Cloud Access Architecture Guide

For access to the full Teradici product documentation visit Teradici Support.

Introduction

Teradici Cloud Access solutions enable enterprises to easily deliver Windows and Linux desktops and applications from public or private clouds, with the highest user experience and security, and total cloud independence.

Who Should Read This Guide?

This guide provides information for system administrators who are looking to implement, install, and develop Teradici Cloud Access solutions. This guide provides you with information you can use to better understand:

- User connection and licensing models for Cloud Access Software.

- The components of a Teradici Cloud Access solution.

- How to architect Teradici Cloud Access solutions for public cloud infrastructure and on-premises datacenters.

- How to optimize and customize a Teradici Cloud Access solution.

- How Teradici Cloud Access Manager enables scalable and cost-effective Cloud Access deployments by managing cloud compute costs, facilitating authentication and brokering PCoIP connections to remote Windows or Linux workstations.

What is PCoIP® Technology?

PCoIP is a display protocol that encodes a complete desktop or workload, which is then displayed through a PCoIP Client device over a standard IP network. PCoIP technology uses advanced display compression to provide remote computing solutions such as remote physical workstations, GPU-enabled virtual workstations, or standard virtual desktops as a progressive alternative to a local deployment model. It also supports many of the devices available to physical machines, including keyboard, mouse, USB devices, tablets, multiple monitors, printers, audio devices, as well as custom options.

The PCoIP protocol ensures ultra-secure remote connectivity between a remote computer and a broad range of client devices including stateless PCoIP Zero Clients, PCoIP Software Clients and PCoIP Mobile Clients. Display images are compressed and transmitted as a stream of encrypted pixels, ensuring corporate IP remains secured within the enterprise data center.

The PCoIP protocol, and PCoIP Cloud Access Software, offers unrivaled performance in terms of user interactivity, frame rate and image quality. PCoIP also features a 'build-to-lossless' capability which ensures lossless reproduction of the original display image at the PCoIP Client endpoint. Lossless reproduction is critical particularly in instances such as medical diagnostics, geospatial analysis, and media production, where the image itself contains important visual information. PCoIP protocol uses the User Datagram Protocol (UDP) which is much better suited for streaming media and real time display situations than TCP-based alternatives, especially over high latency networks.

Key Benefits of PCoIP Technology

The following features and benefits are key aspects of PCoIP technology:

- **Host Rendering:** Pixel-level processing means corporate intellectual property remains secured within the cloud or enterprise data center.

- **Image Decomposition and Optimized Multi-codec:** Highest image quality with efficient build-to-lossless and optimized bandwidth.

- **Dynamic Network Adaptation:** Automatically delivers the best possible user experience under changing network conditions.

- **Encrypted Pixel Transmission:** AES-256 Encrypted pixels ensures ultra-secure connections to PCoIP endpoints.

- **True Multicloud Solutions - End to End:** Deploy Windows or Linux on public, private or hybrid cloud infrastructure, including Amazon Web Services (AWS), Microsoft Azure, Google Cloud, VMware ESXi or Red Hat KVM. Additionally PCoIP is integrated in Amazon Workspaces and VMware Horizon.

Who Uses PCoIP Technology?

Teradici PCoIP technology is used in a wide range of industries, including government, education, financial services, healthcare, oil and gas, automotive, media and entertainment, architecture, engineering and construction, manufacturing, and design. For information on specific industry applications, check out the case studies featured on the Teradici website.

PCoIP Ultra

The PCoIP Client provides support for PCoIP Ultra, the latest protocol enhancements from Teradici. PCoIP Ultra is optimized for truly lossless support with bit-exact color accuracy and preservation of content detail at the highest frame rates.

PCoIP Ultra protocol enhancements propels our industry-recognized performance into the future of remote computing, with faster, more interactive experience for users of remote workstations working with high-resolution content.

PCoIP Ultra is disabled by default. To enable it, see Enabling PCoIP Ultra.

PCoIP Ultra Enhancements

In version 20.07, PCoIP Ultra provides the following benefits:

- Support for 4K/UHD high frame rate content
- Efficient scaling across multicore CPUs leveraging AVX2 instruction sets

The Software Client for Windows 20.07 with PCoIP Ultra contains certain limitations around USB and printer plugin redirection. The latest beta version of PCoIP Ultra is available via our Technology Preview version, as outlined below.

> **🔥 PCoIP Ultra Technology Preview**
>
> PCoIP Ultra is an evolving technology, and new capabilities and enhancements are introduced frequently.
>
> If you would like to test unreleased versions of PCoIP Ultra, we invite you to join the PCoIP Ultra Technology Preview program. Technology Preview users receive pre-release versions of Teradici software for use in non-production environments, and provide feedback to our engineering teams.
>
> To learn more and to join the technology preview, visit the Teradici Support site.

Requirements

To take advantage of PCoIP Ultra, you need to meet these requirments:

- A PCoIP agent (any type) 19.05.0 or later.
- A PCoIP Software Client for macOS or PCoIP Software Client for Linux, 19.05.0 or later.

> ✏️ **PCoIP Software Client for Windows users**
>
> Support for PCoIP Ultra on the PCoIP Software Client for Windows is provided via the PCoIP Ultra Technology Preview as described above.

- The CPUs on bot the agent and the client machines must support the AVX2 instruction set.

Troubleshooting PCoIP Ultra

For troubleshooting information around implementing the PCoIP Ultra protocol enhancements, see the knowledge base article: Troubleshooting PCoIP Ultra.

Overview

Cloud Access Software enables PCoIP connections between users and remote workstations or desktops using any of several connection models dependent on number of users, location of users relative to remote workstations, your desire to incorporate public cloud workstations and your authentication requirements. Ultimately, your deployment architecture may be based on one or more of these connection models according to your corporate use case:

- Unmanaged direct connection

- Managed connections for on-site users

- Managed connections for WAN users connecting to on-premises resources

- Managed connections for on-site users and public cloud workstations

- Managed connections for remote workstations in multicloud environments

- Connections brokered by third parties

You can choose to license your Cloud Access Software deployment using the Teradici Cloud Licensing Service or a PCoIP License Server, as described here.

Session Establishment

For troubleshooting tips, FAQs and specific documentation around PCoIP Session Establishment, see the following KB article https://help.teradici.com/s/article/4529. This article includes guidelines, troubleshooting checklists aswell as links to the PCoIP connection instructions found in the various Teradici component guides.

Unmanaged Direct Connections

Unmanaged direct connections as shown below are well suited to proof of concepts, trials and small LAN deployments where flexibility in machine assignment and multifactor authentication may not be required. Each PCoIP endpoint connects directly to the IP address of a remote workstation.
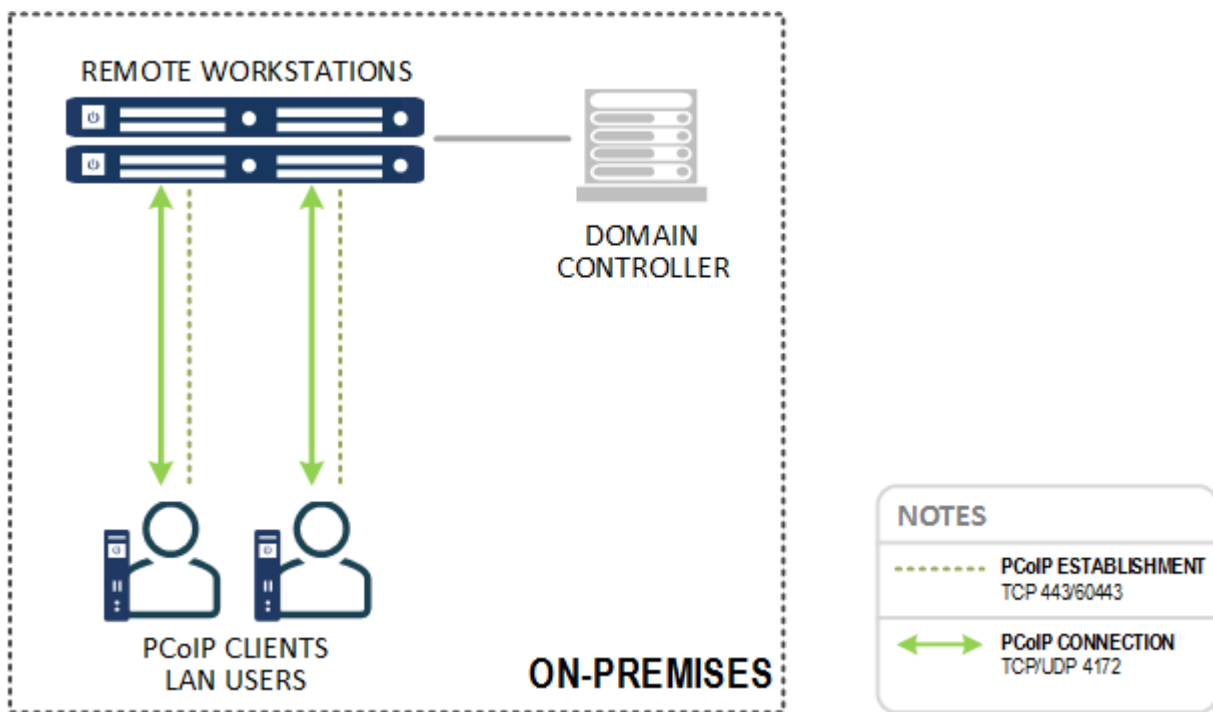

Each PCoIP Client connects to PCoIP Agent software executing as a service on a remote workstation. To learn more about PCoIP Clients, see PCoIP Clients. To learn more about PCoIP Agents, see PCoIP Agents.

