

Teradici Work-From-Home Rapid Response Guide

For access to the full Teradici product documentation visit [Teradici Support](#).

Scope

This guide enables IT administrators to rapidly determine if Teradici offers any immediate solutions to your pressing corporate work-from-home demands. All options are summarized and linked to detailed resources to help you get going as quickly as possible.

Does Teradici technology meet my needs?

The PCoIP protocol is highly trusted and broadly deployed with over 13 million endpoints across many industries including Media and Entertainment, Finance, Governments, CAE, Healthcare, IT and many others!

Teradici products have a significant footprint in industries that demand ultra-secure remote access to standard desktops or workstations delivering graphics intensive workloads. We have customers across all sectors initiating work-from-home initiatives at short notice. In particular, companies in the Media and Entertainment Industry rely on PCoIP Protocol to meet Motion Picture Association of America (MPAA) content security best practices or to maintain Trusted Partner Network (TPN) compliance.

Where to Start?

- If you're new to PCoIP and Teradici remote desktop technology, start [here](#).
- If you're wanting remote access to any standalone corporate computers, start [here](#).
- If you're already using Teradici Remote Workstation Cards and PCoIP Zero Clients, start [here](#).
- If you're already using the PCoIP Management Console, start [here](#).
- If you're already using Teradici Cloud Access Software, start [here](#).
- If you're already using PCoIP Zero Clients with VMware Horizon, start [here](#).

- If you're already using PCoIP Zero Clients with Amazon WorkSpaces, start [here](#).
- If you are looking for performance tips to optimize your Cloud Access Software deployment for work-from-home access, start [here](#).
- For detailed instructions on using Teradici Cloud Access Software for standalone computers, see this [KB article](#).
- For detailed instructions on using Teradici Cloud Access Software for consumer grade NVIDIA GPUs (e.g. GeForce RTX 2080), see this [KB article](#).

To get started immediately, Cloud Access (standard) or Cloud Access Plus (graphics) licenses can be purchased by credit card from the Teradici website . For larger deployments, please contact [Teradici Sales](#) or a [Teradici reseller](#).

This might actually work! What should I do next?

There are links to additional resources at the end of this guide, including security and performance considerations, customer stories , reference architectures, technical guides, licensing options and Teradici contact information.

Welcome to Teradici Solutions

Teradici Cloud Access Software enables remote access to Windows or Linux based computers including:

- Physical workstations or standalone computers (either deskside or centralized).
- Virtual workstations on VMware ESXi; KVM or Nutanix AHV Hypervisors.
- Non-graphics virtual desktops on VMware ESXi; RedHat KVM or Nutanix AHV Hypervisors.
- Remote workstations that reside on the public cloud.

Using Cloud Access Software, a small software agent is installed on any of the above 'host' computer variants. The host computer then uses the Teradici PCoIP protocol to communicate with a client device in a remote location over a LAN, WAN or public internet. The client device is connected to display, keyboard, mouse and peripheral devices such as WACOM tablets, and is what end users interact with.

Teradici also offers a well-established range of PCIe cards, called **Remote Workstation Cards**, that plug into physical workstations and convert the DVI or DisplayPort signals into the same PCoIP protocol used by Cloud Access Software. PCoIP Remote Workstation Cards are excellent for LAN environments and support a broad range of GPUs, including consumer and professional variants. However, they are less flexible than Cloud Access Software for Work-from-Home deployments. Firstly, you'd need to procure and install the hardware which might lengthen your deployment schedule. You'll also need to establish VPN access for all remote users which may not be viable.

New to Teradici Solutions Q&A

How much does it cost?

Check out our web page on [All Access Software Plans](#).

Which GPUs are supported for high performance requirements?

- [Supported GPUs for Windows machines](#)
- [Supported GPUs for Linux machines](#)

What if I have a different graphics card or integrated graphics?

Cloud Access Software can be used for remote access to a variety of other computers and graphics cards, for example NVIDIA GeForce graphics card, subject to some performance constraints. See this [KB article](#) for more information.

What are the endpoint options for my users?

PCoIP Software clients are available for Windows, macOS, and Linux and can be installed on laptops or PCs. Standalone hardware clients such as PCoIP Zero Clients and PCoIP Thin Clients are offered by many vendors.

Work-from-Home options for Standalone Computers

Graphics Workstations with NVIDIA Quadro and Tesla GPUs

Cloud Access Software has longstanding support for select non-virtualized Windows or Linux workstations as called out in the GPU Requirements for Cloud Access Software [Windows](#) or [Linux](#) systems. Read [here](#) for further details on deploying Cloud Access Software.

