



TABLE OF CONTENTS

Virtual Desktops – Attributes and Benefits	2
Benefits of Desktop Centralization and Virtualization	3
Endpoint Architectures Choices	4
Deployment Choices for Virtual Desktops	5
The Pano System – a Zero Client VDI Architecture	6
Physical and Virtual Infrastructure Components	6
Physical Infrastructure – Servers	6
Physical Infrastructure – Storage	7
Physical Infrastructure – LAN	7
Hypervisors	8
Connection Broker – Pano Controller	8
Alternate Connection Brokers	8
Scalability/Redundancy – Pano Maestro	9
Platform Management Tools	9
Directory Services / Authentication	10
Configuring Pano Desktop Virtual Machines	10
Managing Pano Desktop Virtual Machines	11
Putting it all Together	13
The Pano Zero Client	14
Remote Access to Virtual Desktops	15
Pano Remote	15
Pano Gateway	15
Benefits from the Pano System	16
For More Information	16

Virtual Desktops and the Pano System: An Architectural Overview

Extending Server Virtualization to the Desktop and Beyond

Virtualized desktops, running a standard Windows operating system but hosted on centralized servers, promise to radically reduce the ever-increasing drain on IT resources from deploying and supporting desktop computing. By consolidating these virtual desktops in the data center, benefits including improved IT productivity, increased data security, reduced user downtime and even significant power conservation can be realized.

Pano Logic® is the first company to offer a complete, purpose-built solution for virtual desktops combining a unique zero client endpoint with tools designed specifically for the deployment and management of virtual desktops.

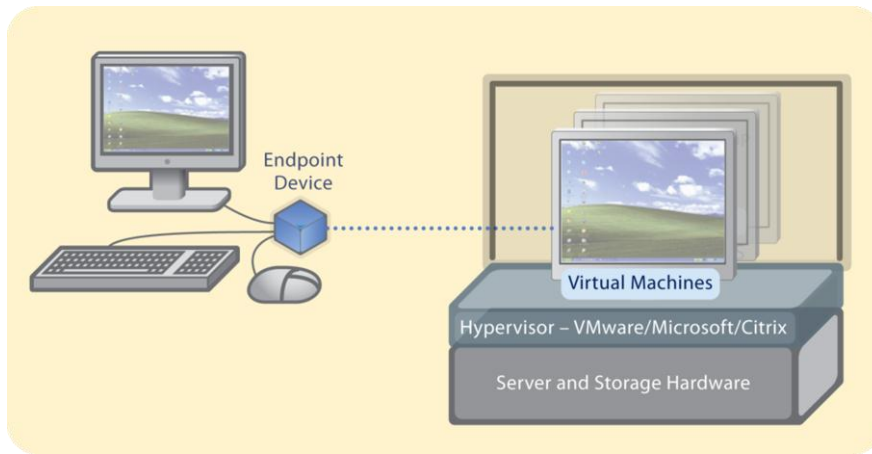
This whitepaper explains the technology and architecture used in server-based virtual desktop computing, exploring some of the benefits and challenges seen by IT organizations adopting the technology. The required hardware and software components are also discussed, using the Pano System™ as an illustration of how they can be combined in different scenarios to deliver the unique benefits of virtual desktops.

Virtual Desktops – Attributes and Benefits

Virtual desktops enable users to access a standard Windows operating system installation, along with whatever applications and data are needed, running on centralized servers in a data center. These servers use specialized software called hypervisors to create a “virtual machine” that simulates roughly the same capabilities as physical desktop computers. Desktop virtual machines (DVMs) connect over local area networks to specialized endpoint devices at the users’ location that in turn are connected to peripherals like monitors, keyboards, mice and other peripherals to make a complete system.

While there are many technological and architectural approaches to virtual desktops, they all share a common goal – to free the user’s desktop computing environment from the constraints and problems associated with deploying, maintaining, securing and supporting it on physically distributed personal computer hardware.

Figure 1:
VDI connects virtual machines running on a server-based hypervisor to endpoint devices.