Overview

Cloud Access Manager is a Software-as-a-Service (SaaS) offering included with Cloud Access subscriptions that enables highly-scalable and cost-effective Cloud Access Software deployments. The Cloud Access Manager solution is comprised of two main components:

- **Cloud Access Manager Service**: This is a service offered by Teradici to manage Cloud Access deployments.

- **Cloud Access Connector**: This access hub is deployed in the customer environment and facilitates user authentication and machine entitlement of remote workstations or desktops located in AWS, Google Cloud, Microsoft Azure or on-premises.

Cloud Access Manager enables you to install multiple Cloud Access Connectors in multiple cloud regions as well as in an on-premises environment.
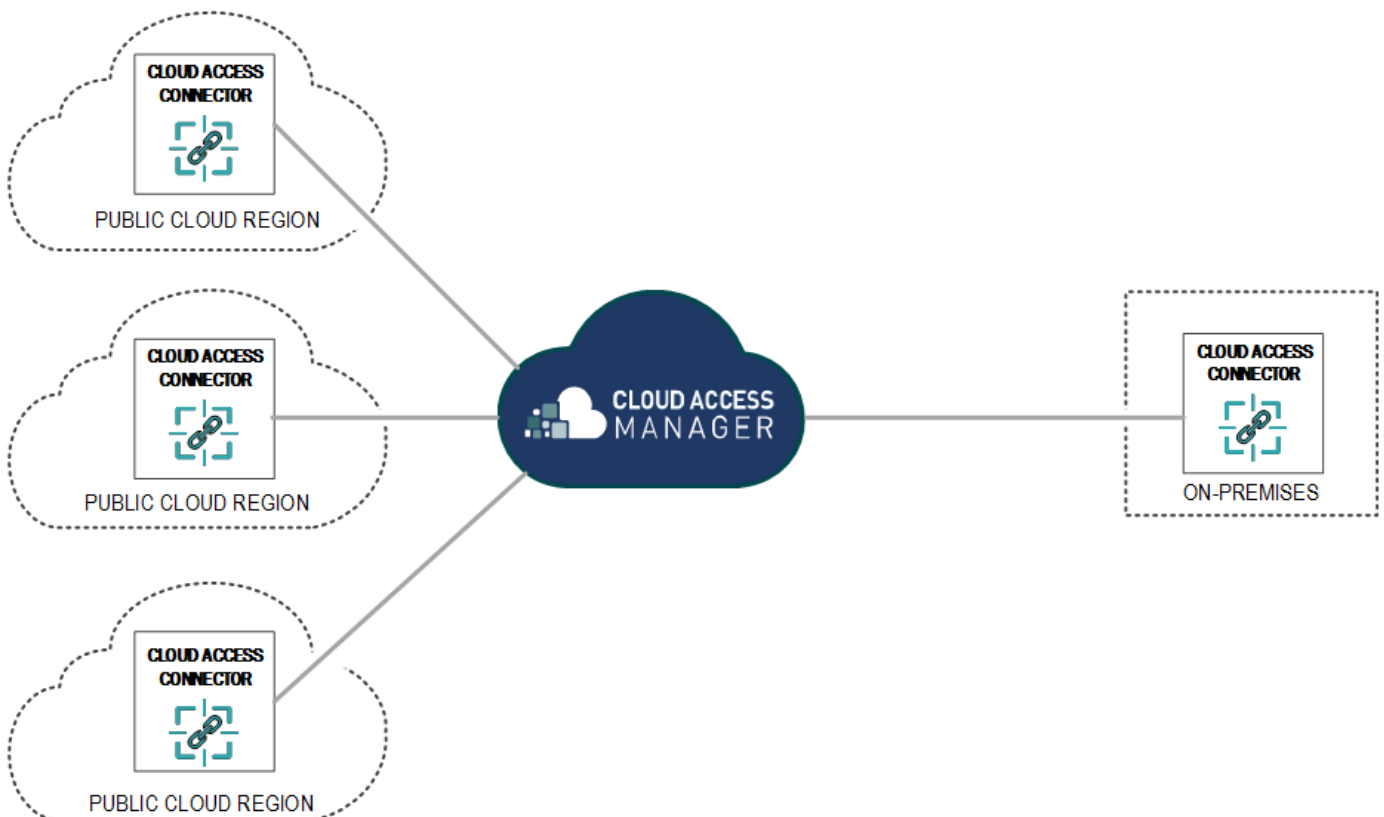

In addition to managing cloud compute costs, Cloud Access Manager handles user entitlement, authentication (including RADIUS-compatible multifactor authentication (MFA)) and brokering of

connections during PCoIP session establishment. The Cloud Access Connector enables external users to access their remote desktops without the complexity of endpoint VPNS.

For more information on Teradici Cloud Access Manager, see Cloud Access Manager.

Managed Connections for On-site LAN Users

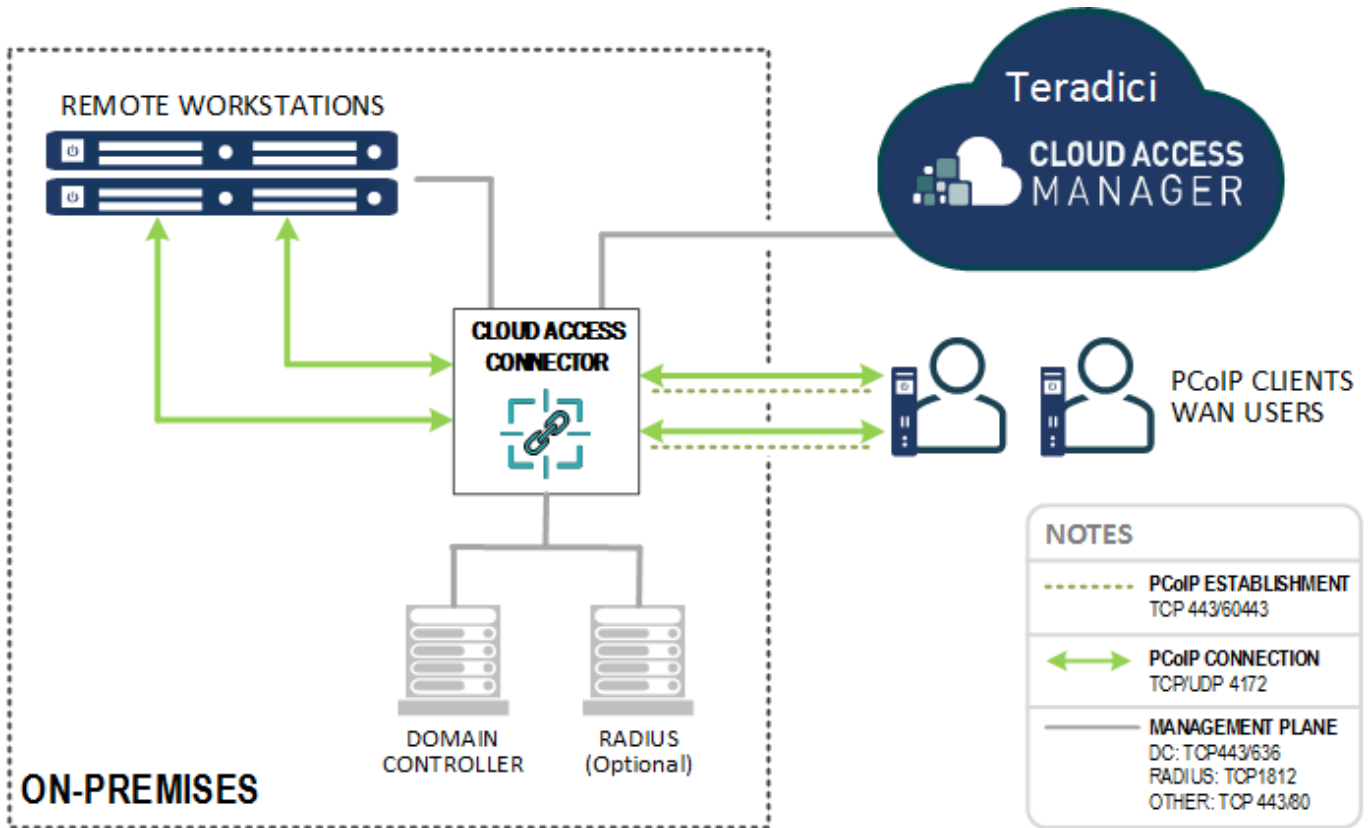LAN Users connect to an internally published IP address of the Cloud Access Connector.
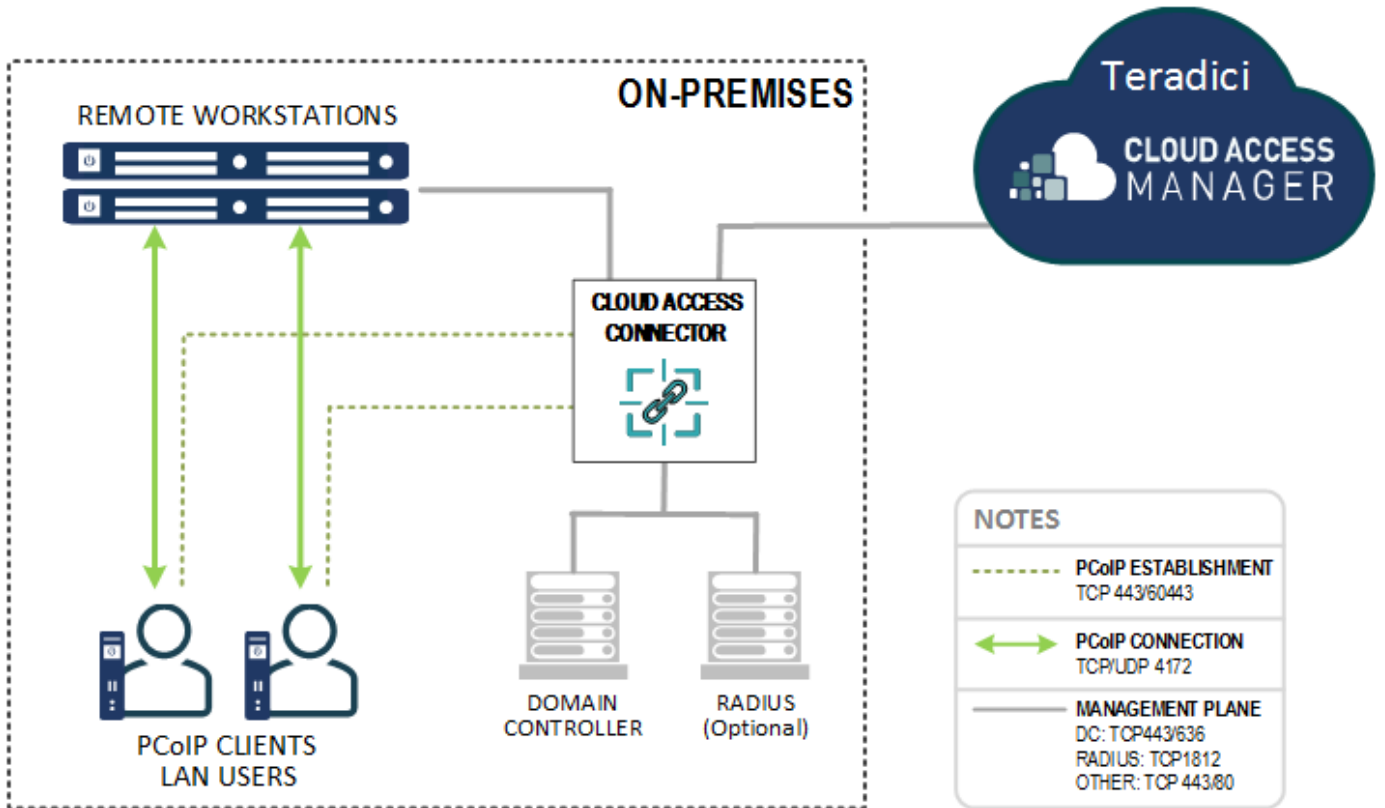
Cloud Access Connector configuration details are described in the Cloud Access Manager Administrators guide.

