. You can also try whitelisting these IPs in your firewall.
The 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 Admin Console also. The Admin Console works with both CAS Manager, and CAS Manager as a Service.

The diagram below outlines a connection workflow for a cloud deployment using the Admin Console with CAS Manager as a Service.
Connecting to the Admin Console

The following section outlines how to access and connect to the Admin Console for CAS Manager, and CAS Manager as a Service.

Connecting to CAS Manager

Once you have unlocked the Admin Console, open a web browser and go to https://public-or-private-ip-address-of-cas-manager to login with the default "adminUser". If you have configured multi-admin support, login with your enterprise identity provider account that has the required admin permission for CAS Manager.

Connecting to CAS Manager as a Service

Go to the Admin Console login page and log in with your Enterprise Microsoft Azure account, or if you are logging in through Google, a G Suite or Cloud Identity account. Enter your credentials to access the Admin Console. If you want to log in using Microsoft Azure, you must have consent to access the Teradici Azure application. Depending on your restrictions, a user or a system administrator could grant this access. For information on how to grant admin consent, see Grant tenant-wide admin consent to an application on the Microsoft site.

---

Email Account Support with CAS Manager

CAS 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 CAS Manager with a personal Gmail account, contact Teradici support. CAS Manager as a Service does not support Microsoft personal email accounts.
If you encounter issues logging into the 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://cas.teradici.com/.
- Pop-ups have been blocked on https://cas.teradici.com/.

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

Once you log into the 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 Connectors, add remote workstations as well as provide links to useful information within the CAS Manager documentation.

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

Configuring the 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 Admin Console.
Managing Deployments

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

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

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 PCoIP registration code. Please store this code in a secure location as it cannot be retrieved later.
   - Click CREATE.

The deployment has now been created and you can edit the deployment by configuring deployment service accounts, cloud service accounts and Connector settings.

Cloud Service Accounts

You can now enter cloud service account credentials for AWS, Azure and GCP if you are working in those environments and want to enable CAS 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 CAS Manager as a Service 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 CAS Manager as a Service and users can still be entitled to the remote workstation and start a PCoIP session, but CAS Manager as a Service 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 Connectors against different Domain Controllers within the same deployment. This will cause the Connectors to crash.
AWS Cloud Credentials

The following sections outline how to manage and configure AWS cloud information for CAS Manager and CAS Manager as a Service. Please note the permissions required for CAS Manager as a Service are different to the permissions for CAS Manager.

AWS Cloud Credentials for CAS Manager

To configure AWS Cloud Credentials for CAS Manager, see the AWS Configuration section of the CAS Manager Admin guide.

AWS Cloud Credentials for CAS Manager as a Service

Through the Admin Console you can generate a CAS Manager Account ID and External ID that can be used when creating an AWS role through the AWS Management Console. The following steps outline how to generate a CAS Manager Account ID and External ID:

1. In the Admin Console select the deployment you wish to use.
2. Click Edit Deployment.
3. Click Cloud Service Accounts.
4. Select AWS and click Generate. Ensure you copy the CAS Manager Account ID and External ID and save them to your clipboard.

⚠️ AWS Role Creation and Permission Policy

You must create a role in your AWS account which CAS Manager as a Service 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.

Once you have entered the CAS Manager Account ID and External ID and created the AWS role, you will need to create a permissions policy for CAS Manager as a Service 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**:
  - Read: GetUser SimulatePrincipalPolicy

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

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:RebootInstances",
        "ec2:DescribeInstances",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "iam:GetUser",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

If the user tries to add an AWS role that doesn't have these permissions, CAS Manager as a Service 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.

1. Once you have created the role in AWS, copy and paste the role ARN and enter it into the Role ARN field in the Admin Console.

2. Click **Submit**.

For information on the AWS Service Account roles and permission policies with CAS Manager as a Service, 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.

⚠️ 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 CAS 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.

For more information on GCP Cloud Service Accounts with CAS 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 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 menu 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 associated with this deployment.
Editing a Cloud Access Connector

Once you have created a Connector you can edit its name by clicking on the 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 Connectors by name by using the search bar in the table toolbar.

Enter the new name and click Save.

Domain Controller Certificates

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

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

Cloud Access Connector - Troubleshooting

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

• Remote Workstation connections
• Active Directory connections
• Cloud Access Connector component information

For information on installer errors related to a change in the distribution system, see here.
The following section outlines how to provision a remote workstation using the Admin Console.

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. The following steps outline how to provision a remote workstation:

1. Click Workstations from the Admin Console sidebar.

2. Click Create new remote workstation from the add remote workstation icon.

3. Select an existing Connector from the dropdown menu.

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

![Remote Workstations > Create Remote Workstation](image)

- **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
  - Disk type: SSD Persistent Disk
  - Disk size (GB): 50
  - Number of GPUs: 1

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

7. Once you have entered all required information, click **CREATE**.

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

---

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

**Remote Workstation Machine Name**
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.
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 CAS Manager. The remote workstation is joined to the active directory domain configured in the 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.
Workstation Pools

You can create workstation pools within the CAS 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.

A floating pool is a remote workstation pool that uses a floating workstation assignment policy. With this pool, a user is entitled to a pool and its remote workstations rather than a single remote workstation. When a user is assigned a remote workstation, this assignment is ephemeral. Once the user disconnects from the remote workstation there is a holding time where it will still be assigned to that user. This holding time can be configured by an admin user. Once this holding period expires, the user is unassigned to the remote workstation and it is added back to the pool and is available for re-assignment.

Once you log in to the CAS Manager Admin Console, you are automatically assigned a remote workstation within the pool, depending on the assignment policy of the pool. When creating a remote workstation pool, the assignment policy can be selected.

Use Cases for Floating Workstation Assignment Policy

The following section outlines potential use cases for the floating workstation assignment policy:

Two user’s and two Windows workstations

- User 1 attempts to log in with a PCoIP Client.
- Windows workstation 1 is successfully assigned to User 1.
- User 2 attempts to log in with a PCoIP Client.
- Windows workstation 2 is successfully assigned to User 2.

Two user’s and a single Windows workstation

- User 1 attempts to log in with a PCoIP Client.
- Windows workstation 1 is successfully assigned to User 1.
- User 1 closes the PCoIP Client.
User 2 then attempts to log in and is presented with an error message stating "Resource does not exist in CAM Service".

User 2 attempts to log in 25 minutes later. The assignment holding time for this example is 20 minutes, which is the default minimum assignment holding.

Windows workstation 1 is successfully assigned to User 2. The Windows session is taken over by User 2.

These use cases also apply for RHEL/CentOS workstations.

The following section outlines how to create a floating workstation pool from the CAS Manager Admin Console:

Creating a Workstation Pool

You can add multiple workstation pools to specific deployments. Each workstation pool will list the remote workstations, users and user groups within that pool. The following steps outline how to create a workstation pool, and choose the floating pool assignment policy:

1. Click on **Workstation Pools** from the CAS Manager Admin Console sidebar.
2. Click the + icon to create a new workstation pool.
3. Name the pool and choose the **Floating** option for the workstation assignment policy. The workstation assignment policy determines how workstations belonging to the workstation pool are assigned to users when they log in. This assignment policy can not be modified after the workstation pool has been created.
4. Enable **Session Tracking** by selecting the toggle.
5. Add the workstation holding time in minutes. Once this holding period expires, the user is unassigned to the remote workstation and it is added back to the pool and is available for re-assignment.
6. Name the pool and click **CREATE**.

There are two possible options for the workstation assignment policy:

**Persistent**: This is the default policy. Once a user logs in they are automatically and persistently assigned a remote workstation within the pool.
Floating: With the floating policy, once a user disconnects their PCoIP session, the remote workstation will be automatically unassigned from the user, and the remote workstation will become available for other users to connect to.

Adding Remote Workstations to a Workstation Pool

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 CAS Manager. The following steps outline how to add remote workstations to a workstation pool:

1. Click on **Workstation Pools** from the CAS Manager Admin Console sidebar.
2. Select the workstation pool you created in the previous section to display the edit pools page.
3. Click **Add Remote Workstations** and add remote workstations to the pool.

Adding Users to a Workstation Pool

Only specified users can establish PCoIP sessions to remote workstations in the workstation pool. If a remote workstation is available (not assigned to a user) it will be automatically assigned to the user. The following steps outline how to add users to a workstation pool:

1. Select the workstation pool and click **Add Users/Add Groups**.
2. Search for the users you want to add, select them and click **SAVE**.

Once users and remote workstations are added to the workstation pool, users from the workstation pool get available workstations upon log in. Once the PCoIP Session is disconnected, the remote workstation will become automatically available for future connections or continue to be assigned to the user depending on the workstation pool assignment policy.

Features and Known Limitations

There are certain limitations associated with this feature, as outlined in the following list:

- This feature is only supported in Connector(s) version 78 or higher.
• If all remote workstations have been assigned, and no remote workstations are available, users will see the following error during session establishment “Resource does not exist on CAM Service”.

• Remote workstations will remain assigned to a user for approximately 20 minutes after the PCoIP session has been disconnected by default. This time period is configurable through assignment holding time, and has to be longer than 20 minutes.

• The current limit is 200 remote workstations in a floating pool. The feature will work with a larger number of remote workstations, but the assignment timing may vary.

• **Limited support for Linux Agents**: When establishing a PCoIP session to Linux Agents, the session must be logged off before another user can connect. If the session is not logged off, the user will see a 6604 error message. To resolve this error reboot the remote workstation. This issue is being worked on.

• When connecting to a PCoIP Agent for Windows, if a previous user has been connected, the other user will see the Windows Switch Users screen. They will then be prompted to enter their credentials again before accessing the desktop.

**Auto Log-Off Service**

When a user disconnects their PCoIP session from a Linux PCoIP Agent, a different user is unable to connect unless the existing remote workstation user session is terminated. This will result in the remote workstation being locked, and unusable in a floating pool assignment, since a different user cannot log-in.

The auto log-off service enables you to bypass this issue by terminating a user session after the PCoIP session has been terminated. The auto log-off service monitors the `pcoip-server` process every minute. If it is not an active process then it samples the CPU load involved and if it is below a certain level for a certain amount of minutes, the script terminates the `pcoip-desktop-child` process which emulates a user logging off.

The auto log-off service disconnects a user if following criteria are met:

• No active PCoIP session detected (`pcoip-server` process is terminated).

• CPU utilization is less than 20% (`CPUUtilizationLimit`) for over 20 minutes (`MinutesIdleBeforeLogOff`).

• Sampling rate is 1 minute (`OnUnitActiveSec`).
Installing and Configuring the Auto Log-Off Service

You must have a CentOS/RHEL 7.8 virtual machine or Ubuntu virtual machine installed in order to run this service.