Personal computers have provided knowledge workers with great utility and power, growing into a robust environment for a wide variety of applications and tasks. Unfortunately along with that growing utility has come an even more rapid growth in deployment and management headaches for the supporting IT organizations.

Physical desktop PCs can require an inordinate amount of management to make them secure, reliable platforms – and even more troublesome is that support issues often require a trip by IT staff to the user’s desk in order to physically troubleshoot problems.

Distributed physical PCs running Windows operating systems also pose many potential security problems as they make it easy for users to create uncontrolled local copies of critical data – exposing the organization to difficulties ranging from simple data archiving and destruction policy violations to complex and costly thefts of customer or financial data resulting in legal liabilities and public relations disasters.

Virtual desktops are growing in popularity because they address many of these issues through their two key attributes: being consolidated in a central location, and by being virtual rather than physical in nature.

BENEFITS OF DESKTOP CENTRALIZATION AND VIRTUALIZATION

Benefits from the consolidation and centralization of desktops include:

- **Improved IT and Help Desk Productivity** – centralization largely eliminates the need for IT staff to spend time traveling to the user's location in order to resolve trouble tickets or perform routine maintenance.
- **Hardware Capital Savings** – PCs typically use only a small fraction of their peak processing capacity meaning that a huge number of CPU cycles, RAM capacity, and local hard disk storage goes unused – consolidating those desktops onto shared server hardware gives users more cost-effective peak computing resources with much greater utilization levels overall. Zero client hardware like a Pano Zero Client also costs 1/2 to 1/3 of what a typical desktop PC costs.
- **Simplified Maintenance** – centralized DVM images can easily and quickly be monitored, backed up and recovered, and patched or upgraded.
- **Greater Data Security** – by centralizing all user files and data rather than relying on distributed, uncontrolled local PC storage devices, data loss stemming from both hardware failures and from the loss or theft of PCs and laptops can be eliminated.
- **Easier Roaming** – since the endpoint's connection to the virtual desktop can be suspended at any location and then immediately resumed from any other endpoint without any interruption of applications or open files – such as when moving from your office to a conference room – users can quickly access resume work at any location.

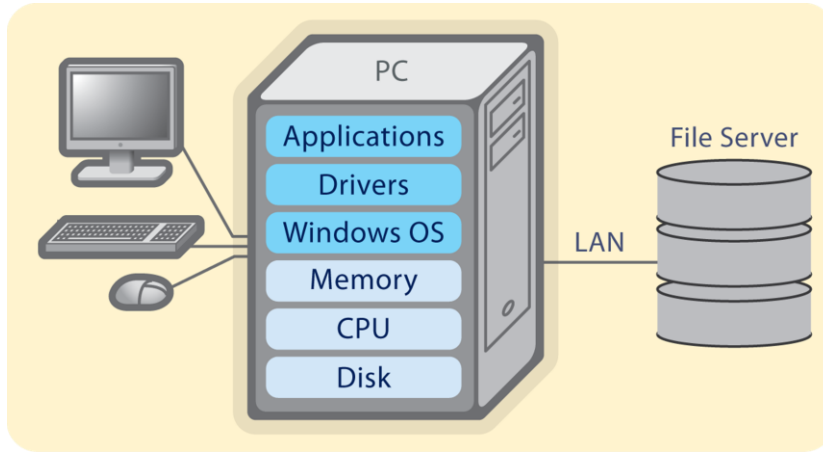
Virtualizing desktop computing can also contribute a number of benefits:

- **Rapid Provisioning** – setting up a virtual computing environment for a new user requires only a few simple commands at a management console. While this might seem like a small gain when deploying single users, deployments in training facilities or computer labs where 20 – 30 desktops need to be reset can see what used to tie up IT staff for a day or two shrink to a 30 minute automated process.
- **Less User Downtime** – virtual desktops can be rapidly recovered by substituting a newly cloned image, allowing users to recover from an OS corruption or malware infection with minimal downtime. And configuration-free zero clients can be swapped out by even untrained users in the event of a hardware problem.
- **Longer Life Spans** – Zero client endpoints which lack fans and fragile moving components like hard drives can have twice or even four-times the life span of traditional PCs in harsh environments like manufacturing plant floors or casino gaming pits. This can save both on purchase cost and replacement parts but also on warranty fees, user downtime and IT staff productivity.
- **Faster Upgrades** – increasing the hardware or storage resources allocated to a user is a simple configuration change to the DVM, without any need to travel to a user's location or to round-trip ship a computer for upgrading.
- **Improved Standardization** – enforcing common standards is much easier with virtualized "hardware," making support and troubleshooting for driver and configuration conflicts much faster and further reducing help desk workload and user downtime.
- **Reduced Power Consumption** – when used with the zero client endpoint devices, virtual desktops can use just a few percent of the electricity consumed by traditional desktop PCs, saving substantially on energy used both to power the devices and for air-conditioning to remove the resulting waste heat – often saving enough to pay for the endpoint devices in a year or two.

These are some of the benefits you may realize from virtual desktops – as with any advanced technology you need to make careful choices of the strategies and architectures you use in a virtual desktop deployment to achieve optimal results.

ENDPOINT ARCHITECTURES CHOICES

Figure 2:
PC Architecture



Virtual desktop infrastructure (VDI) architecture essentially virtualizes the architecture and components of a traditional PC, with some or all of the components centralized onto a server in the data center. What degree of centralization is used will determine a great deal of the maintenance and cost savings for a virtual desktop deployment.

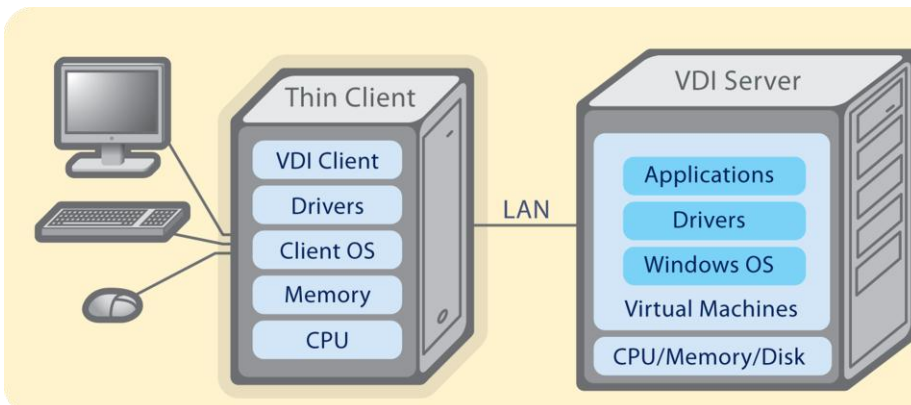
The traditional PC architecture shown in Figure 2 centralizes nothing other than perhaps user files stored on shared file servers accessed across the LAN. Each PC is a fully configured computer with an operating system, drivers, applications, and firmware along with hardware components like a CPU, memory and storage devices needed to hold the operating system and applications.

PCs are sometimes used as deployment platforms for virtual

desktop trials, running VDI Client software much like a thin client and connecting to a desktop virtual machine on a data center server. While this might seem like a simple way to test virtual desktops, leaving a PC at the user's desk also leaves all of the reliability, maintenance, and security problems in place and can effectively wipe out many of virtual desktops' potential benefits for IT productivity and TCO.

One alternative to a PC as a virtual desktop endpoint device is what is commonly referred to as a thin client – the term “thin” being a comparison to the relative “fatness” of a PC used as a client device.

Figure 3:
Thin Client Architecture



Even though they may be smaller than most PCs, these supposedly thin clients have to

include a CPU, memory and often even local storage like disks or flash memory to hold VDI client software, local drivers and a client operating system. This thin client OS is typically Windows Embedded, Windows CE or a proprietary Linux version and just like the OS on a PC, it will need to be patched, managed, and secured.