Managed Connections for WAN Users Connecting On-Premises

Off-site WAN users wishing to connect to on-premises remote workstations connect to an externally published IP address of the Cloud Access Connector.

> ✏️ **Cloud Access Connector DMZ Deployment**
>
> The Cloud Access Connector is conventionally deployed in a DMZ or semi-trusted zone (not shown in the diagram) and may be coupled with a reverse proxy to facilitate load balancing.
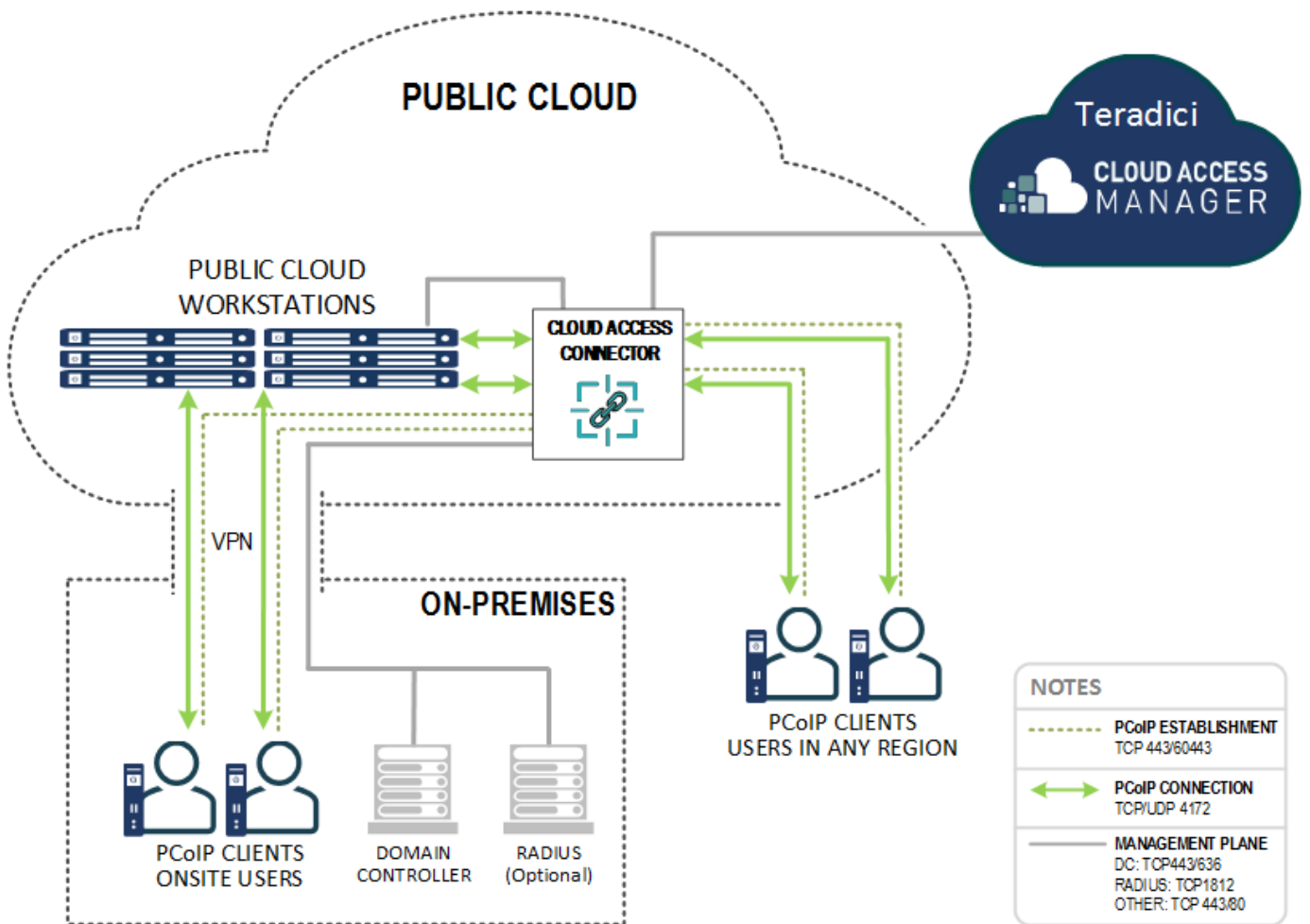

> 🔥 **TCP 60443**
>
> Teradici recommends using TCP 60443 for internal connections. It is not mandatory for TCP 60443 to be opened to the public network.

Cloud Access Connector configuration details are described in the Cloud Access Manager Administrators guide.