CentOS/RHEL Virtual Machine

- Run the following command to install the `pcoip-agent-autologoff` service on a CentOS/RHEL virtual machine:

  ```
  sudo yum install pcoip-agent-autologoff
  ```

Ubuntu Virtual Machine

- Run the following command to install the `pcoip-agent-autologoff` service on a Ubuntu virtual machine:

  ```
  sudo apt-get install pcoip-agent-autologoff
  ```

Once you have installed the service you can manage it via the `pcoip-agent-autologoff-mgmt` script. This script is located in `/opt/teradici/pcoip-agent-autologoff/pcoip-agent-autologoff-mgmt`.

The following table outlines the options you can use to manage the auto log-off service:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--enable</code></td>
<td>Enable the service.</td>
</tr>
<tr>
<td><code>--disable</code></td>
<td>Disable the service.</td>
</tr>
<tr>
<td><code>--change-params</code></td>
<td>Modify CPU utilization limit (CPUUtilizationLimit) and Idle time before logging off (MinutesIdleBeforeLogOff).</td>
</tr>
<tr>
<td><code>--change-timer</code></td>
<td>Modify polling interval (OnUnitActiveSec). This value sets how often the service runs.</td>
</tr>
<tr>
<td><code>--show-logs</code></td>
<td>Shows last 100 log messages.</td>
</tr>
<tr>
<td><code>--follow-logs</code></td>
<td>Shows live log messages.</td>
</tr>
</tbody>
</table>
Enabling the Auto Log-Off Service

The default settings are shown in the table below. It is possible to modify these settings after the auto log-off service has been installed and configured:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MinutesIdleBeforeLogOff</td>
<td>20 minutes</td>
<td>Number of minutes the remote workstation must be considered idle before it logs a user off. The timer only starts when a user is not in PCoIP session.</td>
</tr>
<tr>
<td>CPUUtilizationLimit</td>
<td>20%</td>
<td>Value between 0 and 100 representing CPU utilization percentage. If average CPU utilization is below this value, the machine is considered idle, and will log-off if maintained for <code>MinutesIdleBeforeLogOff</code>.</td>
</tr>
<tr>
<td>OnUnitActiveSec</td>
<td>1 Minute</td>
<td>Polling interval in minutes for checking the CPU utilization.</td>
</tr>
</tbody>
</table>

Enabling the Auto Log-Off Service

The following section outlines how to enable the auto log-off service.

1. To enable the service run the following command:

   ```
   sudo pcoip-agent-autologoff-mgmt --enable
   ```

2. To disable the service run the following command:

   ```
   sudo pcoip-agent-autologoff-mgmt --disable
   ```

Updating the Auto Log-Off Service Configuration

The following section outlines how to update the auto log-off service configuration.

- Run the following command to change `MinutesIdleBeforeLogOff` or `CPUUtilizationLimit`:

© 2021 Teradici
Run the following command to change `OnUnitActiveSec`:

```
sudo pcoip-agent-autologoff-mgmt --change-params
```

# follow the prompt to apply changes to the service

Run the following command to change `OnUnitActiveSec`:

```
sudo pcoip-agent-autologoff-mgmt --change-timer
```

# follow the prompt to apply changes to the service

Run the following command to show the log history:

```
sudo pcoip-agent-autologoff-mgmt --show-logs
```

Run the following command to follow the logs:

```
sudo pcoip-agent-autologoff-mgmt --follow-logs
```

Run the following command to display help information:

```
sudo pcoip-agent-autologoff-mgmt --help
```
SAML Configuration with CAS Manager

What is SAML?

SAML stands for Security Assertion Markup Language (SAML) and is a standard which Identity Providers use to communicate authorization credentials to different Service Providers. This enables users to manage one set of credentials to authenticate with different services.

SAML enables federated login to several services by passing authorization credentials between services. A SAML flow has three main roles:

- **End User**: A user who is trying to access a service using federated login credentials
- **Identity Provider (IDP)**: An identity provider performs the authentication about the end users identity and sends the necessary data to the service provider along with any other access control data in the form of SAML Assertions. Popular examples are Azure Active Directory and Okta.
- **Service Provider (SP)**: A service provider is the system that requests authentication from an identity provider to authorize an end user. **CAS Manager plays the role of a SP**

SAML Assertions

SAML Assertions are XML documents that the IDP sends to a given SP to validate user authorization. There are three different types of SAML Assertions:

- **Authentication**: This assertion provides user identity and the time at which a user was authenticated and the method of authentication that was used.
- **Attribute**: This assertion passes the SAML attributes about the user to the service provider. There can be more than one attribute assertions in a SAML response.
- **Authorization**: This assertion is the decision that determines if the user was successfully authorized to access the service or not by the IDP. Most common causes of failed authorization are incorrect password and/or insufficient access to the service the end user tried to access.
CAS Manager Initiated SAML Authentication Flow

1. An end user wants to login to CAS Manager. The user uses the SSO link for CAS Manager.
2. CAS Manager requests the configured IDP for the SAML response for the user.
3. IDP requests the user to login and verifies credentials.
4. User logs in with the desired credentials to IDP.
5. The IDP now sends a SAML response to CAS Manager based on the user provided credentials.
6. CAS Manager validates the SAML response and **SAML Attribute Assertions for CAS Manager** received from the IDP, and then grants access to the end user.

**SAML Attribute Assertions for CAS Manager**

CAS Manager checks for the following attributes in the SAML response received from the configured IDP:

- **NameID**: CAS Manager verifies the NameID attribute, which is used to uniquely identify a user. The NameID value is typically a user's UPN or email.
- **Group Attributes**: CAS Manager can also verify a user's group membership from properties in the AttributeStatement of the SAML Assertion. The **Group attribute name** (configured in the **Allowed Groups** tab on the **Multi Admin Setting** page of the Admin Console) specifies the name of the Attribute where the groups are returned. The AttributeValue can match either a
Group ID or Group Name based on how an Allowed Group was created in the Multi-Admin Settings page.

CAS Manager will allow access to a user through a SAML configuration if the user is in the list of Allowed Admins in CAS Manager or the user is a member of one or more of the Allowed Groups in your IDP. Hence if you need to revoke a user’s access to CAS Manager through a SAML configuration, you will need to remove the user from the Allowed Admins list in CAS Manager and remove the user’s membership from any Allowed Groups through your IDP.

Configure CAS Manager as a SAML Service Provider to Enable Multi-Admin

The following section outlines the steps to setup and configure SAML for CAS Manager using the CAS Manager Admin Console:

1. From the account icon click Multi Admin Settings to create a new multi-admin configuration.
2. Register CAS Manager as a SP with your IDP. You can obtain the Assertion Consumer Service URL and Audience URL from the Configuration Info section. This information should be used to configure your IDP to recognize CAS Manager as a SP.
3. Configure CAS Manager to be able to connect to your IDP. Obtain the Identity Provider Login URL and Identity Provider Certificate from your IDP and configure the IDP Settings section accordingly. Alternatively you can also upload an IDP XML Metadata file in the IDP Settings section.
4. Enable Multi-Admin configuration to use configured IDP. Make sure that your configuration is enabled by toggling the switch at the bottom of the Configuration Info section and confirm that you see the Configuration is enabled message.
5. Configure CAS Manager Assertion Attributes:
   - To allow individual user as admin, go to the Allowed Admins section and add the UPN associated to that user. CAS manager validates the UPN against the NameId SAML assertion attribute in the SAML response received from the IDP.
   - To allow user groups. Go to the Allowed Groups section and configure the Group Attributes accordingly. This configures CAS Manager to validate the Group Name and/or Group ID SAML attribute assertions in the SAML response received from the IDP.
You can configure either Allowed Admins or Allowed Groups or both in the Multi-Admin Settings.

6. Allowed users can now access CAS Manager by opening the CAS Manager login page URL which is available in the Configuration Info section. Alternatively, users can also directly login via the IDP using the Direct login via identity provider URL also available on the Configuration Info section.

Configuration Information

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

- **CAS Manager login page**: A link to the page for multi-administrator login to the Admin Console. This is the SSO link used by the end user in Step 1 of SAML auth flow diagram

- **Direct login via identity provider**: An endpoint to which multi-admin sign-in requests can be sent. This is the login page for the configured IDP.

- **Assertion Consumer Service URL**: The callback URL provided to the IDP to which user information is sent once the IDP has authorized the user. This is the CAS Manager endpoint that the IDP sends the SAML response to in Step 5 of the SAML auth flow diagram

- **Audience URL**: The entity ID that the IDP can use to identify the Admin Console.

IDP Settings

This section contains IDP settings that can be updated to manage the SAML configuration within CAS Manager:

- **Identity Provider Login URL**: The IDP endpoint to which SAML authentication requests are sent. This endpoint is the one that CAS Manager sends the SAML login request to in Step 2 of SAML authentication flow diagram above.

- **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.
Allowed Admins

This section enables you to add new admins and displays all existing admins that are allowed to login via your IDP. To add a new admin, enter their e-mail, and click the Add Admin button.

Allowed Groups

This section enables you to add new groups and displays all existing groups that are allowed to login via your IDP. To enable the access for a group of users, enter the claim type and group claim and click Add Group.

- The claim type informs CAS Manager how the group is returned in the SAML attribute assertions in the SAML response received from your IDP.
- The group claim matches against the group either in the Group Name claim or in the Group ID claim received in the SAML attribute assertions for a user based on the claim type defined for the group.
Service Account and API Access

CAS Manager as a Service provides direct API access in the CAS Manager as a Service 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.

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

CAS Manager Service Accounts

The CAS Manager service account is an account that is created from the Admin Console for the purpose of creating future deployments and deployment service accounts through the CAS Manager as a Service APIs. The CAS Manager 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 CAS Manager 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 in the Account Ownership section of the CAS Manager as a Service guide.
Creating a CAS Manager Service Account

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

1. Click on your account name and select **CAS Manager service account**.
2. Click the + icon from the CAM service account page and name your new account.
3. Once you have created the CAS Manager 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 CAS Manager as a Service 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 CAS Manager as a Service Admin Console. The following steps outline how to add a deployment service account to an existing deployment:

1. Click on your deployment from the console dropdown to display your existing deployments.
2. Click the kebab icon and click **Edit deployment** to display the deployment properties page.
3. Under the **Deployment Service Accounts** tab click the + sign to create a service account.
4. Once the service account has been created it will return service account information. This information should be saved as a JSON file in a secure location, as it can only be retrieved once. It will return a CAS Manager as a Service API token that you can use to query the CAS Manager as a Service APIs. This token is only authorized to access resources associated to the deployment that service account is associated with.