Other Standalone Computers running Windows with consumer grade GPUs

To support our many customers with an urgent need for remote access to standalone or deskside corporate computers with consumer grade graphics, please review the following [KB article](#).

Other Standalone Computers running Linux with consumer grade GPUs

The best option for remote access to standalone Linux workstations is to use Teradici Remote Workstation Cards in conjunction with a VPN, as described [here](#).

Security Considerations for Graphics-based Deskside Computers

When remote access is provided to a workstation or computer using the PCoIP Graphics Agent, its local monitors remain active and visible to bystanders during the remote session which poses a local security risk. Local keyboards and mice also remain active and usable by anyone standing near them.

To mediate this risk, Teradici recommends that you:

- Turn off local monitors and leave them attached or disconnect local monitors and replace them with virtual monitor dongles, as described in the following [KB article](#).
- Unplug the local keyboard and mouse.

Usability and Performance of Standalone Computers using PCoIP Standard Agent

When remote access is provided to a standalone computer using the PCoIP Standard Agent, it can only be operated via a PCoIP client. Local operation of the computer is not possible until the PCoIP

Standard Agent is removed. Monitor security is not a concern in this case because the local display system is disabled during a remote session. No virtual monitor emulation emulator is needed.

GPU-dependent Applications

The PCoIP Standard Agent cannot make use of GPUs, so any GPU-dependent applications running on a standalone PC will not function properly. If you have GPU-dependent workloads, you must use the PCoIP Graphics Agent.

Teradici also recommends unplugging your local keyboard and mouse which remain active during a remote session.

For instructions on how to use Cloud Access Software with Standalone Computers, see the following [KB article](#).

Work-from-Home options with Remote Workstation Cards

	VPN Access	Public Internet Access
Windows	Described here	Disconnect Remote Workstation Card and use Cloud Access Software
Linux	Described here	Disconnect Remote Workstation Card and use Cloud Access Software*

*This does not apply to workstations with consumer grade GPUs.

VPN Option

A VPN enables external connections to an enterprise-based workstation with Remote Workstation Card by extending the corporate network to the home environment over a secure connection. The decision to deploy a VPN should be weighed against alternative approaches such as using Teradici Cloud Access Software. PCoIP connections and communications are inherently secure so adding a VPN may unnecessarily expose corporate infrastructure.

It also add licensing costs and may degrade the performance of the remote desktop. When deploying a PCoIP Zero Client in a work-from-home scenario, home users would require a home router with VPN support because a PCoIP Zero Client has no operating system and is therefore

unable to terminate a VPN connection. A home PC with VPN software and a PCoIP Software Client provides an alternative to using a PCoIP Zero Client with a VPN router. Follow security best practices when deploying VPN infrastructure.

The US Federal Government publishes useful guidelines [here](#) and [here](#).

VPN Deployment for Remote Workstation Card

The following points detail prerequisite information you should follow when setting up your Remote Workstation Card for VPN deployment:

- Install and license the Remote Workstation Card Agent (which provides connection broker functions). See [Linux](#) or [Windows](#).
- Install the Remote Workstation Card Software.
- Ensure that the Remote Workstation Card and host computer are connected on the same local network.
- Have a hardware VPN device on the hardware endpoint host network. (The PCoIP Software Client can use a software VPN connecting to the host network).

Deployment Steps

1. Create a VPN between your home network device and office. See your network devices documentation for instructions on how to create a hardware VPN. Home users with Teradici Software Clients can use a software VPN solution that connects to their office.
2. Connect your client to your Remote Workstation Card:
 - Configure your Zero Client session type to [Direct to host](#) using:
 - The Remote Workstation Card IP address.
 - The host IP address when the Remote Workstation Card Agent is installed.
3. If you are using a PCoIP Software Client, configure with the host PC IP address in the [Host Address or Code field](#).
4. Connect as normal.

After authentication and brokering, the Remote Workstation Card Agent passes control to the Remote Workstation Card directly, which enables a direct connection of PCoIP traffic between the Remote Workstation Card and the PCoIP Client.

NAT Option

This option requires a NAT device that can port forward from a source WAN IP address. It offers less overhead than the VPN option thus allowing for a limited performance increase. See [KB 1487](#) for additional details. Similarly to VPN solutions, NAT solutions require additional networking expertise and should be weighed against alternative approaches such as Teradici Cloud Access Software.