Managed Connections for Public Cloud Workstations

Cloud Access Manager supports connections to public cloud workstations. By deploying the Cloud Access Connector in your preferred public cloud (in one or more regions and/or multiple public clouds), you can provide your on-site users with public cloud workstations or support users across different geographic regions with the nearest public cloud workstations. By choosing public cloud workstations situated geographically close to your remote users, the user experience is optimized.
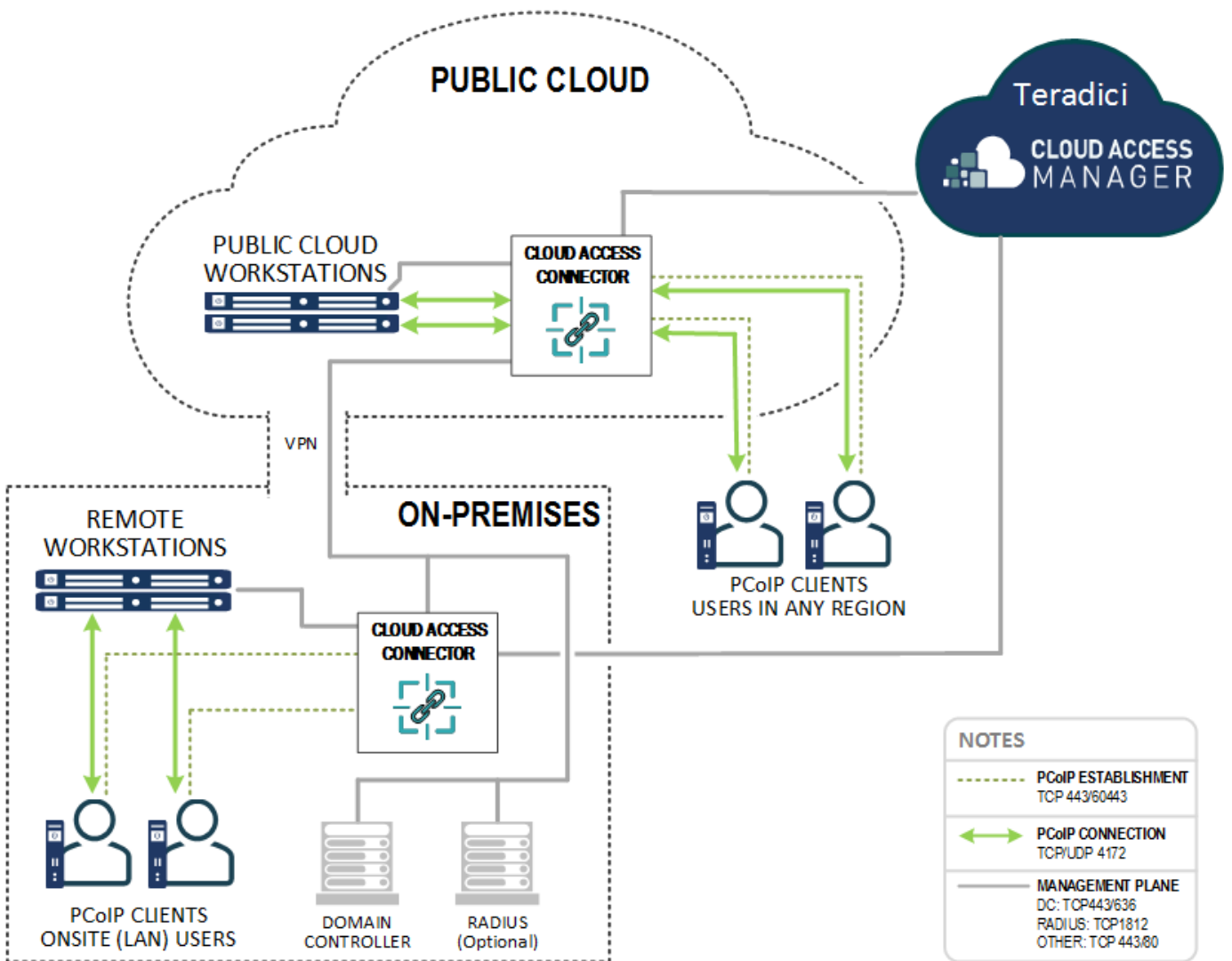

> 🔥 **TCP 60443**
>
> Teradici recommends using TCP 60443 for internal connections. It is not mandatory for TCP 60443 to be opened to the public network.

Cloud Access Connector configuration details are described in the Cloud Access Manager Administrators guide.

Managed Connections for Multicloud Workstations

Cloud Access Manager supports hybrid multicloud deployments comprising a combination of on-premises remote workstations (e.g. on VMware ESXi or KVM) and public cloud workstations in your preferred public cloud (in one or more regions and/or multiple public clouds). This is achieved by deploying the Cloud Access Connector both on-premises and in one or more public clouds. By choosing public cloud workstations situated geographically close to your remote users, the user experience is optimized.
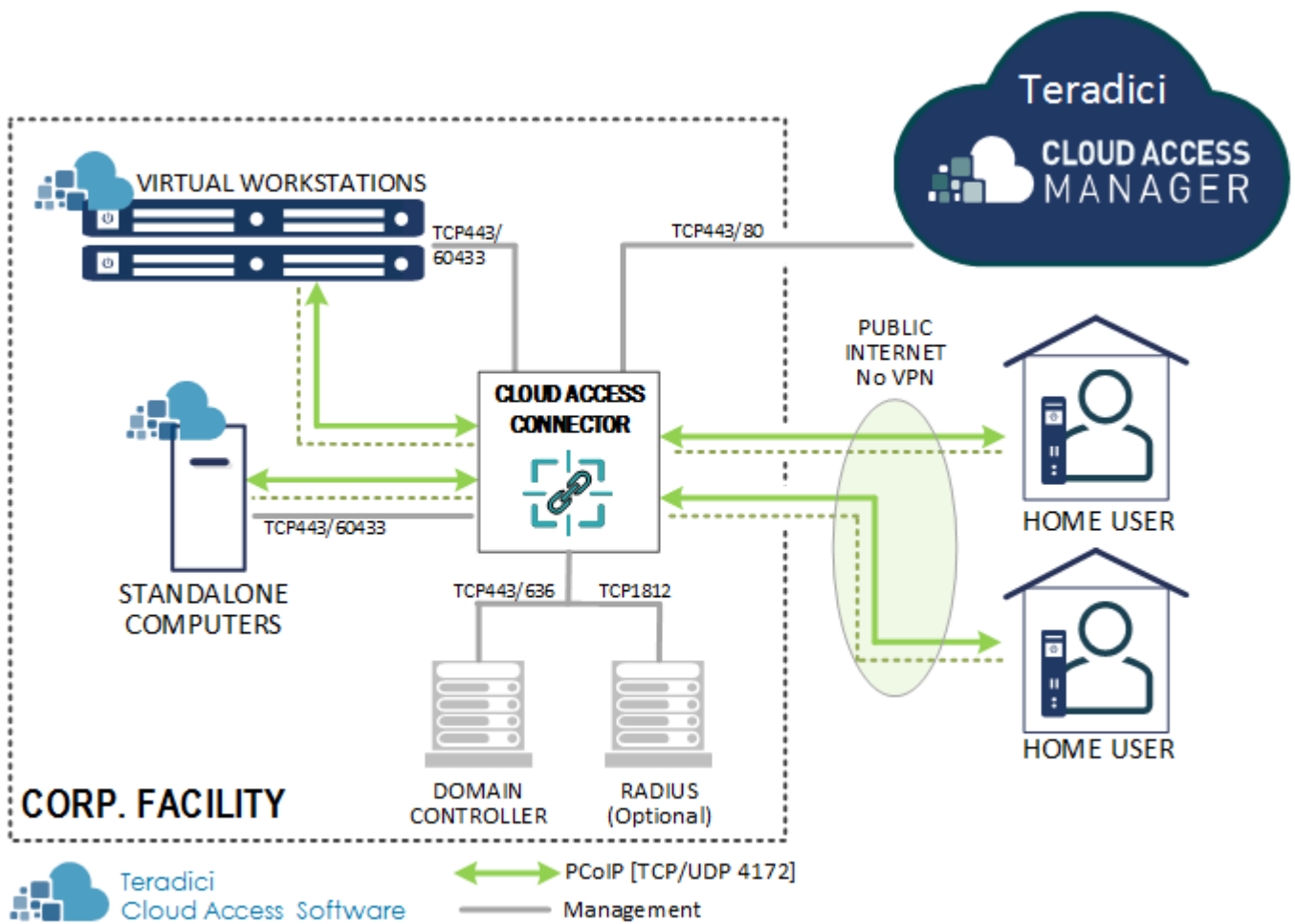
> 🔥 **TCP 60443**
>
> Teradici recommends using TCP 60443 for internal connections. It is not mandatory for TCP 60443 to be opened to the public network.

Cloud Access Connector configuration details are described in the Cloud Access Manager Administrators guide.

Work-from-Home Options with Cloud Access Software

Teradici Cloud Access Software can offer a number of different solutions to your corporate work-from-home demands. The following image outlines a top-level architecture of the Work-from-Home scenario with Cloud Access Software:

> 🔥 **TCP 60443**
>
> Teradici recommends using TCP 60443 for internal connections. It is not mandatory for TCP 60443 to be opened to the public network.

For an in-depth view of our work-from-home offerings, please see our Work-from-Home Rapid Response Guide.

This guide outlines:

- Work-from-Home options for Standalone Computers.

- Work-from-Home options with Remote Workstation Cards.

- Work-from-Home options with Cloud Access Software.

- Work-from-Home options for VMware Horizon.

- Performance Tips for Work-from-Home Use Cases.

Load Balancer Solutions

Load balancers may be added to a Cloud Access Software deployment to distribute system and to optimize performance.