All deployment service accounts associated with a specific deployment will be listed on the deployment page. You can delete deployment service accounts from this page. For information on using the deployment service accounts and deployment service keys with the CAS Manager as a Service APIs, see [here](https://cam.teradici.com/api/docs).
Obtaining a CAS Manager as a Service API Access Token

API access tokens permit you to enable other tools and applications to interact with CAS Manager as a Service 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 CAS Manager as a Service API Access token:

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

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

Teradici Advantage Partner Program

To access and use the CAS Manager as a Service 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.
Setting Time and Date

You can configure the time zone, time format and date format within the 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 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 Admin Console.
Activity Log

The CAS Manager activity log enables you to view a record of all activity and operations performed in your CAS 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 Admin Console:

1. Click the user account icon within the 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 occurred. You can download all the logs available in CAS Manager by clicking the **Download CSV** button. For information on CAS Manager levels and how they impact the activity log, see [CAS Manager](#).

### Activity Log Expiration Timeframe

The Activity Log in the 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 CAS Manager APIs

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

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

This section outlines beta features and enhancements that have not yet been pushed to the production version of the CAS Manager Admin Console. As a result, these features may change as they are developed, and they will not be supported by Teradici Global Support Services. Features in the beta version are considered not yet ready for full production and you use them at your own risk.

The following beta features for the CAS Manager Admin Console are currently documented:

- Azure Remote Workstation Provisioning
- Workstation Profiles

Once these features have been fully developed and moved to the production version of the CAS Manager Admin Console, they will be removed from this section and added to the main Administrators' guide.
Azure Remote Workstation Provisioning

⚠️ Beta Feature

Please be aware that the feature outlined below is only currently available in the beta version of the CAS Manager Admin Console. As such, this feature may change as it is developed, and it will not be supported by Teradici Global Support Services. Features in the beta version are considered not yet ready for full production and you use them at your own risk.

🔧 Pre-Defined Images and Templates

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

Users are now able to create and provision remote workstations in Azure in the beta version of the Admin Console. This beta feature is currently only supported with CAS Manager as a Service. This feature is currently at parity with GCP in terms of creating a remote workstation, add a remote workstation to a pool, entitling users to a pool, etc.

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. The following steps outline how to provision a remote workstation:

1. Click Workstations from the Admin Console sidebar.
2. Click Create new remote workstation from the add remote workstation icon.
3. Select **Azure** from the Provider menu.

4. Select an existing Connector from the Connector Information menu.

5. Select a remote workstation template from the Workstation Template menu.

6. Enter the provider properties for the Azure resource group, remote workstation location, Azure virtual network and Machine subnet.

   **Remote Workstation Location**
   
   The location of the remote workstation must match the location of the Azure resource group.

7. Enter the remote workstation properties from the Workstation Properties menu. Enter the machine name, Azure VM size, remote workstation username and remote workstation admin
password, as outlined below.

Create a new remote workstation

<table>
<thead>
<tr>
<th>SELECT PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider</td>
</tr>
<tr>
<td>✅ Azure</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONNECTOR INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a connector</td>
</tr>
<tr>
<td>test connector</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WORKSTATION TEMPLATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a remote workstation template</td>
</tr>
<tr>
<td>CentOS 7 Standard Agent - 20210701010219</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PROVIDER PROPERTIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the location of the remote workstation</td>
</tr>
<tr>
<td>(US) West US</td>
</tr>
<tr>
<td>Azure resource group</td>
</tr>
<tr>
<td>cloud-shell-storage-westus (westus)</td>
</tr>
<tr>
<td>Azure Virtual Network</td>
</tr>
<tr>
<td>Select Virtual Network</td>
</tr>
<tr>
<td>Machine Subnet</td>
</tr>
<tr>
<td>Virtual network required</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WORKSTATION PROPERTIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine name</td>
</tr>
<tr>
<td>TEST1</td>
</tr>
<tr>
<td>Select the size of the machine</td>
</tr>
<tr>
<td>Basic_A1</td>
</tr>
<tr>
<td>Remote Workstation username</td>
</tr>
<tr>
<td>testytest</td>
</tr>
<tr>
<td>Remote workstation admin password</td>
</tr>
<tr>
<td>*******</td>
</tr>
</tbody>
</table>

**Remote Workstation machine and user names**

Due to a Windows limitation, remote workstation machine names are limited to only characters, letters, hyphens and must be 15 characters or less. Remote workstation user names are limited to 20 characters or less and cannot end in a period. The password entered for a remote workstation must be between 6-72 characters long and satisfy at least 3 of the following password requirements:

- Contains an uppercase character.
- Contains a lowercase character.
- Contains a numeric digit.
- Contains a special character.
- Control characters are not allowed.

For information on the remote workstation name and password requirements for Azure, see the following FAQs:

- Windows Requirements
- Linux Requirements

**Machine Type GPU**

If you select a Graphics Agent from the remote workstation template, you must ensure that your machine type has an NVIDIA GPU. If the remote workstation does not have the correct GPU driver it will fail during the GPU driver installation phase and you will be unable to connect to your remote workstation.
8. Enter the active directory information for the remote workstation. The service account must have permission to join computers to the domain.

![Active Directory Information](image)

Active Directory information is used only during provisioning to join the remote workstation to the domain. This information will not be saved by the CAS Manager.

9. Click **Deploy**.
Workstation Profiles

⚠️ Beta Feature

Please be aware that the feature outlined below is only currently available in the beta version of the CAS Manager Admin Console. As such, this feature may change as it is developed, and it will not be supported by Teradici Global Support Services. Features in the beta version are considered not yet ready for full production and you use them at your own risk.

Workstation profiles logically group remote workstation provisioning information. Profiles define a set of workstation deployment settings that will be shared by any workstation deployed from this profile. This feature enables administrators to streamline deploying workstations and improves the experience of deploying a large number of identical remote workstations.

Creating a Workstation Profile

The following steps outlines how to create a workstation profile from the Admin Console. Once you have created a workstation profile, you can use it to deploy a remote workstation.

1. Click on **Workstation Profiles** from the Admin Console sidebar.
2. Click the + icon to create a new workstation profile.
3. Enter a unique name for the workstation profile.
4. Select the cloud provider you wish to use. Currently Azure and GCP are supported.
5. Select a remote workstation template. The remote workstation template defines the base OS and provisioning steps for the remote workstation you will deploy. The only required field is the
Resource template ID parameter.

6. Once you entered all the required information, click CREATE.

The workstation profile you created will now be visible in the list of workstation profiles. You can delete any workstation profiles from this view.

Deploying a Remote Workstation with a Workstation Profile

Once you have created a workstation profile you can use it to populate the Create Workstation page. The following steps outline how to use the workstation profile when creating a new remote workstation:

1. Click Workstations from the Admin Console sidebar.
2. Click **Create new remote workstation** from the add remote workstation icon.

3. Select the cloud provider you wish to use. This must be the same cloud provider you entered when you created the workstation profile.

4. From the **WORKSTATION PROFILE** tab select the workstation profile you created to auto-fill the page with the provider properties, workstation template and workstation properties.

5. If you chose Azure as your cloud provider, enter the remote workstation username and password.

6. Enter the Active Directory account and password. The Active Directory information is only used during provisioning to join the remote workstation to the domain. This information will not be saved by the CAS Manager or Admin Console.

7. Click **DEPLOY**.

The remote workstation has now been created and deployed and will be visible on the **Workstations** page. Using a specific workstation profile ensures that the identical information is used for all remote workstations created.

---

**Workstation profile checkbox**

If you deploy a remote workstation and do not use a workstation profile, you will be prompted by a message asking if you want to use this configuration as a workstation profile. You can select to not show this message again, but then you will not be prompted to create a workstation profile for future deployments.
Overview

The Connector is an access hub installed in the customer environment which facilitates PCoIP Client connections to remote workstations. It operates in conjunction with the Teradici CAS Manager to provide user authentication and entitlement for remote workstation access, including MFA. Connector is software that runs within an Ubuntu server and enables secure connectivity between users and the remote workstations by eliminating the need for a dedicated VPN by providing NAT services for external users.

The Connector enables CAS Manager to broker desktops or workstations located in AWS, Google Cloud, Microsoft Azure and on-premises environments. Based on customers' infrastructure, they may need more than one Connector. The Connector communicates with the CAS Manager which orchestrates and manages Cloud Access deployments.

You are required to have a valid registration code for Teradici Cloud Access Software to be able to successfully deploy CAS 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.
System Requirements

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

Creating the Connector Server

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

You need to create a dedicated Ubuntu server with the following specifications:

- Ubuntu Server 18.04.
- At least 4GB RAM.
- 30GB available storage or more.
- 2 vCPUs or more.

Once you have setup a dedicated virtual machine for the Connector, please ensure the following environment conditions are met:

- You must have access to the internet.
- You must have an Active Directory (AD) user account located in the designated Connector domain admins group, in order to log into the Admin Console.
- 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 Connector is operational.
- The server must have a single network interface and IP address. If the server has multiple network interfaces, the Connector will fail to install.
If you are deploying Ubuntu on ESXi, you must install open-vm-tools to enable the ESXi host to communicate with the Connector server.

The Connector runs on the following 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.

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

### Creating a DNS record

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

### Verifying the Connector Server

To verify your 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 Connector server might be misconfigured. For more information on DNS configuration, see Configuring Network Settings in Ubuntu 18.04.
Enabling Connections over WAN

If the 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 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 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 Connector has been installed, reboot the Connector server.
Multi-Factor Authentication

When you install the Connector you can specify whether the PCoIP session uses Multi-Factor Authentication (MFA) during authentication or not. The Connector can be integrated with your RADIUS server. To do this you will need to provide the following information during the 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 Connector, you can enable it later when performing an update, see Updating the Connector. For more information on Connector MFA, see Multi-Factor Authentication.
Active Directory Service Accounts

The following sections outline the Active Directory (AD) Service Account permissions required for installing the Connector. It also outlines the steps required to set these permissions.

Permissions Required to Install the Connector

There are no mandatory permissions required for the AD Service Account to install the Connector. You can optionally delegate the Reset user passwords and force password change at next logon task in the Delegation of Control Wizard panel. For steps on how to delegate the password reset task to the AD Service Account, see Permissions to Change and Reset Passwords.

Delegating this task will enable users to change and reset their passwords while connecting to the remote workstations. If this is not set, the user will receive an error.

Higher AD Service Account Permissions

If the user has a higher level of permissions than the AD Service Account, then you will experience password change errors even if the delegation is configured as outlined above.

Domain Controller Certificates

If all DC certificates have expired, the Connector will stop working. An error indicator will display on the Connectors page when a 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 Connector has a certificate that less than a week away from expiring. 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.