NAT Deployment for Remote Workstation Card

The following points detail prerequisite information you should follow when setting up your Remote Workstation Card for deployment with a NAT device:

- Ensure ports 4172 and 443 are open for TCP and UDP communications.
- If you are using the Remote Workstation Card Agent for Windows, add the following registry to *HLM\SOFTWARE\Policies\Teradici\PCoIP\pcoip_admin* :

```
pcoip.client_connection_address REF_SZ
```

- If you are using the Remote Workstation Card Agent for Linux, the `pcoip.client_connection_address` must be set to the WAN address of the Remote Workstation Card in the host PC */etc/Teradici/pcoip-agent.conf* file.

Deployment Steps

1. Configure the corporate NAT device to forward PCoIP traffic from each client static WAN IP address to either:
 - The dedicated Remote Workstation Card IP address (Zero Client)
 - The dedicated host PC IP address and the dedicated Remote Workstation Card IP address if the Remote Workstation Card Agent is installed (Zero Client or Teradici Software Client).
2. Configure the client connections to point to the provided corporate WAN IP using either your PCoIP Zero Client or PCoIP Software Client:
 - Use PCoIP Zero Client session type [Direct to Host](#).

- Configure your Software Client with the host PC IP address in the [Host Address or Code](#) field.
3. Connect as normal.

Avoid a VPN by using Cloud Access Software

The Remote Workstation Card can only be used outside your firewall via a VPN or NAT. In scenarios where a VPN is not available, or the complexity and expense of adding new VPN infrastructure is prohibitive, Teradici strongly recommends Cloud Access Software as an alternative. Besides avoiding the complexities and expense of new VPN infrastructure, Cloud Access Software offers the benefits of connection management, user entitlements and multifactor authentication.

Direct Connect Considerations

As of Cloud Access Software release 2020.01, direct connections from PCoIP Clients to Remote Workstation Card machines must be made to the host computer's IP address or FQDN. In previous versions, connections were made directly to the Remote Workstation Card; this connection method is no longer supported.

Work-from-Home options using PCoIP Management Console

If you are an IT Administrator using Management Console on your corporate network, you can easily allow your PCoIP Zero Clients or Remote Workstation Cards be moved to your employees home network and continue to manage them via the Management Console as long as you are using DNS to provision your endpoints. For [PCoIP Management Console Remote Endpoint Management](#) perform the following tasks:

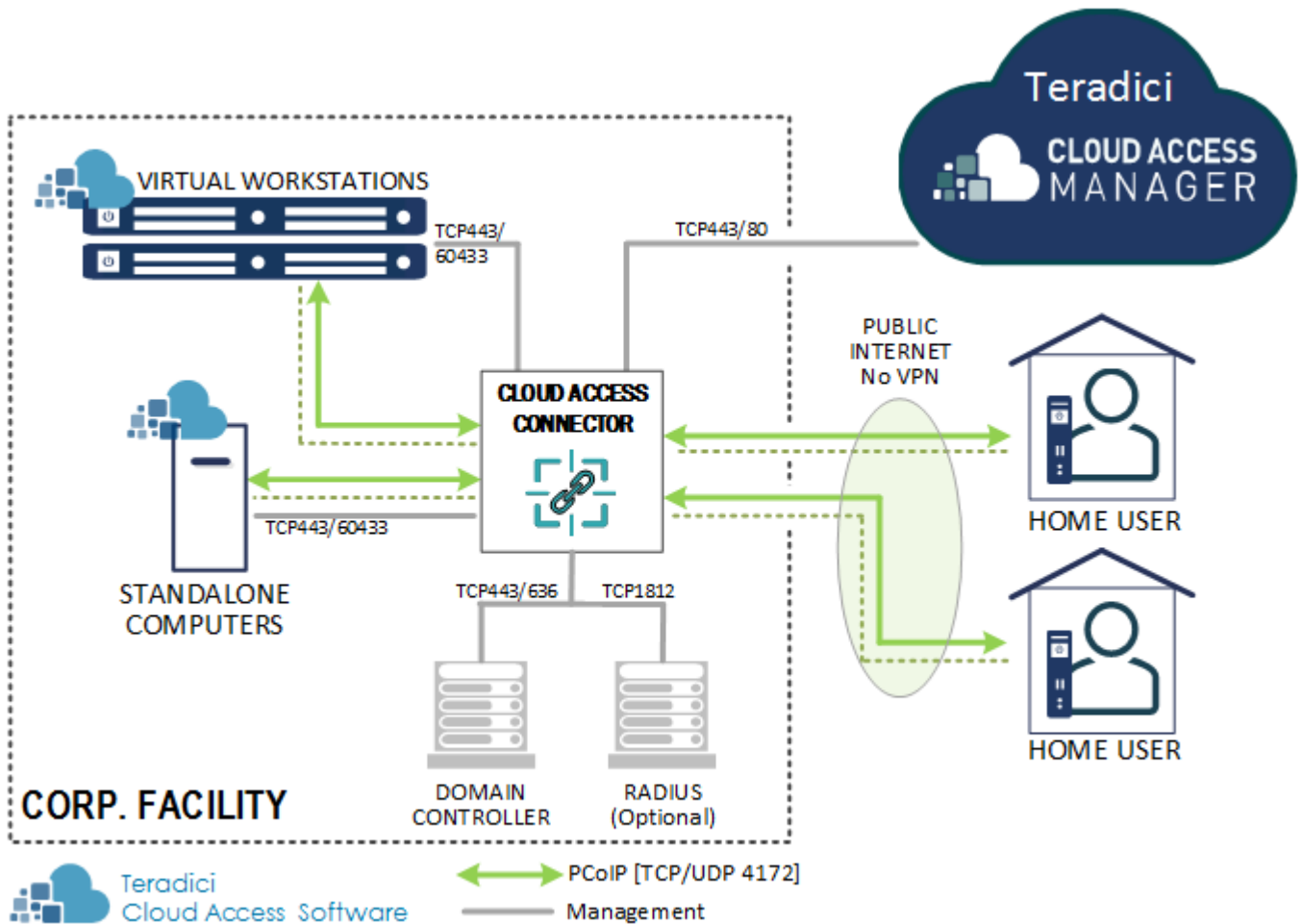
1. Configure the [PCoIP Management Console reverse proxy](#).
2. Connect the Remote Workstation Card or PCoIP Zero Client to your home network.
3. Follow the instructions regarding [connecting to a remote endpoint](#).

VPN or NAT Configuration

You will only be able to successfully peer endpoints after you have configured a VPN or NAT environment.

Work-from-Home options with Cloud Access Software

The following image outlines a top level architecture of the Work-from-Home scenario with Cloud Access Software.



Architecture Considerations

Ensure the virtual workstations and/or standalone host computer meets the system requirements as detailed in Cloud Access Software Administration Guides:

	WINDOWS	LINUX
Graphics Workstation - PCoIP Graphics Agent	System Requirements	System Requirements

	WINDOWS	LINUX
Virtualized Non-Graphic - PCoIP Standard Agent	System Requirements	System Requirements
Standalone Computer - Consumer Graphics	Guidelines	Guidelines
Virtualized and standalone computers with Quadro and Tesla NVIDIA GPUs - PCoIP Graphics Agent	System Requirements	System Requirements
Virtualized desktops with no discrete GPUs - PCoIP Standard Agent	System Requirements	System Requirements
Standalone computers with consumer grade NVIDIA GPUs (eg. GeForce RTX 2080) - PCoIP Graphics Agent	Guidelines	Use Remote Workstation Card
Standalone computers with no discrete GPUs - PCoIP Standard Agent	Guidelines	Guidelines

Internet Access Strategy and Connection Management

Decide whether the host computer will be accessed from home via VPN or public internet. Teradici highly recommends using Teradici Cloud Access Manager and associated Cloud Access Connector components which offer security gateway features and multifactor authentication integrated with connection management and user assignment capabilities. While a VPN offers 'direct connect' capabilities for a small set of users, licensing costs and scalability are deterrents to scalability. Scalability is more easily achieved using Cloud Access Manager or a third party connection broker such as the [Leostream](#) broker.

Local Monitor Security Considerations

If relevant, pay attention to the [considerations](#) discussed for standalone computers

Load Balancing Considerations

For larger deployments, it is recommended that multiple Cloud Access Connectors are deployed behind a load balancer. Consult the [Cloud Access Architecture Guide](#) for details.