Using Load Balancing for On-Premises Deployments

The following diagram outlines a load balancing scenario for a Cloud Access Software deployment with Cloud Access Manager integration.
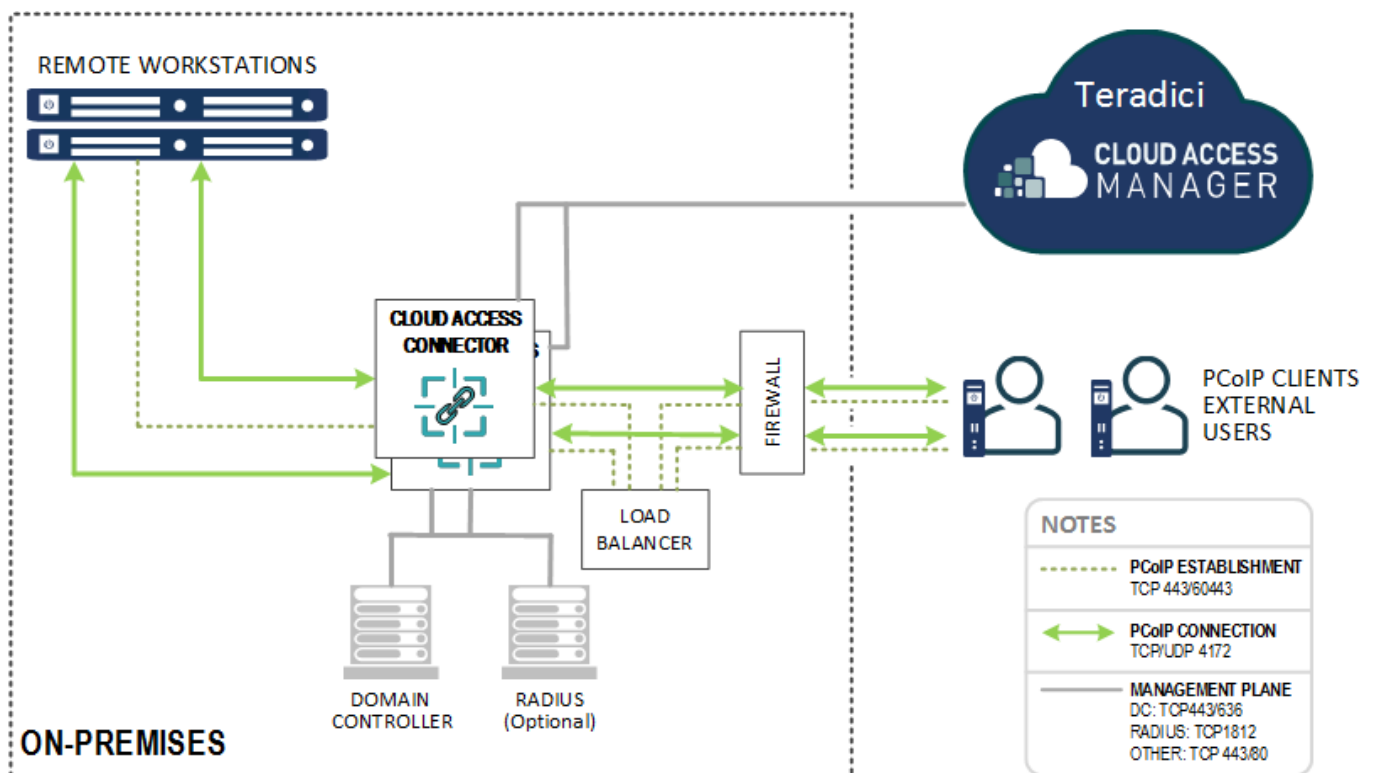
Load balancers must support both HTTP and sticky sessions (jsessionid). During the session establishment phase, the Cloud Access Connector passes it's `ExternalRoutableIP` configuration value to the PCoIP Client. After the session has been established, the PCoIP Client uses the provided IP address to communicate directly with the Cloud Access Connector. TCP Ports 443/60443 can be opened for session establishment.

> 🔥 **TCP 60443**
>
> Teradici recommends using TCP 60443 for internal connections. It is not mandatory for TCP 60443 to be opened to the public network.

> 🔥 `ExternalRoutableIP` **must point to the Cloud Access Connector**
>
> If the `ExternalRoutableIP` setting is configured to point to the load balancer instead of the Cloud Access Connector, the load balancer may direct the PCoIP Client to the incorrect Cloud Access Connector on the wrong server and the PCoIP Client will not be able to establish a session.

> 🔥 **Cloud Access Connector Public IP Addresses**
>
> In the above configuration, each Cloud Access Connector must have a unique public IP address and it must be routable externally for port 4172.

Load Balancer Session Planning

The number of users allocated per individual Cloud Access Connector varies according to user type and considerations such as display topology and resolution. At present, the throughput of PCoIP traffic through an individual Cloud Access Connector is limited to approximately 400 Mbps. As an example, a typical 1080p VDI workloads demanding less than 5 Mbps per session would allow in excess of 80 concurrent sessions per Cloud Access Connector instance. In contrast, a 4K/ UHD video editorial user or VFX artist may require upward of 50 Mbps on average, limiting each Cloud Access Connector instance to less than 10 concurrent sessions.

Third Party Connection Brokers

Cloud Access Software is fully compatible with third-party brokers without the deployment of Cloud Access Connector or features included with Cloud Access Manager. Consult third party documentation for pricing and deployment details. When using a third-party connection broker, PCoIP connections are brokered in conjunction with the Teradici Connection Manager and Security Gateway, see Connection Manager and Security Gateway. Please consult the third-party broker documentation for information on what what deployment architectures are supported.
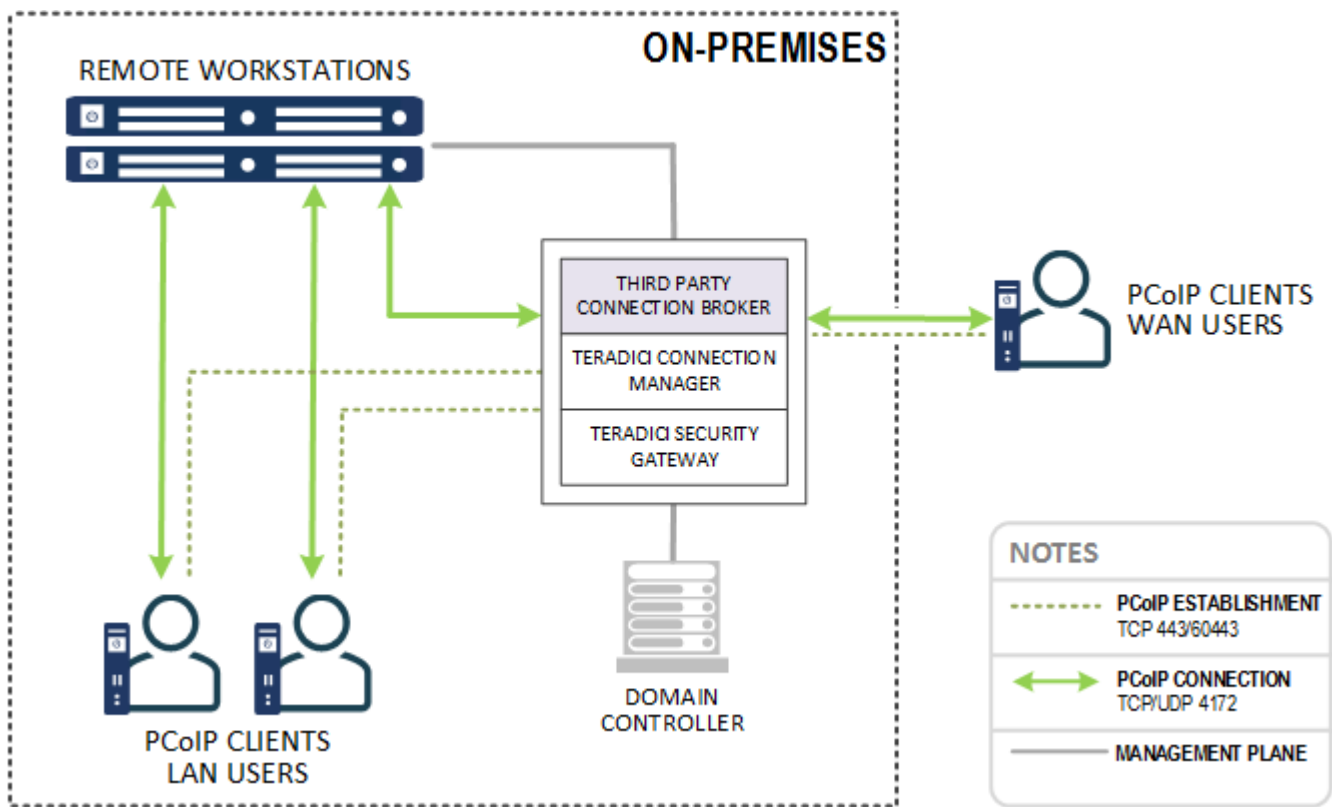
TCP 60443

Teradici recommends using TCP 60443 for internal connections. It is not mandatory for TCP 60443 to be opened to the public network.

Licensing Models for Cloud Access Software

Cloud Access Software is supported by two licensing models. Each model requires a specific license type:

- **Teradici Cloud Licensing Service:** These licenses should be used if your PCoIP agent has access to the internet.

- **License Server based licenses:** These licenses should be used if your PCoIP agent runs in a restricted environment and does not have access to the internet.