Permissions to Change and Reset Passwords

The following steps outline how to delegate the Reset user passwords and force password change at next logon task in the Delegation of Control Wizard:

1. Open the Active Directory Users and Computers application.
2. Select the user or group you want to delegate, and click Delegate Control.
3. Click Next.
4. Click Add and enter the username or group name that will be granted reset permission.
5. Click OK.
6. Click Next.
7. Select Delegate the following common tasks and select the Reset user passwords and force password change at next logon task.
8. Click Finish.

During Installation

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

• The AD Service Account username.
• The AD Service Account password.

Permissions Required to Provision Remote Workstations

Before provisioning a remote workstation you need to ensure that the AD Service Account is correctly configured. This should be a different AD Service Account to the account used when installing the Connector. The AD Service Account needs to have specific permissions, for information on these permissions and how to configure them, see Provisioning Remote Workstations.
Assigning an SSL Certificate

You can assign an SSL certificate to the Connector during installation. This will prevent certificate verification errors when connecting to the CAS Manager or CAS Manager as a Service 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 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 ‘casm.test.com’ for example, is registered to the public IP address of the application gateway.

When the 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 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 Connector and deleting the old one. For information on updating SSL certificates, see Updating Connector.
The following section outlines how to download and install the Connector. There are three steps involved in this process:

- Downloading the Connector installer files.
- Obtaining an authorization token.
- Installing the Connector.

**Prerequisite Steps**

For instructions and documentation on the Connector prerequisite steps, see [Connector System Requirements](#).

It is important to read and address all the prerequisites outlined.

**1. Downloading the Connector**

The following section outlines how to download the installer files for the Connector. First, connect to the machine and download the Connector files. The commands below will download the Connector archive, and extract it.

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

**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:

```bash
ssh <username>@<server-ip-address>
```
2. Download the installer from Teradici:
   
   • Open a web browser and navigate to the Downloads and Scripts tab on the Teradici support site.
   • 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/:

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

2. Obtaining the 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 Admin Console, see Admin Console Connection. The following section outlines how to obtain a Connector token using the Admin Console:

1. Click Connectors from the console sidebar.

2. Click the add connector button (± sign located beside the 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 in the private cloud install instructions panel.

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.
3. Installing the Connector

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

3.1 Installing the Connector for CAS Manager as a Service

Install the Connector for CAS Manager as a Service by running the following command:

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

Ensure that you use the options and flags that best suit your system architecture and requirements. If required values are not provided on the command line, you will be prompted for them. For additional flags and options, see Installation Flags and Options.
3.2 Installing the Connector for CAS Manager

Once you have downloaded the Connector installer and have obtained a Connector token, run the following command to install Connector to the CAS Manager instance you have just installed. The first line of this command maps the Connector token to a variable in the shell:

```bash
export token=<token from CAS Manager admin console>
sudo cloud-access-connector install \ 
  -t $token \ 
  --casm-url=https://ip-address-of-cas-manager \ 
  --external-pcoip-ip public.ipv4.clients.connect.to \ 
  --casm-insecure
```

- When you are installing the Connector for CAS Manager you need to ensure that you enable and specify the `--casm-url` flag. This flag specifies the CAS Manager URL that the Connector connects to. If it is not specified by default it will point to https://cas.teradici.com.

- The `--external-pcoip-ip` flag is highly recommended to use in order to explicitly set the public IP that PCoIP Clients will connect to during PCoIP sessions. This is the public IP that the Connector is listening to on port 4172. The installer will reach out to cas.teradici.com and first try to automatically resolve the external IP; if this fails, or is not able to resolve the correct IP, this flag is required. In the case that the Connector machine doesn't have an internet connection, for example in a dark site environment, or the ingress and egress internet traffic are running through different public IPs, this flag is required.

- The `--casm-insecure` flag is only required when the Connector is connecting to a CAS Manager that is using self-signed certificates. If CAS Manager is using trusted TLS certificates signed by a public CA, then users will not need to use the `--casm-insecure` command.

- The `--casm-ca-cert` flag can used to provide the PEM formatted public certificate for the private CA used to sign the CAS Manager certificate. This flag is useful if the Connector fails to fetch a certificate from the CAS Manager.

Ensure that you use the options and flags that best suit your system architecture and requirements. If required values are not provided on the command line, you will be prompted for them. For additional flags and options, see Installation Flags and Options.
Multi-Factor Authentication

When installing the Connector you can enable multi-factor authentication (MFA) by running the `--enable-mfa` flag. MFA will be disabled by default. If you want MFA to only apply to external connections, you should have separate Connectors. One Connector should be for external connections, where MFA is enabled, and one for internal or direct connections, where MFA is disabled. For steps on how to install the Connector with MFA bypassed for internal connections, see Installing the Connector for Internal Connections.

For external facing Connectors you should apply firewall and network settings, such as placing it in a DMZ for example. For external facing Connectors, ensure that you set `--external-client-cidr` to `0.0.0.0/0` so that everything through this Connector is treated as an external connection. It is not recommended to rely on the IP range to manage authentication levels, and for better security you should use separate Connectors.

Ensure that you use the options and flags that best suit your system architecture and requirements. If required values are not provided on the command line, you will be prompted for them. For additional flags and options, see Installation Flags and Options.

Installing the Connector for Internal Connections

The following steps outline how to install the Connector for internal connections to bypass MFA:

1. Prepare a virtual machine in your private network that meets the system requirements with the following sub-steps:
   - Skip the step for preparing the system for external access.
   - Skip the step for setting up MFA.

2. Install the Connector with the following sub-steps:
   - Do not set the Public IP using the `--external-pcoip-ip` flag. The Connector will instead return the virtual machines IP address.
   - No MFA flag is required as MFA is disabled by default.

3. Once you have installed the Connector connect to a remote workstation with a PCoIP Software Client with the following sub-step:
   - In the *Host Address or Code* field enter the private IP of the internal Connector you just installed and log-in.
If you want to use the same url for an external Connector as an internal Connector, for example connector.domain.com, you must set-up an internal/private DNS. In this DNS create an entry called connector.domain.com and map it to the private IP of the internal Connector. Users will then be able to connect to this entry by entering connector.domain.com in the **Host Address or Code** field in the PCoIP Client. The internal connection will connect to the internal Connector, and the external connection will connect to the external Connector.

**Installation Flags and Options**

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

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--casm-url</td>
<td>String</td>
<td>Required for CAS Manager, Specifies the CAS Manager URL that the Connector connects to. If this is not specified it will point to <a href="https://cas.teradici.com">https://cas.teradici.com</a> by default, which is the URL for CAS Manager as a Service.</td>
</tr>
<tr>
<td>--casm-ca-cert</td>
<td>String</td>
<td>Enables users to supply a CA certificate for CAS Manager to enable the Connector to connect to a CAS Manager instance using self-signed certificates.</td>
</tr>
<tr>
<td>--casm-insecure</td>
<td>String</td>
<td>Is required when the Connector is connecting to a CAS Manager instance that is using self-signed certificates. If CAS Manager is using trusted TLS certificates signed by a public CA, then users will not need to use the this command.</td>
</tr>
<tr>
<td>--ldaps-ca-cert</td>
<td>String</td>
<td>Enables users to supply a CA certificate for the connection to Active Directory over LDAPS.</td>
</tr>
<tr>
<td>--self-signed</td>
<td>String</td>
<td>Installs the Connector with self-signed certificates. This mode is not secure and is intended for testing. The --insecure flag is still supported.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--token (-t)</td>
<td>String</td>
<td>Required. The token generated for CAS Manager.</td>
</tr>
<tr>
<td>Flag</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>--accept-policies</td>
<td>String</td>
<td>Automatically accept the EULA and Privacy Policy.</td>
</tr>
<tr>
<td>--force-install</td>
<td>String</td>
<td>Replaces any existing Connector installation.</td>
</tr>
<tr>
<td>--debug</td>
<td>String</td>
<td>This flag can be run if you initial install of the Connector fails. It provides a detailed output of the Connector installation. This is useful for self-troubleshooting or to provide to the Teradici support team when logging a support ticket.</td>
</tr>
<tr>
<td>--local-license-server-url</td>
<td>String</td>
<td>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: <code>--local-license-server-url http://10.10.10.10:7070/request</code>. For more information on the PCoIP License Server, see PCoIP License Server.</td>
</tr>
<tr>
<td>--add-pool-group</td>
<td>String</td>
<td>Specifies one or more Active Directory groups, by entering the distinguished name (DN), to be assigned to pools for remote workstation management (eg, <code>--pool-group 'CN=GroupPool1,CN=Users,DC=sample,DC=com' --pool-group 'CN=GroupPool2,CN=Users,DC=sample,DC=com'</code>). By providing all the existing pools groups in the Connector settings would get replaced by the user specified ones. When running this command you need to run it with adconfig. Example: <code>sudo ./cloud-access-connector adconfig --add-pool-group</code>.</td>
</tr>
<tr>
<td>--setup-docker-image</td>
<td>String</td>
<td>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.</td>
</tr>
<tr>
<td>Flag</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>--docker-registry</td>
<td>String</td>
<td>This is an optional flag that enables users to specify the docker image registry that they want to use when installing or updating a Connector. If an option is not specified, the default registry <code>docker.cloudsmith.io/teradici/cloud-access-connector</code> 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.</td>
</tr>
<tr>
<td>--prune-image</td>
<td>Boolean</td>
<td>Removes all unused docker images on this machine to reclaim more disk space. <strong>Warning:</strong> This command will remove all unused images under Connector and other services, if any. This is equivalent to the <code>docker image prune</code> command.</td>
</tr>
</tbody>
</table>

**Firewall**

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--https-proxy</td>
<td>String</td>
<td>Specify the URL for a HTTPS proxy (overrides related proxy settings in environment variables)</td>
</tr>
<tr>
<td>--connector-network-cidr</td>
<td>String</td>
<td>This is the CIDR to use for the Connector’s docker network. The default docker network subnet is 10.101.0.0/16.</td>
</tr>
<tr>
<td>--internal-client-cidr</td>
<td>String</td>
<td>The CIDR for PCoIP Clients that connect to remote workstations directly. It is possible to specify multiple <code>--internal-client-cidr</code> networks.</td>
</tr>
<tr>
<td>--external-client-cidr</td>
<td>String</td>
<td>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. It is possible to specify multiple <code>--external-client-cidr</code> networks.</td>
</tr>
</tbody>
</table>