Deployment Steps

Detailed Deployment Steps for Cloud Access Software are described in respective Windows and Linux Administration Guides for Graphics and Standard PCoIP Agents respectively. Instructions for using Cloud Access Manager with an on-premises deployment are detailed in the [Cloud Access Manager Administration Guide](#). Cloud Access Manager enables highly-scalable and cost-effective Cloud Access Software deployments by managing cloud compute costs and brokering PCoIP connections to remote workstations. The high-level deployment process is as follows:

1. Procure Cloud Access Software licenses.
2. Install the necessary GPU drivers (if required depending on need).
3. Install the appropriate Cloud Access Software Agent and activate the Cloud Access Software license during installation.
4. Install Cloud Access Software on your host device and activate licenses.
5. Setup and verify the Cloud Access Connector, see [Setting up the Cloud Access Connector Server](#) and [Verifying the Cloud Access Connector Server](#).
6. Download the Cloud Access Connector component files from Teradici, see [Downloading the Cloud Access Connector](#).
7. Obtain a Cloud Access Connector token, see [Obtaining a Cloud Access Connector Token](#).
8. Install the Cloud Access Connector, see [Installing the Cloud Access Connector](#).
9. Connect to the Cloud Access Manager Admin Console to manage your remote workstations and deployments, see [Connecting to the Cloud Access Manager Admin Console](#).

Cloud Access Manager Deployment Scripts

Teradici has an open github repository that contains a collection of scripts that simplify the setup, installation and usage of Cloud Access Manager. This repository enables users to set-up the necessary cloud resource (networking, firewalls, NAT gateway, storage buckets, etc), as well as Domain Controllers, Cloud Access Connectors and remote workstations from scratch to produce a working environment for testing and evaluation purposes. For information on how to access this repo, see [Cloud Access Manager Deployment Scripts](#).

Public Cloud Deployment Options

As an alternative to, or in addition to on-premises computer access, Cloud Access Software enables deployment of public cloud desktops on AWS, Google Cloud or Azure. For instructions on Azure, AWS or GCP deployments, consult the [Cloud Access Manager Administration Guide](#). Teradici also hosts a micro-site for each public cloud partner where you can find additional valuable deployment guidelines.

PARTNER	TERADICI MICROSITE
AWS	http://www.teradici.com/aws/
Microsoft Azure	http://www.teradici.com/microsoft/
Google Cloud	http://www.teradici.com/google/

For customers seeking cost flexibility using partial GPU options, the Azure NVv4 instances leverage AMD vGPU graphics which are available in fractions as low as $\frac{1}{8}$ of a GPU. For more information, see the [Teradici Cloud Access Software with Azure NVv4 Graphic Instance](#) reference architecture.

Work-from-Home options for VMware Horizon

PCoIP Zero Clients are certified for VMware Horizon can therefore be used in work-from-home scenarios.

VMware Horizon Work from Home

VMware have published an [excellent article](#) in Virtualization and Cloud Review online magazine on work from home strategies for VMWare Horizon customers.

If you currently operate a Horizon environment without home access to business resources, then additional configurations may be required. A typical environment that enables users to connect from home via a PCoIP Zero Client to a VMware Horizon server requires the following:

1. Set up an internal [View Connection Server](#).

2. Set up a [replica View Connection Server](#) which has been configured for external access.
3. Pair the replica View Connection Server with a [Security Server](#) which is exposed on the internet.
4. Finally, you need to complete the firewall rules for the [View Connection Server](#).
5. Configure your Zero Client [session type to View Connection Server](#) and enter the IP address of the Security Server.

Work-from-Home options for Amazon WorkSpaces with PCoIP Zero Clients

If your users are already using subscription-based Amazon WorkSpaces desktops, they can continue to use their PCoIP Zero Clients from home without any client configuration changes. If users are switching from on-premises VDI desktops to Amazon WorkSpaces, the [session type](#) must be reconfigured to Amazon WorkSpaces before connecting to the desktop. All that is required is the registration code from the invitation email sent after creating your Amazon WorkSpace. Enter this code in the [OSD Amazon WorkSpaces session](#) page.

Future Disaster Recover (DR) Strategy and Planning

Many enterprises will be seeking to re-evaluate business continuity and disaster recovery planning once the pressing issues related to COVID19 have been addressed. Teradici has a [DR Planning Guide](#) and [customer stories](#) showing how to augment a VMWare Horizon deployment with public-cloud based DR resources.