Most PCoIP deployments can take advantage of the automated Teradici Cloud Licensing Service which eliminates the complexity of on-premises licensing infrastructure. If your deployment cannot use cloud licensing, either because the site is not connected to the public internet or local management of licenses is necessary then License Server based licensing may be the appropriate licensing model.
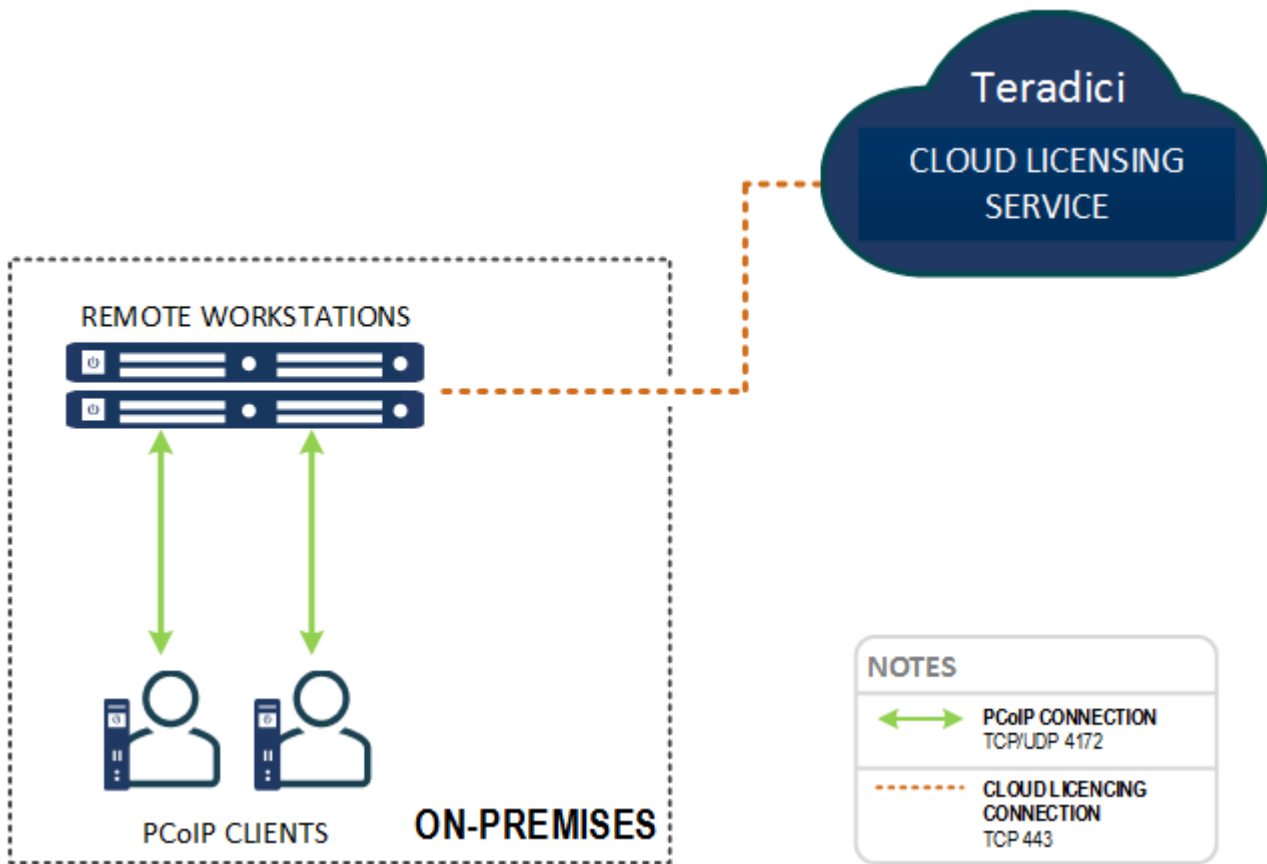
> 🔥 **Whitelisting the Licensing URLs**
>
> If the remote workstation does not have internet access you can whitelist the licensing URLs and and still use cloud licensing, see Teradici Cloud Licensing - Whitelisting FAQ

Cloud Licensing Service for On-Premises
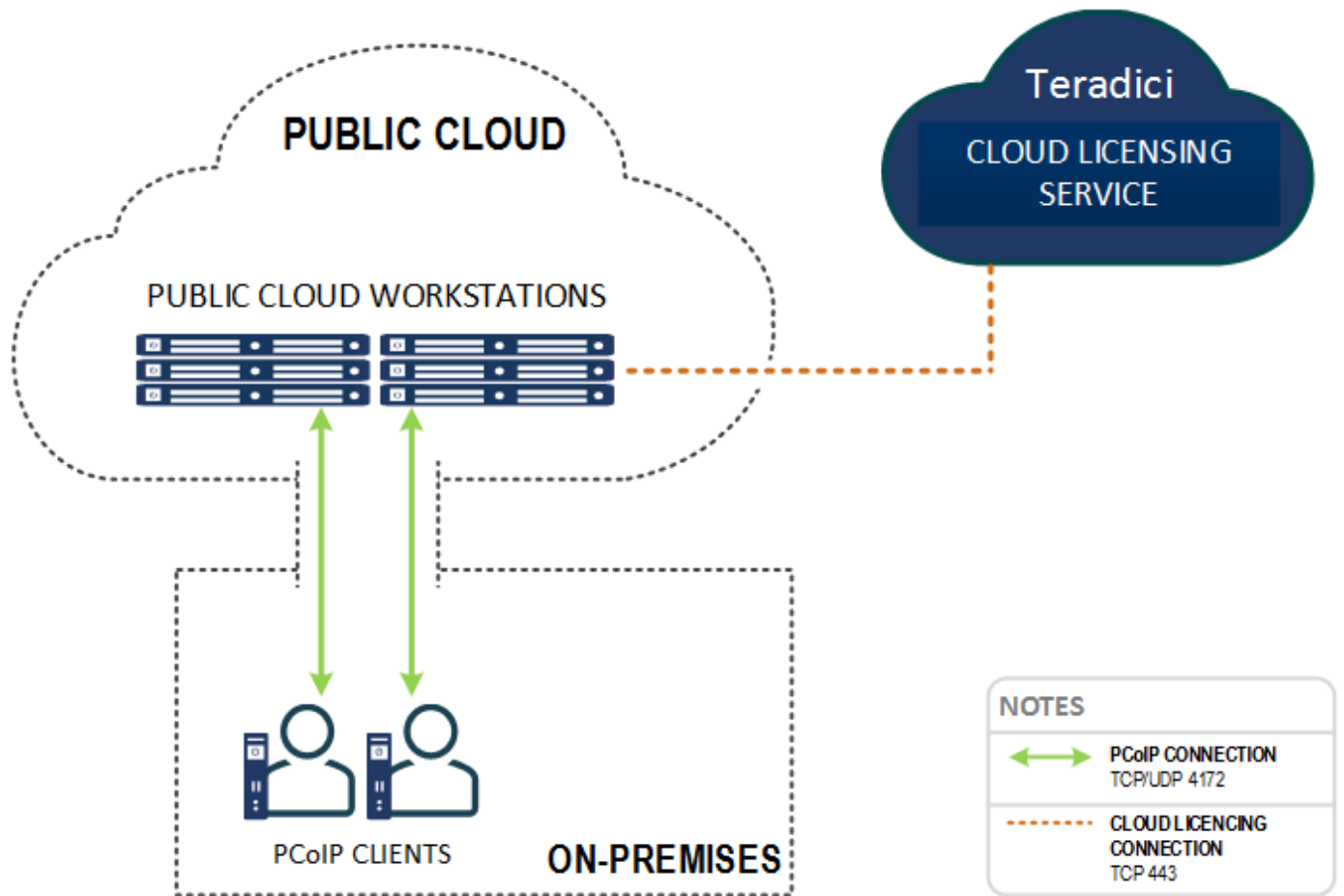
The following image outlines the Cloud Licensing Service model for an on-premises scenario.

Cloud Licensing Service on the Public Cloud

The following image outlines the Cloud Licensing Service model for a public cloud scenario.

PCoIP License Server Model

The following image outlines the PCoIP License Server model. The License Server can be used either online and offline.
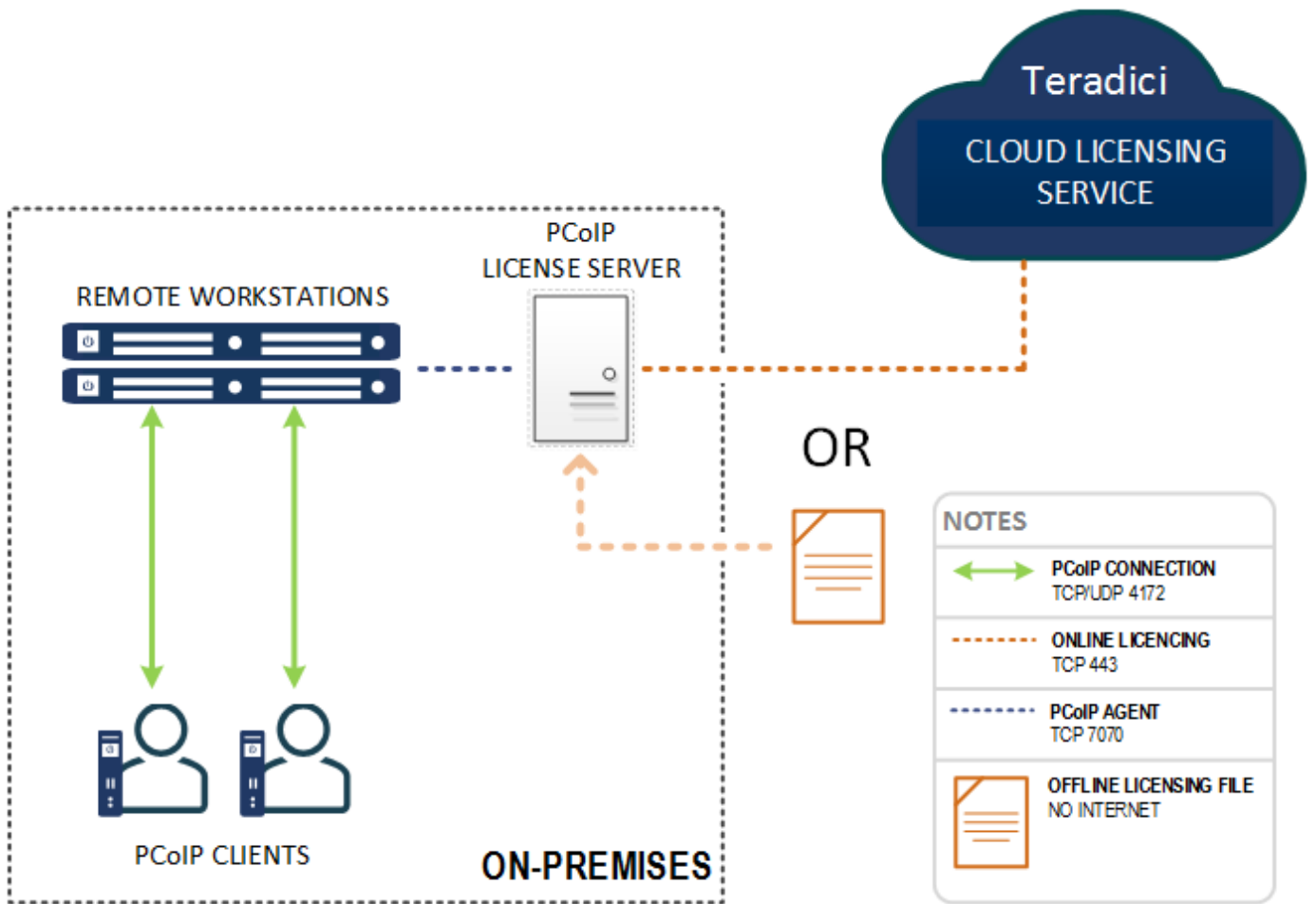
For information on the Teradici License Server, see Teradici License Server.