**PCoIP Software Client**
### Flag

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--retrieve-agent-state</td>
<td>Boolean</td>
<td>Enables the broker to retrieve the agent state for unmanaged and managed remote workstations. The default value for this flag is false. The available states are In Session, Ready, Starting, Stopping, Stopped and Unknown. The value of this flag can either be true or false.</td>
</tr>
<tr>
<td>--show-agent-state</td>
<td>Boolean</td>
<td>Controls if the agent state is displayed as part of the remote workstation name in the PCoIP Client. The default value for this flag is true. Setting the value of this flag to true and the --retrieve-agent-state flag to false will result in no agent state displaying.</td>
</tr>
<tr>
<td>--external-pcoip-ip</td>
<td>String</td>
<td>Sets the public IP for PCoIP Client to PCoIP Agent connection. This is the public IP that the Connector is listening to on port 4172. The installer will reach out to cas.teradici.com and first try to automatically resolve the external IP; if this fails, or is not able to resolve the correct IP, this flag is required. In the case that the Connector machine doesn't have an internet connection, for example in a dark site environment, or the ingress and egress internet traffic are running through different public IPs, this flag is required. For more information on external network access, see Enabling External Network Access.</td>
</tr>
</tbody>
</table>

### Domain

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--domain</td>
<td>String</td>
<td>The AD domain that remote workstations will join.</td>
</tr>
<tr>
<td>--sa-user</td>
<td>String</td>
<td>The Active Directory service account username.</td>
</tr>
<tr>
<td>--sa-password</td>
<td>String</td>
<td>The Active Directory service account password.</td>
</tr>
<tr>
<td>--domain-controller</td>
<td>String</td>
<td>Specifies one or more domain controllers to use with the Connector.</td>
</tr>
<tr>
<td>--users-filter</td>
<td>String</td>
<td>The filter to search for users within Active Directory. Specify multiple filters with multiple options. Default user filter: (&amp;(objectCategory=person)(objectClass=user)).</td>
</tr>
<tr>
<td>Flag</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>--computers-filter</td>
<td>String</td>
<td>The filter to search for computers within Active Directory. Specify multiple filters with multiple options. Default computer filter: (&amp;(primaryGroupID=515) (objectCategory=computer)).</td>
</tr>
<tr>
<td>--users-dn</td>
<td>StringArray</td>
<td>The base DN to search for users within AD. Specify multiple DNs with multiple options. Newly provided base DN(s) will automatically replace previous base DN(s). This field is looking for user's within the user-defined DN and SGs.</td>
</tr>
<tr>
<td>--computers-dn</td>
<td>StringArray</td>
<td>The base DN to search for computers within AD. Specify multiple DNs with multiple options. Newly provided base DN(s) will automatically replace previous base DN(s).</td>
</tr>
<tr>
<td>--sync-interval</td>
<td>uint8</td>
<td>The interval (in minutes) for how often to sync AD users and computers with the CASM Service.</td>
</tr>
</tbody>
</table>

**MFA**

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--enable-mfa</td>
<td>String</td>
<td>Installs with multi-factor authentication enabled.</td>
</tr>
<tr>
<td>--radius-server</td>
<td>String</td>
<td>The FQDN or IP address of the RADIUS server to use for MFA. This flag is optional.</td>
</tr>
<tr>
<td>--radius-port</td>
<td>String</td>
<td>The RADIUS server port. If not specified, the default port (1812) is used. If --radius-server is specified then this flag is optional.</td>
</tr>
<tr>
<td>--radius-secret</td>
<td>String</td>
<td>The shared secret used for configuring RADIUS authentication. If --radius-server is specified then this flag is required.</td>
</tr>
</tbody>
</table>

**Certificates**

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--ssl-key</td>
<td>String</td>
<td>The full path and filename of the SSL key to use. The --self-signed flag overrides this flag.</td>
</tr>
</tbody>
</table>
### Connecting to a Remote Workstation with a PCoIP Client

After successfully installing a Connector, you can initiate a session to connect to a remote workstation with a PCoIP Software Client. Teradici enables customers to use multi-factor authentication for these PCoIP Client sessions. The following steps outline how to connect to a remote workstation using the PCoIP Software Client:

1. Double-click the PCoIP Client desktop icon or program file **PCoIPClient** to launch the application.

2. In the **Host Address or Code** field, enter one of the following:
   - For direct connections, provide the address of the host machine.
   - For managed connections, provide the address of the connection manager.

3. Click **NEXT**.

4. Select your domain and enter the credentials for the remote workstation. If you have enabled MFA then you will be prompted for the 2nd factor passcode. The method of how this passcode is communicated depends on the provider you used. It is usually either a One Time Password or push notification.

5. Click **LOGIN**.

6. If your login is successful you should be able to select the remote workstation and connect to it. Please note that if you have a single remote workstation, that remote workstation is

---

**Troubleshooting the Connector**

If you encounter issues when attempting to install the 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 Connector. For information on installer errors related to a change in the distribution system, see Installer Issues.

---

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--ssl-cert</td>
<td>String</td>
<td>The full path and filename of the SSL certificate (in PEM format) to use.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The <strong>--self-signed</strong> flag overrides this flag.</td>
</tr>
</tbody>
</table>
automatically selected and the connection is initiated immediately. In this case you will not be presented with a remote workstation selection screen.

For more information about the PCoIP Software Client, please see the following PCoIP Software Client guides:

- PCoIP Software Client for Windows
- PCoIP Software Client for macOS
- PCoIP Software Client for Linux
Updating the Cloud Access Connector

When updating an installed Connector you must download the latest version of the Connector installer. For information on how to download the Connector installer, see Installing the Connector. All parameters persist from installation using pre-defined configurations and do not need to be updated unless new configurations are required. For more information on this please see the Persistent Parameters section below.

Once you have downloaded the latest installer, run the update command:

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

### Internal IP Address

As part of the update command the Connector will send its internal IP address to CAS Manager. Previously, this only occurred during installation.

### Latest Installer Version

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

- The installer is out of date. Please obtain the latest version and try again. See Downloading the Connector for instructions.

- The installer is out of date. Please download the latest version from teradici.bintray.com/cloud-access-connector/cloud-access-connector-0.1.1.tar.gz and try again.

- A newer version is available. Please go to Downloading the Connector to obtain the latest.

For information on troubleshooting Connector installer issues related to this distribution change, see Installer Issues.

### Persistent Parameters

Parameters can persist from installation through an update using the pre-defined configurations. As part of the update command, the Connector will search and read from the existing configuration and use the pre-existing information as part of the update.
If you wish to update any parameters with new information as part of the update, you can add these parameters when you are running the update command, for example, if you wanted to update the domain controller you would run the following command:

```
cd /usr/sbin
sudo cloud-access-connector update --domain-controller mydomain.com
```

If you do not add domain controllers during the update, any domain controllers that have been previously saved in the configuration will be used. If there are no domain controllers saved, the system will do an auto-discovery to find which domain controllers could be used.

---

### Expired User Credentials

Be aware that you have a `--sa-user` or `--sa-password` that are expired and you do not add the new credentials to the update, then the update will fail. Please ensure these credentials are valid when performing an update of the Connector.

---

### Installation Flags and Options

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

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--casm-url</code></td>
<td>String</td>
<td>Required for CAS Manager, Specifies the CAS Manager URL that the Connector connects to. If this is not specified it will point to <code>https://cas.teradici.com</code> by default, which is the URL for CAS Manager as a Service.</td>
</tr>
<tr>
<td><code>--casm-ca-cert</code></td>
<td>String</td>
<td>Enables users to supply a CA certificate for CAS Manager to enable the Connector to connect to a CAS Manager instance using self-signed certificates.</td>
</tr>
<tr>
<td><code>--casm-insecure</code></td>
<td>String</td>
<td>Is required when the Connector is connecting to a CAS Manager instance that is using self-signed certificates. If CAS Manager is using trusted TLS certificates signed by a public CA, then users will not need to use the this command.</td>
</tr>
</tbody>
</table>

---

© 2021 Teradici
### Flag

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--ldaps-ca-cert</code></td>
<td>String</td>
<td>Enables users to supply a CA certificate for the connection to Active Directory over LDAPS.</td>
</tr>
<tr>
<td><code>--self-signed</code></td>
<td>String</td>
<td>Installs the Connector with self-signed certificates. This mode is not secure and is intended for testing. The <code>--insecure</code> flag is still supported.</td>
</tr>
</tbody>
</table>

### Connector

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--token (-t)</code></td>
<td>String</td>
<td>Required. The token generated for CAS Manager.</td>
</tr>
<tr>
<td><code>--accept-policies</code></td>
<td>–</td>
<td>Automatically accept the EULA and Privacy Policy.</td>
</tr>
<tr>
<td><code>--force-install</code></td>
<td>String</td>
<td>Replaces any existing Connector installation.</td>
</tr>
<tr>
<td><code>--debug</code></td>
<td>String</td>
<td>This flag can be run if you initial install of the Connector fails. It provides a detailed output of the Connector installation. This is useful for self-troubleshooting or to provide to the Teradici support team when logging a support ticket.</td>
</tr>
<tr>
<td><code>--local-license-server-url</code></td>
<td>String</td>
<td>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: <code>--local-license-server-url http://10.10.10.7070/request</code>. For more information on the PCoIP License Server, see PCoIP License Server.</td>
</tr>
<tr>
<td><code>--add-pool-group</code></td>
<td>String</td>
<td>Specifies one or more Active Directory groups, by entering the distinguished name (DN), to be assigned to pools for remote workstation management (eg. <code>--pool-group 'CN=GroupPool1,CN=Users,DC=sample,DC=com' --pool-group 'CN=GroupPool2,CN=Users,DC=sample,DC=com'</code>). By providing all the existing pools groups in the Connector settings would get replaced by the user specified ones. When running this command you need to run it with <code>adconfig</code>. Example: <code>sudo ./cloud-access-connector adconfig --add-pool-group</code>.</td>
</tr>
<tr>
<td>Flag</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>--setup-docker-image</code></td>
<td>String</td>
<td>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.</td>
</tr>
<tr>
<td><code>--docker-registry</code></td>
<td>String</td>
<td>This is an optional flag that enables users to specify the docker image registry that they want to use when installing or updating a Connector. If an option is not specified, the default registry <code>docker.cloudsmith.io/teradici/cloud-access-connector</code> 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.</td>
</tr>
<tr>
<td><code>--prune-image</code></td>
<td>Boolean</td>
<td>Removes all unused docker images on this machine to reclaim more disk space. <strong>Warning:</strong> This command will remove all unused images under Connector and other services, if any. This is equivalent to the <code>docker image prune</code> command.</td>
</tr>
</tbody>
</table>

**Firewall**

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--https-proxy</code></td>
<td>String</td>
<td>Specify the URL for a HTTPS proxy (overrides related proxy settings in environment variables)</td>
</tr>
<tr>
<td><code>--connector-network-cidr</code></td>
<td>String</td>
<td>This is the CIDR to use for the Connector's docker network. The default docker network subnet is 10.101.0.0/16.</td>
</tr>
<tr>
<td><code>--internal-client-cidr</code></td>
<td>String</td>
<td>The CIDR for PCoIP Clients that connect to remote workstations directly. It is possible to specify multiple <code>--internal-client-cidr</code> networks.</td>
</tr>
<tr>
<td><code>--external-client-cidr</code></td>
<td>String</td>
<td>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. It is possible to specify multiple <code>--external-client-cidr</code> networks.</td>
</tr>
</tbody>
</table>
# Flag Description