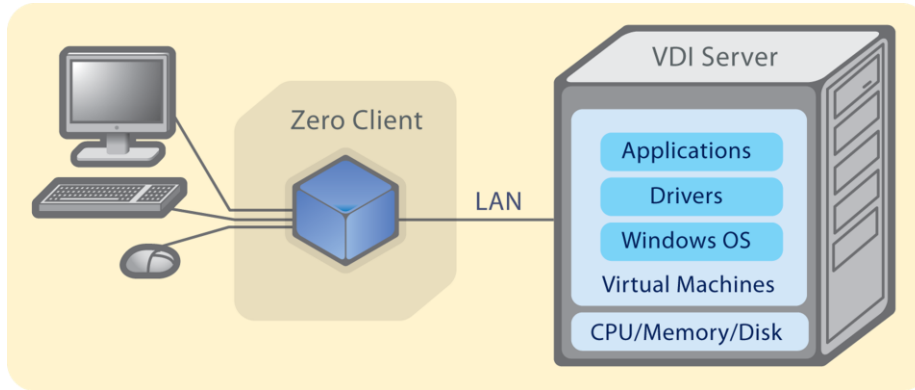
Some thin client vendors even charge significant fees for firmware, protocol extension, and maintenance tool upgrades, further increasing costs and complexity. In many cases these thin clients begin to duplicate the CAPEX/OPEX costs and IT management overhead of the traditional PCs they replaced, significantly neutering the potential benefits from deploying virtual desktops.

Over the years, many thin clients have evolved into “chubby” clients – effectively miniature PCs but running an uncommon operating system and doing nothing more than running VDI client software or firmware. With the addition more and more powerful hardware

needed to store and execute more complex client operating systems and remote display protocol extensions, these “chubby” thin clients can defeat most or all of the simplification and cost-containment benefits of virtual desktops.

A more effective endpoint alternative to thin client complexity is a “zero client” where the term “zero” refers to the complete lack of client-side CPU, OS, drivers, client software or even firmware, eliminating all of the licensing costs and maintenance complexity from the distributed endpoints and providing a much stronger base for fully realizing the potential benefit of virtual desktops.¹

Figure 4:
Zero Client Architecture



Zero clients effectively extend the system bus of the virtualized desktop machine from the hypervisor server out to the peripherals on the user's desk. This architecture completely centralizes all software, processing and management to just what is running on the server.

As a result, the duplication of endpoint costs, availability risks, and management overhead

forced by thin client architectures is gone and it is much easier to capture the TCO, productivity, and reliability benefits of virtual desktops.

DEPLOYMENT CHOICES FOR VIRTUAL DESKTOPS

In addition to the choice of what endpoint architecture to deploy, other architecture choices for virtual desktops include:

- What hypervisor or virtualization platform is used
- Whether virtual desktops are personal and dedicated or standardized and shared
- What server hardware and network configuration is used
- What storage resources and architecture is used for desktop images
- What level of management capabilities and tools are used

Putting adequate server and storage resources in place for a virtual desktop rollout (or even a pilot) can have a significant impact on the success of the project. Getting users to accept a physical to virtual conversion of their personal computing environment will be conditioned in large part by what performance changes they perceive. Choosing the right architectures and technologies will help ensure that the virtual desktop user experience is comparable to a PC but only if they are allocated sufficient CPU capacity, RAM and storage throughput.

IT organizations often run trials of virtual desktops on servers that have some spare capacity or that might be underutilized after a server virtualization and consolidation rollout. That approach may work for limited trials but committing the resources needed to provide sufficient capacity in servers, storage, and networks can be one of the most important choices made in rolling out a full-scale virtual desktop deployment.

To help illustrate the benefits of virtual desktops and how each of your architecture choices can influence them, a more detailed examination of specific architecture and technology choices possible with the Pano System follows in the sections below.