For more information on these licensing options, see System Requirements for Licensing.

Security Features

Cloud Access Software incorporates features that maximize the security of any deployment model, including on-premises, hybrid or public cloud architectures:

- RADIUS-based multi-factor authentication (MFA).

- All PCoIP components use security certificates to ensure a trusted, end-to-end Transport Layer Security (TLS) connection for TCP communications.

- The PCoIP UDP protocol is encrypted with industry-standard secure AES-256 encryption.

- Cloud Access Connector ensures secure PCoIP traffic flow between external and internal networks.

- The PCoIP protocol is host-rendered and no data ever leaves the remote workstation, except encrypted pixels.

Firewall Settings

The PCoIP protocol uses ports UDP:4172, TCP:4172 and either TCP:443 or TCP:60443 as preferred. These ports must be open to allow the flow of PCoIP traffic through the firewall. For an in-depth look at the port settings for different environments relating to Cloud Access Software, PCoIP Management Console and PCoIP Zero Clients, see the following KB Article.

Security Certificates

Certificates are used to ensure that all communication endpoints are trusted. All communications between PCoIP components are performed over encrypted secure channels that use certificates for validation.

Disaster Recovery

Business continuity can take many forms. Whether it be a bank processing transactions without interruptions, a retail store transacting sales at point of sale terminals, or universities running computer labs with zero downtime, business continuity is important to every type of organization. Downtime can result in significant losses in revenue or permanent damage to a brand's reputation.

Cloud Access Software from Teradici is a perfect option and solution to base your companies and organizations disaster recovery plan around. For detailed information on ow to use Cloud Access Software as part of your disaster recovery strategy, see Disaster Recovery for Virtual Desktops.

Isolating a Secure Content Network

Major media and entertainment corporations rely on the PCoIP protocol to conform with MPAA (Motion Picture Association of America) and CDSA (Content Delivery and Security Association) best practices in addition to meeting Trusted Partner Network (TPN) compliance obligations. Media assets are securely isolated on production networks, only accessible from authorized network endpoints as an AES-256 encrypted stream of pixels. As media assets themselves are never downloaded to the endpoints, intellectual property remains secured, no matter what applications are used, as outlined in the image below.
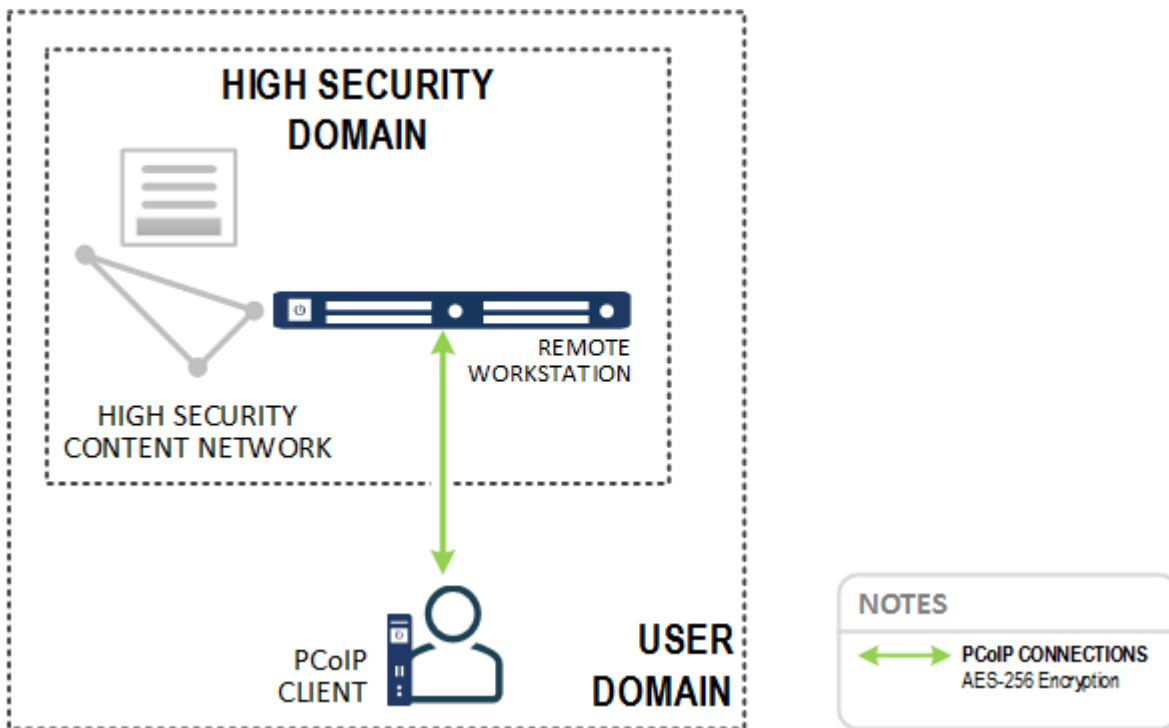
Accessing the Public Internet from an Isolated Workstation

Users inside highly secured enterprises, such as TPN certified environments or those compliant with MPAA or CDSA best practices, may require the public internet for access to media assets or other information. Cloud Access Software enables isolated remote workstations, such as those attached to content networks, to access the public internet via back-to-back PCoIP connections as outlined in the image below.
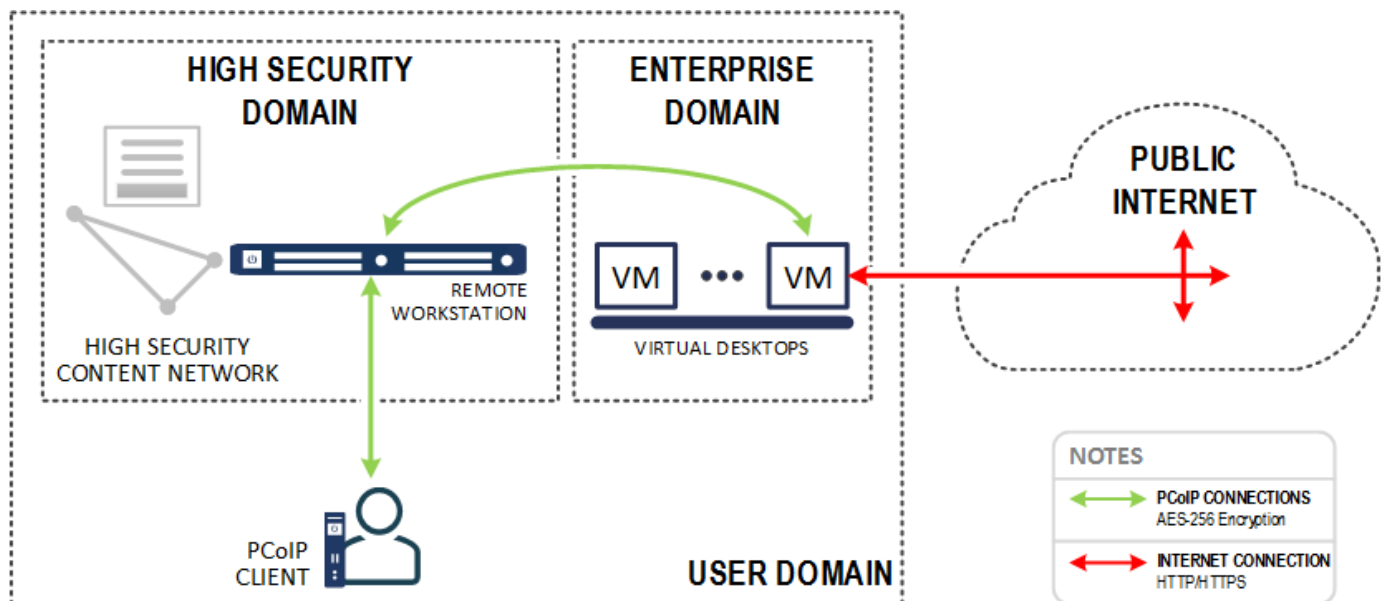
Referring to the diagram above, the secured remote workstation is deployed with both PCoIP Agent software and PCoIP Client software. While the PCoIP Agent software serves encrypted pixels to the user at the PCoIP Client, a second PCoIP Agent deployed on a generic virtual desktop outside the high security domain serves the remote workstation with the internet browser image of the virtual desktop, also in the form of encrypted pixels. Such an architecture which is supported on both Linux and Windows remote workstations, ensures that the airgap perimeter of the high security domain is only traversed with encrypted pixels which adheres to compliance practices.