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PCoIP Software Client</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>--retrieve-agent-state</code></td>
<td>Boolean</td>
<td>Enables the broker to retrieve the agent state for unmanaged and managed remote workstations. The default value for this flag is false. The available states are <strong>In Session</strong>, <strong>Ready</strong>, <strong>Starting</strong>, <strong>Stopping</strong>, <strong>Stopped</strong> and <strong>Unknown</strong>. The value of this flag can either be true or false.</td>
</tr>
<tr>
<td><code>--show-agent-state</code></td>
<td>Boolean</td>
<td>Controls if the agent state is displayed as part of the remote workstation name in the PCoIP Client. The default value for this flag is true. Setting the value of this flag to true and the <code>--retrieve-agent-state</code> flag to false will result in no agent state displaying.</td>
</tr>
<tr>
<td><code>--external-pcoip-ip</code></td>
<td>String</td>
<td>Sets the public IP for PCoIP Client to PCoIP Agent connection. This is the public IP that the Connector is listening to on port 4172. The installer will reach out to <code>cas.teradici.com</code> and first try to automatically resolve the external IP; if this fails, or is not able to resolve the correct IP, this flag is required. In the case that the Connector machine doesn't have an internet connection, for example in a dark site environment, or the ingress and egress internet traffic are running through different public IPs, this flag is required. For more information on external network access, see <a href="#">Enabling External Network Access</a>.</td>
</tr>
</tbody>
</table>

## Domain

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--domain</code></td>
<td>String</td>
<td>The AD domain that remote workstations will join.</td>
</tr>
<tr>
<td><code>--sa-user</code></td>
<td>String</td>
<td>The Active Directory service account username.</td>
</tr>
<tr>
<td><code>--sa-password</code></td>
<td>String</td>
<td>The Active Directory service account password.</td>
</tr>
<tr>
<td><code>--domain-controller</code></td>
<td>String</td>
<td>Specifies one or more domain controllers to use with the Connector.</td>
</tr>
</tbody>
</table>

© 2021 Teradici
<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--users-filter</td>
<td>String</td>
<td>The filter to search for users within Active Directory. Specify multiple filters with multiple options. Default user filter: (&amp;(objectCategory=person)(objectClass=user)).</td>
</tr>
<tr>
<td>--computers-filter</td>
<td>String</td>
<td>The filter to search for computers within Active Directory. Specify multiple filters with multiple options. Default computer filter: (&amp;(primaryGroupID=515) (objectCategory=computer)).</td>
</tr>
<tr>
<td>--users-dn</td>
<td>StringArray</td>
<td>The base DN to search for users within AD. Specify multiple DNs with multiple options. Newly provided base DN(s) will automatically replace previous base DN(s). This field is looking for user's within the user-defined DN and SGs.</td>
</tr>
<tr>
<td>--computers-dn</td>
<td>StringArray</td>
<td>The base DN to search for computers within AD. Specify multiple DNs with multiple options. Newly provided base DN(s) will automatically replace previous base DN(s).</td>
</tr>
<tr>
<td>--sync-interval</td>
<td>uint8</td>
<td>The interval (in minutes) for how often to sync AD users and computers with the CASM Service.</td>
</tr>
</tbody>
</table>

**MFA**

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--enable-mfa</td>
<td>String</td>
<td>Installs with multi-factor authentication enabled.</td>
</tr>
<tr>
<td>--radius-server</td>
<td>String</td>
<td>The FQDN or IP address of the RADIUS server to use for MFA. This flag is optional.</td>
</tr>
<tr>
<td>--radius-port</td>
<td>String</td>
<td>The RADIUS server port. If not specified, the default port (1812) is used. If --radius-server is specified then this flag is optional.</td>
</tr>
<tr>
<td>--radius-secret</td>
<td>String</td>
<td>The shared secret used for configuring RADIUS authentication. If --radius-server is specified then this flag is required.</td>
</tr>
</tbody>
</table>

**Certificates**
Enabling MFA While Updating

You can enable MFA to the Connector with the `--enable-mfa` flag when performing an update:

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

You need to have the following information:

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

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 Connector with the `--disable-mfa` flag when performing an update:

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

---

### Connector Upgrade and Diagnose Issues

Several previous versions of Connector installers are no longer compatible with our latest infrastructure 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 Connector installer from here.

---

### Flags and Description

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--ssl-key</code></td>
<td>String</td>
<td>The full path and filename of the SSL key to use. The <code>--self-signed</code> flag overrides this flag.</td>
</tr>
<tr>
<td><code>--ssl-cert</code></td>
<td>String</td>
<td>The full path and filename of the SSL certificate (in PEM format) to use. The <code>--self-signed</code> flag overrides this flag.</td>
</tr>
</tbody>
</table>
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 Connector. You can update your 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 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.
Scaling and PCoIP Session Limits

When using CAS Manager as a Service there are certain session establishment and session bandwidth limits when dealing with external connections.

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

<table>
<thead>
<tr>
<th>vCPUs</th>
<th>RAM</th>
<th>Estimated Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>2vCPU</td>
<td>7.5 GB RAM</td>
<td>~ 365 Mbit/s</td>
</tr>
<tr>
<td>4vCPU</td>
<td>15 GB RAM</td>
<td>~ 830 Mbit/s</td>
</tr>
<tr>
<td>8vCPU</td>
<td>30 GB RAM</td>
<td>~ 1100 Mbit/s</td>
</tr>
</tbody>
</table>

1100 Mbit/s is approximately the maximum bandwidth that can be achieved. Additional gains may be possible with larger sizing.
Firewall and Load Balancing Considerations

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

Ports and Component Connections

<table>
<thead>
<tr>
<th>Component</th>
<th>Allow</th>
<th>Port/Protocol</th>
<th>Source/Destination Component</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connector</td>
<td>Inbound</td>
<td>80 TCP</td>
<td>From administrative web browsers.</td>
<td>For accessing the Management Interface, redirects to port 443.</td>
</tr>
<tr>
<td>Connector</td>
<td>Inbound</td>
<td>443 TCP</td>
<td>From PCoIP Clients and administrative web browsers.</td>
<td>For users to negotiate connections to their remote workstations. For accessing the Management Interface for (legacy) management of CAS Manager.</td>
</tr>
<tr>
<td>Connector</td>
<td>Outbound</td>
<td>443 TCP</td>
<td>To CAM Service, PCoIP Cloud License Server and to SumoLogic.</td>
<td>To sync AD information to the CAM service and call CAS Manager APIs related to negotiating PCoIP sessions. To verify license activation code during the Connector installation. For log aggregation for support purposes.</td>
</tr>
<tr>
<td>Connector</td>
<td>Outbound</td>
<td>60443 TCP</td>
<td>To remote workstations.</td>
<td>Prepares PCoIP Agents for a new user session.</td>
</tr>
<tr>
<td>Connector</td>
<td>Inbound</td>
<td>4172 TCP/UDP</td>
<td>From PCoIP Clients.</td>
<td>For PCoIP Sessions with users that are outside of the corporate network.</td>
</tr>
<tr>
<td>Connector</td>
<td>Outbound</td>
<td>4172 TCP/UDP</td>
<td>To remote workstations.</td>
<td>For PCoIP Sessions with users that are outside of the corporate network.</td>
</tr>
<tr>
<td>Component</td>
<td>Allow</td>
<td>Port/Protocol</td>
<td>Source/ Destination Component</td>
<td>Descriptions</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------</td>
<td>---------------</td>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Connector</td>
<td>Outbound</td>
<td>636 TCP</td>
<td>To Domain Controllers.</td>
<td>To authenticate users, and query user and computer information.</td>
</tr>
<tr>
<td>Connector</td>
<td>Outbound</td>
<td>1812 UDP</td>
<td>To RADIUS Server.</td>
<td>For authentication against RADIUS Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(This port is configurable)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connector</td>
<td>Outbound</td>
<td>53 UDP</td>
<td>To DNS.</td>
<td>Domain name resolution.</td>
</tr>
<tr>
<td>PCoIP License Server</td>
<td>Inbound</td>
<td>7070 TCP</td>
<td>From remote workstations.</td>
<td>For license activation and verification from PCoIP Agent if the PCoIP License Server is used instead of the Cloud License Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(This port is configurable)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.
Using the Cloud Access Connector with a Web Proxy

If web access is being blocked to the machines in your environment the Connector will not work. In order to give the 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 Connector with a Web Proxy

The following steps outline how to use the 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:

```plaintext
# 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
```

© 2021 Teradici
To test that the proxy is working correctly, using SSH, open a terminal on the Connector host machine and run the following set of commands:

```
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
```

1. To test that the proxy is working correctly, using SSH, open a terminal on the 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>
<bodybgcolor="white">
<center><h1>308 Permanent Redirect</h1></center>
<hr><center>nginx</center>
</body>
</html>
```
1. To run the installer with the proxy settings, you can apply them in the environment:

```bash
$ export https_proxy=$http_proxy
$ curl https://cam.teradici.com
```

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 Connector at this time.
Configuring the Active Directory for Cloud Access Connector

Teradici recommends having a single Active Directory 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=CASM, CN=Users, DC=example, DC=com`. You can also configure the frequency at which the Cloud Access Connector syncs this data with the CASM service, as outlined in the following table:

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

© 2021 Teradici
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.

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--users-filter</td>
<td>String</td>
<td>The filter to search for users within Active Directory. Specify multiple filters with multiple options. Default user filter: <code>(&amp;(objectCategory=person)(objectClass=user))</code>. An example for a user group filter: <code>(&amp;(objectCategory=person)(objectClass=user)(memberOf: 1.2.840.113556.1.4.1941:CN=PCoIP Users Group,CN=Users,DC=example,DC=com))</code>.</td>
</tr>
<tr>
<td>--cam-insecure</td>
<td>String</td>
<td>Skips certificate validation when connecting to CAS Manager as a Service. This option should only be used when connecting to CAS Manager as a Service deployed with self-signed certificates.</td>
</tr>
</tbody>
</table>
## Configuring Active Directory Pool Groups

<table>
<thead>
<tr>
<th>Flag</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--add-pool-group</td>
<td>String</td>
<td>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.</td>
</tr>
<tr>
<td>--remove-pool-group</td>
<td>String</td>
<td>Removes specified pool Active Directory group by its DN.</td>
</tr>
<tr>
<td>--clear-pools-groups</td>
<td>String</td>
<td>Clears all pools Active Directory groups. This operation is exclusive and cannot be combined with <code>--remove-pool-group</code> or <code>--add-pool-group</code>.</td>
</tr>
<tr>
<td>--get-cam-settings</td>
<td>String</td>
<td>Prints all CAS Manager as a Service settings to Admin console.</td>
</tr>
</tbody>
</table>
Floating Workstation Assignments

Floating workstation assignments is a feature of the Connector v78 or higher, which enables a user's entitlement to a workstation to be temporary. The remote workstation can be used by multiple users. Floating workstation assignments enables remote workstations that are part of a Remote Workstation Pool, to be assigned to a user for the duration of the PCoIP session. Once this session has been disconnected, the remote workstation will be automatically unassigned, and will be available for other users to connect.

This feature is useful for managing persistent remote workstations that are shared by multiple users and that have expensive software and applications, such as video editing, video proofing, etc. Multiple users can access the same remote workstation and utilise these applications. It can be used for project based remote workstations, where remote workstations are associated with projects instead of users. Teams can log into the project and access a specific remote workstation for that project. This also enables organisations to enforce logical separation of remote workstations.

The following sections outlines the steps involved in enabling this feature.

---

**Applicable for CAS Manager as a Service in Beta Mode**

Currently, the floating workstation assignment feature is **only** available for Connectors deployed to CAS Manager as a Service. It is not currently supported with CAS Manager.

This feature is currently supported in the Beta mode of the Admin Console. Features in this mode are still being worked on and refined by Teradici, as a result there may be certains issues that arise.

---

Enable Session Tracking

In order to enable this feature, you must first enable session tracking from the Admin Console.

1. Log in to the Admin Console.
2. Click on the Beta UI toggle from the top menu. This feature currently only works in the Beta version of the Admin Console.
3. Navigate to the deployment you want to enable floating workstation assignments on. In the top menu bar beside the deployment click on the kebab menu item and click **Edit deployment**.

4. Select the **CONNECTOR SETTINGS** tab from the deployment and click on the **Session Tracking** toggle.

Create a Floating Pool

The next step is to create a floating pool group from the Admin Console.

1. Open the **Workstations Pools** page and click the + icon to create a new pool.
2. Select **Floating** for the workstation assignment policy, name the pool and click **CREATE**.
3. Click on the newly created pool from the Pools menu.
4. Click **ADD REMOTE WORKSTATIONS** to add workstations to the pool and click **SAVE**.
Assign Users to the Pool

Once you have enabled session tracking and created and added remote workstations to your pool, you now need to add specific users. Only specified users can establish PCoIP sessions to remote workstations in the pool.

1. Click on the newly created pool from the Pools menu.
2. Click **ADD USERS** from the top menu, select the users you want to add and click **SAVE**.

Once you have completed these steps any user from the pool will be able to get any available remote workstation from the same pool on login. Once the PCoIP session has been disconnected, the remote workstation will automatically become available for future connections.

---

**Remote Workstation Limit**

There is a limit of 200 remote workstations in a floating pool. This feature will work with a larger number of remote workstations, but assignment timing may vary as a result.

---

**Session Disconnection**

Please note that remote workstations will remain assigned to a user for approximately 25 minutes after the PCoIP session has been disconnected.

---

**Limited Support for PCoIP Agents for Linux**

PCoIP sessions to PCoIP Agents for Linux must be logged off before another user can connect. If the session is not logged off, the user will see a 6604 Error. If you observe this error, reboot the remote workstation.
Configuring the Broker Response Timeout

The following section outlines how to increase and set the `BROKER_MAX_WAIT_SECONDS` parameter for the Connector.

1. Make a copy of the `docker-compose.yaml` file by running the following command:

   ```bash
cp /opt/connector_data/docker-compose.yaml /opt/connector_data/docker-compose-new.yaml
   ```

2. Edit `/opt/connector_data/docker-compose.yaml` to add an environmental variable.
   - If you have an active Security Gateway, find the `cmsg` service section and add the following parameter and enter a value in seconds:

   ```yaml
   BROKER_MAX_RESP_WAIT_SECONDS=<required_value>
   ```
   - If you don't have an active Security Gateway, find the `cm` service section and add the following parameter and enter a value in seconds:

   ```yaml
   BROKER_MAX_RESP_WAIT_SECONDS=<required_value>
   ```

3. Update the Connector by running the following command:

   ```bash
   cloud-access-connector update --compose-file /opt/connector_data/docker-compose-new.yaml
   ```
Multi-Factor Authentication (MFA)

CAS Manager as a Service supports Multi-Factor Authentication (MFA) for PCoIP client sessions. The CAS Manager as a Service MFA implementation is based on the RADIUS protocol. Customers can leverage their existing RADIUS server installation to enable MFA for CAS Manager as a Service 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 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 Connector it will require the following information to configure the Duo Radius server:

- Radius Client IP (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 CAS Manager as a Service, see CAS Manager as a Service Duo MFA.
Multi-Factor Authentication with Azure

Microsoft Azure MFA Component Versions

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

Teradici component versions:

- PCoIP Software Client for Windows 19.11.
- 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 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 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 3\textsuperscript{rd} party components to enable Azure MFA with Connector, see \textit{CAS Manager as a Service Azure MFA}.
The CAS Manager as a Service Privacy Statement details information around the collection, use, processing and disclosure of personal information and other information in connection with the CAS Manager as a 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 Admin Console supports Microsoft Azure Active Directory for authentication. All users with a work or school account from Microsoft can sign in to the 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.
CAS Manager as a Service Multi-Factor Authentication

Duo Authentication

If you wish to use Duo authentication with CAS Manager as a Service 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 Connector was tested with Duo version 2.4.21.

The following are key items in the authproxy.cfg file that are relevant for the CAS Manager as a Service 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 Connector with Microsoft Azure MFA on November 15th 2019 with the following components.

Teradici component versions:
- PCoIP Software Client for Windows 19.11.
- 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 Connector you need to configure a number of 3rd party components. The following steps outline this process:

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

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

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

6. Restart NPS services to enable these changes to take effect.
Specifying Domain Controllers

You can optionally specify one or more domain controllers to use with the 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 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 CAS Manager as a Service Idle Shutdown

The following section outlines how to install and configure idle shutdown on remote workstations not provisioned by CAS Manager as a Service on Windows and Linux.

Any remote workstations provisioned by CAS Manager as a Service 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 CAS Manager as a Service and are not managed by CAS Manager as a Service, 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 CAS Manager as a Service 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 CAS Manager as a Service.

### Installing on Windows

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

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

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

© 2021 Teradici
# Install Service

```
$ret = .\IdleShutdownAgent.exe -install
# Check for success
if (!$?) {
    $msg = "Failed to install {0} because: {1}" -f $serviceName, $ret
    Write-Host $msg
    throw $msg
}
```

# Configure Service

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

# Disable service if desired

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

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

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

- PCoIP Agent version 19.05 and later, the settings are stored in:
  HKLM\SOFTWARE\Teradici\CAMShutdownIdleMachineAgent

The table below outlines the settings and defaults:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DWORD</td>
<td>PollingIntervalMinutes</td>
<td>15</td>
<td>minutes</td>
</tr>
<tr>
<td>DWORD</td>
<td>MinutesIdleBeforeShutdown</td>
<td>240</td>
<td>minutes</td>
</tr>
<tr>
<td>DWORD</td>
<td>CPUUtilizationLimit</td>
<td>20%</td>
<td></td>
</tr>
<tr>
<td>DWORD</td>
<td>EnableCAMDebug</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

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

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

### Installing on Linux

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

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

### Configuring on Linux

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

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

```
systemctl daemon-reload
```

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
```

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

Teradici has an open github repository that contains a collection of scripts that simplify the setup, installation and usage of CAS Manager as a Service. This repository enables users to set-up the necessary cloud resources (networking, firewalls, NAT gateway, storage buckets, etc.), as well as Domain Controllers, 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 Connectors is available at https://github.com/teradici/cloud_deployment_scripts.
Licensing Options with CAS Manager as a Service

With CAS Manager as a Service, 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 Connector during the installation process. You must enter this key in the 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 CAS Manager as a Service 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 CAS Manager as a Service 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 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**

<table>
<thead>
<tr>
<th>Features</th>
<th>Cloud License Server</th>
<th>PCoIP License Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online activation supported?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Offline (Dark site) activation supported?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Internet proxy supported?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>High Availability options available?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Ability to track license usage?</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

For more information on Licensing with Teradici, see here.

---

**Using Cloud Licensing with CAS Manager as a Service**

If you are using CAS Manager as a Service 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 Connector.

**Installation Steps**

- When installing the Connector, use your registration code to register with the Teradici licensing system. For more information on installing the 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 CAS Manager as a Service**

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 CAS Manager as a Service 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 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 CAS Connector, 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 purchase 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 CAS Manager as a Service**

- CAS Manager as a Service requires a Cloud License Server registration code to be entered in the Admin Console when creating a deployment.
- The user can install the PCoIP License Server URL directly into the Connector during installation.
- Any remote workstations provisioned by CAS Manager as a Service 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 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
CAS Manager as a Service Maintenance

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

OS Updates

The 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
```

Connector Updates

The 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 Connector, it is important to run updates regularly. For more information on how to update the Connector, see here. Teradici recommends updating once a month. Updates can be carried out in place or by deploying a new Connector machine as part of a red-black deployment update.

Disk Space Updates

The 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 Connector:

```
docker system prune
```

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

CAS Manager as a Service’s capabilities 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 CAS Manager as a Service is able to assume. For more information on creating roles in AWS, see Creating a role to delegate permissions to an IAM user. You must use the Account ID and External ID that can be generated from the Admin Console, for information on how to generate these credentials, see the section outlined below.

AWS Cloud Credentials for CAS Manager as a Service

The following section outlines how to generate the Account ID and External ID from the CAS Manager Admin Console. The following steps outline how to generate a CAS Manager Account ID and External ID:

1. In the CAS Manager Admin Console select the deployment you wish to use.
2. Click Edit Deployment.
3. Click Cloud Service Accounts.
4. Select AWS and click Generate. Ensure you copy the CAS Manager Account ID and External ID and save them to your clipboard.

AWS Role Creation and Permission Policy

You must create a role in your AWS account which CAS Manager as a Service 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.
Once you have entered the CAS Manager Account ID and External ID and created the AWS role, you will need to create a permissions policy for CAS Manager as a Service that contains the permissions outlined in the section below.

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:

- **Service**: IAM
- **Actions**
  - Read: **SimulatePrincipalPolicy**

The following example can be copied and pasted into the JSON field when creating the policy instead of manually selecting each role:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Resource": "*"
      }
   ]
}
```
If the user tries to add an AWS role that doesn't have these permissions, CAS Manager as a Service 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.