Performance Tips for Work-from-Home Use Cases

Home users may be faced with last-mile bandwidth constraints, additional network latency and higher-than-usual packet loss compared to their office environment. A little tuning of PCoIP parameters may go a long way at optimizing user experience over challenging WAN conditions compared to the default settings which are optimized for corporate LAN conditions. The [PCoIP Session Planning Guide](#) provides detailed optimization guidelines, a few key optimization tips are listed here:

Network bandwidth reduction

The major contributors to network bandwidth associated with PCoIP traffic include frame rate, image quality and display resolution. These parameters may all be tuned by adjusting PCoIP policies for either Windows or Linux deployments.

Reducing the frame rate

Many Media and Entertainment users require 60 frames per second (fps) for an optimum content creation environment – while not ideal, many such users will tolerate 30 fps for most tasks; thereby halving the network bandwidth demand in some cases. Knowledge workers should generally tolerate a 24 fps limit and task workers should tolerate up to 16 fps.

Tuning image quality

PCoIP has a default (max initial) image quality of Q80, which is optimized for knowledge worker usage. Media and Entertainment users typically adjust this initial image quality upwards to Q90 under LAN conditions; by returning the setting to Q80, 20-30% bandwidth savings may be had dependent on use case. Further significant savings may be gained by reducing the max initial image quality to Q70 which might be appropriate for knowledge users or task workers.

Display resolution considerations

Because PCoIP transmits compresses pixels into the home environment, a reduced display resolution offers a direct reduction on network bandwidth. A user with a 4K/UHD display at home will see up to 50% peak bandwidth usage by setting a 2560x1600 resolution. For highly constrained low bandwidth networks, consider adopting a single monitor configuration.

Adopt chroma-subsampling

For customers using PCoIP Graphics Agent in conjunction with NVIDIA Quadro vDWS deployments, consider switching to PCoIP Ultra for GPU Optimization and configuring chroma-sub-sampling to YUV 4:2:0. For video playback use cases, using H.264 with chroma-subsampling can reduce network bandwidth by up to 75% over default LAN settings.

Build-to-lossless

Turn off the Build to lossless image quality setting to limit network bandwidth consumption.

Video editorial vs. Text editorial use cases

Optimizing for video editors

Users involved in heavy video editorial work will accomplish bandwidth savings by switching to PCoIP Ultra for GPU Optimization and configuring chroma-sub-sampling to YUV 4:2:0 – this is because video content is generally already compressed in YUV 4:2:0 format so no further quality degradation is noticed. However, text and fine line details are subject to some distortion.

Optimizing for text editors

Task workers involved in text-oriented operations will achieve highest bandwidth efficiency adjusting the default PCoIP settings using the bandwidth reduction strategies discussed above. PCoIP presents text as a lossless reproduction which not only reduces eye strain but is very bandwidth efficient by design.

Addressing packet loss

If packet loss is higher than the recommended 0.1% or home users are complaining about occasional display stuttering, adjust the bandwidth floor to somewhere between 5 Mbps and 50 Mbps dependent on severity.

Dealing with increased latency

A small loss in interactivity is a natural consequence of users accessing the datacenter remotely compared to LAN connectivity. However, in-region latency should rarely be problematic unless there are underlying network problems. If users are using PCoIP from laptops, home PCs or thin clients, be sure these devices have sufficient CPU resources for the use case at hand.

Windows Updates Degradation

Background Windows updates can cause a temporary degradation in interactivity, especially in the case of low-performance PCs as endpoints.

WACOM tablet local termination

Artists using WACOM tablets are particularly sensitive to interactive latency. If your artists are used to using PCoIP in LAN environments without 'local termination' enabled, be sure to reconfigure the deployment and enable 'local termination' as per instructions in the PCoIP Agent and PCoIP Client administration guides.

Additional Resources

Performance Considerations - What bandwidth per user? For information on Teradici's sample bandwidth and network settings and policies, see [here](#).

Telework Security Guidelines As published by NIST [here](#).

Enterprise VPN Security Alert As published by the US Department of Homeland Security (CISA) [here](#).

Additional Teradici Documentation The [resources](#) section of the Teradici Website includes a wealth of information including whitepapers, datasheets, reference architectures, solution briefs, webinars, blogs and much more.

- [Cloud Access Software Customer Stories](#)
- [Solution Briefs](#)
- [Reference Architectures](#)
- [Cloud Access Architecture Guide](#)
- [Cloud Access Session Planning Guide](#)
- [Cloud Access Software Technical Documents](#)

How To Buy

To get started immediately, Cloud Access (standard) or Cloud Access Plus (graphics) licenses can be purchased by credit card from the Teradici [website](#). For larger deployments, please contact [Teradici Sales](#) or a [Teradici reseller](#).