Public Cloud Implementations

Cloud Access solutions can be implemented and deployed on Microsoft Azure, AWS and Google Cloud environments, as well as on-premises. The following section points to reference information on these cloud vendors, specifically looking at the platform architectures.

Cloud Access on Microsoft Azure

For general information on Microsoft Azure's cloud architecture, see Azure Architecture Center.

For information about graphics processing options for Microsoft Azure, see https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-gpu#nv-series

For information on the system requirements for Cloud Access on Microsoft Azure:

- Graphics Agent for Windows - System Requirements

- Standard Agent for Windows - System Requirements

- Graphics Agent for Linux - System Requirements

- Standard Agent for Linux - System Requirements

Cloud Access on AWS

For general information on AWS's cloud architecture, see https://docs.aws.amazon.com/index.html#lang/en_us

For information around building a GPU workstation on AWS with Cloud Access Solutions, see https://aws.amazon.com/blogs/compute/building-a-gpu-workstation-for-visual-effects-with-aws/

For information on AWS cloud video editing with Teradici Cloud Access, see https://aws.amazon.com/quickstart/architecture/cloud-video-editing/

For information on AWS cloud VFX workstations with Teradici Cloud Access, see https://aws.amazon.com/quickstart/architecture/vfx-workstations-with-teradici/

For information on the system requirements for Cloud Access on AWS:

- Graphics Agent for Windows - System Requirements

- Standard Agent for Windows - System Requirements

- Graphics Agent for Linux - System Requirements

- Standard Agent for Linux - System Requirements

Consume Cloud Access Software using pre-configured machine images with integrated billing, available through our cloud partner marketplaces: https://aws.amazon.com/marketplace/search/?filters=vendor_id&vendor_id=04ffecf1-f40e-4387-b015-59428958d233&category=2649340011

Cloud Access on Google Cloud

For general information on Google Cloud's cloud architecture and products, see https://cloud.google.com/docs/

For information around building a virtual linux workstation on Google Cloud with Cloud Access Solutions, see https://cloud.google.com/solutions/creating-a-virtual-gpu-accelerated-linux-workstation

For information on the system requirements for Cloud Access on Google Cloud:

- Graphics Agent for Windows - System Requirements

- Standard Agent for Windows - System Requirements

- Graphics Agent for Linux - System Requirements

- Standard Agent for Linux - System Requirements

Consume Cloud Access Software using pre-configured machine images with integrated billing, available through our cloud partner marketplaces:

- Windows: https://console.cloud.google.com/marketplace/details/teradici-public/teradici-cloud-access-software-windows-2016

- Linux: https://console.cloud.google.com/marketplace/details/teradici-public/teradici-cloud-access-software-centos

Using Third Party Connection Brokers

Cloud Access Software is fully compatible with third-party brokers without the deployment of Cloud Access Connector or other features included with Cloud Access Manager. Consult third party documentation for pricing and deployment details. For more information on the Teradici Connection Manager and Security Gateway, see Connection Manager and Security Gateway.

The third-party connection broker specifies the authentication method used in advance of secure PCoIP session establishment. These authentication methods include the use of passwords, tokens, disclaimers and dialogs. Consult third party documentation for further details.

PCoIP Clients

The PCoIP Client is a standalone hardware device or software application that enables the user to connect to the remote workstation. The PCoIP Client decodes a stream of PCoIP pixels from the remote workstation and presents the results to the user. The PCoIP Client is offered in different forms, including PCoIP Zero Clients, iOS, Android and Chrome OS mobile clients and software clients compatible with Windows, Linux and macOS operating systems.

PCoIP Zero Clients   Mobile Clients   Software Clients

For more information on the PCoIP Clients, see the following guides:

- PCoIP Zero Client Administrators' Guide

- PCoIP Software Client for Windows Administrators' Guide

- PCoIP Software Client for Mac Administrators' Guide

- PCoIP Software Client for Linux Administrators' Guide

> ✏️ **Other PCoIP Compatible Clients**
>
> Other PCoIP-compatible clients are available through OEM partners, resellers, and developers, such as a Teradici PCoIP Zero Client or a PCoIP-optimized thin client.

PCoIP Agents

The PCoIP Agent is a standalone software application installed on a virtual computer or remote workstation that will securely encode the desktop and efficiently stream pixels-only to the PCoIP Client. There are different versions of agents available for supporting both standard and graphics PC architectures. PCoIP Agents are available for Windows and Linux platforms.

PCoIP Graphics Agent

A PCoIP Graphics Agent leverages a discrete graphics processor and associated 3D APIs, including OpenGL and DirectX, The PCoIP Graphics Agent is optimized for the latest GPUs, including NVIDIA GRID GPUs supporting NVIDIA Capture SDK and AMD GPUs supporting AMD RapidFire SDK.

PCoIP Standard Agent

A PCoIP Standard Agent provides each user with a dedicated remote desktop. A PCoIP Standard Agent is optimized for VDI, DaaS, and cloud deployments. A PCoIP Standard Agent does not support GPU-accelerated 3D graphics.

For more information on the PCoIP Agents and supported operating systems, see the following guides:

- Graphics Agent for Windows - System Requirements
- Standard Agent for Windows - System Requirements
- Graphics Agent for Linux - System Requirements
- Standard Agent for Linux - System Requirements

Cloud Access Manager

Cloud Access Manager is a deployment provisioning and management solution for Cloud Access Software. The Cloud Access Manager Service is a service offered by Teradici to manage Cloud Access Manager deployments. The Cloud Access Manager Service works in conjunction with the Cloud Access Connector.

For more information on how Cloud Access Manager can provision and manage your solution with Cloud Access Software, see Solutions for Managed Connections with Cloud Access Manager.

For more information on Cloud Access Manager, see Cloud Access Manager.

Cloud Access Connector

The Cloud Access Connector is an access hub installed in the customer environment which facilitates PCoIP Client connections to remote workstations. The Cloud Access Connector operates in conjunction with the Teradici Cloud Access Manager Service to provide user authentication and entitlement for remote workstation access, including MFA. For more information on the Cloud Access Connector, see Cloud Access Manager.

PCoIP Licensing

Teradici cloud licensing simplifies the deployment and activation of Cloud Access licenses. Cloud licensing avoids the need to deploy and maintain a license server. Whether you are a new Cloud Access Software administrator, or upgrading your existing Cloud Access Software deployment, licenses are now much easier to obtain and manage.

If your users have internet access from their host VMs, you should be using cloud licensing. It's simple to deploy and easily managed, avoids the need for a license server,and supports internet proxy services. If your users do not have internet access (and you cannot use a proxy), use a license server. Although the license server requires installation and maintenance, you can manage your licenses from a single location and easily license new VMs

For a more detailed view of operating system requirements, memory recommendations, socket configuration recommendations, port configuration and bandwidth and CPU recommendations for the PCoIP License Server, see the guide listed below:

- Teradici PCoIP License Server 2.1 Administrators' Guide

PCoIP Management Console

PCoIP Management Console allows IT administrators to quickly provision new Zero client devices, review metrics, configure settings, update firmware, and view event logs. For more information on the Management console, see PCoIP® Management Console Administrators' Guide.

PCoIP Virtual Channel SDK

The PCoIP Virtual Channel Software Development Kit (SDK) enables developers to build custom PCoIP Virtual Channel plug-ins for PCoIP sessions. You can implement PCoIP Virtual Channel functionality as a plug-in to send encrypted data between servers and client endpoints during an active PCoIP session.

The PCoIP Virtual Channel Application Programming Interface (API) is available as an optional add-on to solution developers who want to extend the types of traffic flowing through the PCoIP session, such as clipboard redirection, local printing, and customised device support.

The PCoIP Virtual Channel SDK supports up to 15 virtual channels and once a customer's use case is established can be accessed, and utilised.

Required Knowledge

A developer should have an understanding of how the PCoIP protocol works, have knowledge of C++/C, Visual Studio and CMake. Building plugins for other platforms requires the SCons software construction tool which in turn supports Python, a gcc compiler or a corresponding toolchain which supports the pthreads library. Developers can use CMake to configure and generate platform and compiler specific build files and build the target plugins across all platforms. Customers can also engage with the Teradici Professional Services team to build these plugins. For information on this, see here.

> ⚠️ **Support for Customization Components**
>
> Teradici recommends consulting the PCoIP Agent and PCoIP VChan SDK documentation for the install, upgrade and uninstall of the PCoIP VChan plugins. There is no support from Teradici's GSS team for customization components such as SDKs and APIs. If customers require support from GSS for these components they are required to purchase Premium/Developer Support from Teradici.

For Third Party Brokers

For a list of PCoIP-compatible connection brokers available from third party vendors, see Commercial Third-Party Brokers on the Teradici support site. As an alternative to using a third party connection broker, Teradici Cloud Access Manager is a cloud service included with Cloud Access subscriptions that simplifies and automates Cloud Access Software deployments, including connection broker services. For more information on Cloud Access Manager, see Cloud Access Manager.