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 CAS Manager as a Service. 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 CAS Manager as a Service.

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

### Default Roles and Feature Requirements - GCP

<table>
<thead>
<tr>
<th>Default Roles</th>
<th>Workstation Provisioning</th>
<th>Power Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment Manager Editor</td>
<td>Required</td>
<td>—</td>
</tr>
</tbody>
</table>

© 2021 Teradici
For GCP the service account requires access to the following APIs:

- Service Usage API
- Cloud Resource Manager API
- Cloud Deployment Manager V2 API
- Cloud Key Management Service (KMS)
- Compute Engine API

The following links have more information on GCP service accounts:

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

Creating a Cloud IAM Custom Role

Users can create a single custom IAM role by using the following permissions for CAS Manager as a Service:

- 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 CAS Manager as a Service 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 Connector versions, and the cloud providers that work with the CAS Manager as a Service.

Cloud Access Manager Features enabled by Cloud Service Accounts

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

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

Permissions to Create and Delete Computer Objects

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

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

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

1. Go to the security tab of the OU you want to give permissions to.
2. Right-click the relevant OU and click Properties.
3. Go to the security tab and click Advanced.
4. Click Add and browse to your user account. As stated above you need to add the user account to the OU.
5. Limit the Apply Onto scope to Descendant Computer objects and select the following settings:
   - Read All Properties
   - Write All Properties
   - Read Permissions
   - Modify Permissions
   - Validated write to DNS host name
   - Validated write to service principal name
6. Click OK.
The following section outlines how to verify your on-premises AD DS account lockout policy. The steps below need to be carried out on a domain-joined system with administrator privileges:

1. Open the Group Policy Management Editor by clicking the start menu and searching for Edit group policy.
2. Edit the group policy that includes your organization’s account lockout policy, such as the Default Domain Policy.
4. Verify your Account lockout threshold and Reset account lockout counter after values.
CAS Manager as a Service accounts have a single account owner, and one or more administrators who have the ability to authenticate to the Admin Console and manage CAS Manager as a Service 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 CAS Manager as a Service account owner:

- Account ownership changes will change all account data, including all deployment, remote workstation and user data to another account owner and cannot be reversed without the new account owner providing authorization.
- 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’s 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 CAS Manager as a Service 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.

Identity Providers

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 identity provider in question. Once the account has been transferred through the identity provider, the user will be able access CAS Manager as a Service but they will not see any of their old data as CAS Manager as a Service recognizes this as a different account. CAS Manager as a Service uses a unique object identifier returned by the identity providers to associate specific data to specific user’s. This identifier is immutable and cannot be changed.
Account Ownership Transfers

If a CAS Manager as a Service 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:

- **CAS Manager as a Service Authorization token from the old account**: This needs to be provided by the user.
- **CAS Manager as a Service Authorization token from the new account**: This needs to be provided by the user.

For information on how to obtain a CAS Manager as a Service authorization token from the Admin Console, see the [API Access Token](#) section of the CAS Manager Administrator’s Guide.

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

### Account Data Transfers

Transferring an account means that all data from one account is moved to another. This might not be suitable for Managed Service Providers that may be managing multiple deployments.

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 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. CAS Manager as a Service 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 CAS Manager as a Service user account:

1. Sign into the 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 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:

- 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 Knowledge Center.
Getting Your Registration Code

You need a registration code to activate your PCoIP agent and to use it in conjunction with Teradici CAS Manager as a Service. 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.
Teradici provides service status at the following site: CAS Manager as a Service Status. From this site it is possible to view the current status of the CAS Manager as a 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 CAS Manager as a 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.
Retrieving Cloud Access Connector Version Numbers

Understanding the version number of a Connector can be useful when troubleshooting issues and to ensure you are running the latest version of the Connector. The Connector, from version 67 on, has a single version number. Previously, the installer and connector version numbers were different. These have now been combined to display a single version number going forward.

Connector Installer Version

The installer is used for installing, updating and diagnosing issues related to the Connector installation process. It can be updated at the same time as the Connector, and also updated independent of the Connector as updates are made to improve installation specific areas. A change in the version of the installer does not require an upgrade to the Connector itself.

If you have downloaded the Connector installer you can obtain the version number by running one of the following commands (depending on where it has been copied to):

```
./cloud-access-connector --version
```

or

```
/usr/sbin/cloud-access-connector --version
```

A successful response is outlined below:

```
cloud-access-connector v66.0.63_9606001760
```

The first command should be used if you are currently in the same directory as the installer. This is more common for older versions of the installer. The second command is the location where newer versions of the installer have been copied to.

The Connector installer version also appears at the top of the output when you run an installation:
It will also be logged by the installer:

User@vm:~$ sudo /usr/sbin/cloud-access-connector install
[2021-02-03T17:16:01Z] INFO Set docker registry as: docker.cloudsmith.io/teradici/cloud-access-connector
[2021-02-03T17:16:01Z] INFO Starting cloud-access-connector
version=v66.0.63_9606001760
...

user@vm:/var/log$ sudo more /var/log/cloud-access-connector/install_2021-02-03T17-16-01.log

```
time="2021-02-03T17:16:01Z" level=info msg="Starting cloud-access-connector"
version=v66.0.63_9606001760
time="2021-02-03T17:17:14Z" level=error msg="You must accept the EULA and Privacy Policy to continue."
```
...

You can also view the Connector installer version number from the Teradici download site when viewing the download filename.

**Connector Version**

The Connector version, sometimes referred to as the YAML or compose file, denotes the combination of containers that make up a particular release of the Connector. The primary location to view the version of your running Connector is from the Connectors page in the Admin Console.

This version number represents a combination of specific versions of services that run on the Connector. For example, version 42 of the Connector includes the PCoIP Connection Manager 21.01.0. When troubleshooting issues, this version is used by Teradici's support team to inform them as to which version of each service is running on your Connector.

---

**Legacy Connector Versions**

You should ensure that you keep this version as up to date as possible. Teradici is continuously enhancing, adding features, fixing bugs and improving the overall security of the Connector. If you have a version that is v38 or lower, you should update your Connector as previous versions were integrated with an installer that predates our current Connector download location, and further installs or updates from that legacy installer may not work correctly.
If you are unable to access the Admin Console, you can obtain the version of the Connector from the configuration file itself, as outlined in the below example:

```
user@vm:/var/log$ cat /var/local/teradici/docker-compose.yaml | grep CACV2_VERSION
  CACV2_VERSION: 42
```
Cloud Access Connector Installer Issues

Teradici moved to a new distribution system and on December 31, 2020 the legacy system was shut down. As a result of this change some errors may occur for users with Connectors that were installed from older installer versions.

In almost all cases downloading the latest installer version and running the `cloud-access-connector install`, `cloud-access-connector update` or `cloud-access-connector diagnose` commands with the new install should work.

For information on this, see here.

Error Messages

The following are a list of potential error messages that a user may encounter as a result of the change of distribution system:

**Attempting to download the installer**

Error 1

```
user@vm:~$ mkdir ~/v2connector && cd ~/v2connector
user@vm:~$ curl -LO https://teradici.bintray.com/cloud-access-connector/cloud-access-connector-0.1.1.tar.gz
% Total    % Received % Xferd Average Speed   Time    Time     Time  Current
        0      0      0          0     0              0            0          0             0 --:--:-- --:--:-- --:--:-- --:--:--
user@vm:~$ curl -LO https://teradici.bintray.com/cloud-access-connector/cloud-access-connector-0.1.1.tar.gz
% Total    % Received % Xferd Average Speed   Time    Time     Time  Current
        0      0      0          0     0              0            0          0             0 --:--:-- --:--:-- --:--:-- --:--:--
user@vm:~$ tar xzvf cloud-access-connector-0.1.1.tar.gz
gzip: stdin: not in gzip format
```

```
tar: Child returned status 1
```

```text
tar: Error is not recoverable: exiting now
```

Error 2

```
user@vm:~$ mkdir ~/v2connector && cd ~/v2connector
user@vm:~$ curl -LO https://teradici.bintray.com/cloud-access-connector/cloud-access-connector-0.1.1.tar.gz
% Total    % Received % Xferd Average Speed   Time    Time     Time  Current
        0      0      0          0     0              0            0          0             0 --:--:-- --:--:-- --:--:-- --:--:--
```

```text
gzip: stdin: not in gzip format
```

```
tar: Child returned status 1
```

```text
tar: Error is not recoverable: exiting now
```
Running older installer versions

If the Connector installer was installed before December 11, it may generate some of the following errors:

Error 3

```
[2020-12-22T20:36:57Z] INFO Verifying installer version
[2020-12-22T20:36:57Z] ERROR yaml: unmarshal errors:
    line 1: cannot unmarshal !!str `The req...` into docker.ComposeConfig
```

Error 4

```
[2020-12-22T20:07:09Z] INFO Downloading compose file
[2020-12-22T20:07:09Z] INFO curl: (60) SSL certificate problem: self signed certificate
[2020-12-22T20:07:09Z] INFO curl failed to verify the legitimacy of the server and therefore could not establish a secure connection to it. To learn more about this situation and how to fix it, please visit the web page mentioned above.
[2020-12-22T20:07:09Z] ERROR exit status 60
```

Error 5

```
[2020-12-22T20:24:06Z] INFO Configuring Docker Daemon
[2020-12-22T20:24:06Z] INFO populateTrustAndKeyStore: Pulling setup container and populating Java trust and key store
[2020-12-22T20:24:07Z] INFO Error response from daemon: error parsing HTTP 404 response body: invalid character `<' looking for beginning of value: "<!doctype html>"<html lang="en">"<head>"<title>HTTP Status 404 - Not Found"</title>"<style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line {height: 1px;background-color:#525D76;border:none;}"</style>""<head>""<body>""<h1>HTTP Status 404 - Not Found</h1>""<hr class="line" />
```

© 2021 Teradici
Error 6


[2021-02-11T01:02:42Z] ERROR exit status 1
CAS Manager as a Service provides some diagnostic checks that can be used to troubleshoot the cause of issues you may be experiencing with your 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 Connector has been correctly configured. The diagnostic checks cover Remote Workstation connectivity and Active Directory connectivity.

The following table lists the flags associated with this command:

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

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

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

Example command to diagnose remote workstation connectivity issues:

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

Check Passes

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

Check Fails

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

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

Active Directory Connectivity Check

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

Example command to diagnose Active Directory connectivity issues:

```
```

Connector Upgrade and Diagnose Issues

Several previous versions of Connector installers are no longer compatible with our latest infrastructure 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 Connector installer from here.
Check Passes

• The Connector is able to resolve the FQDN of the domain controller and authenticate to it.

Check Fails

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

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

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

To view the status of all services in the 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/`.