¹ For more information please see the [Thin Clients vs. Zero Clients: VDI Endpoint Choices](#) whitepaper and the [Thin vs. Zero Benefit Brief](#)

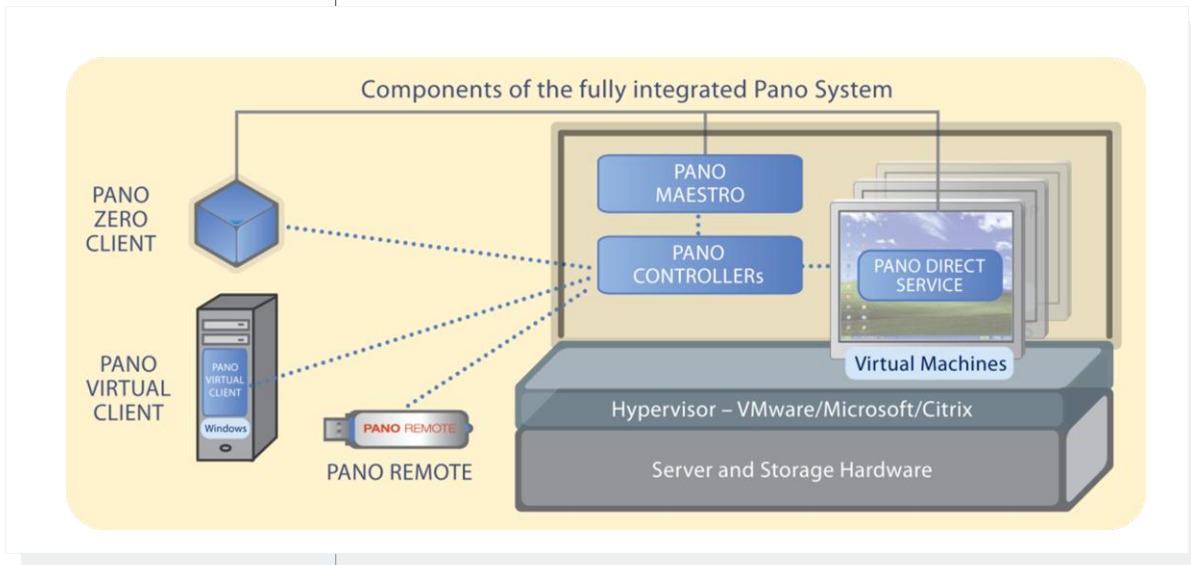
The Pano System – a Zero Client VDI Architecture

The complete Pano System solution includes the Pano Controller™ and Pano Maestro™ virtual appliances, the Pano Direct Service™ software, the Pano Zero Client hardware endpoint, and the optional Pano Virtual Client software for repurposing PCs and laptops to be Pano System endpoints. In addition, it requires server and storage hardware, a few network services, hypervisors from VMware, Microsoft or Citrix and a few other platform software components to help provision, manage and authenticate virtual desktops.

Together, these elements form an integrated solution, as illustrated in Figure 5. The rest of this document examines each of the key building blocks – server, storage and network hardware infrastructure, supporting tools and software infrastructure, and the Pano Zero Client – in detail.

Figure 5:

The Pano System includes the Pano Zero Client, Pano Virtual Client, Pano Controller, Pano Maestro and the Pano Direct Service



Physical and Virtual Infrastructure Components

Virtual desktops, at least in server-based approach such as that used by the Pano System, rely on a physical computing infrastructure of servers, storage, and networks along with a number of centralized virtual infrastructure software components running on the physical infrastructure. This section will discuss each of these components along with making some general configuration or sizing suggestions.

PHYSICAL INFRASTRUCTURE – SERVERS

The foundation of the virtualization infrastructure is a standard x86-based virtualization server or cluster of servers, often with multiple multi-core processors and a large complement of RAM. These servers' primary responsibility is to host the DVMs as well as the systems management virtual machines (VMs) and the Pano Controller VM. These servers are often configured as a cluster of servers for scalability and deployed in a failover configuration to provide enhanced reliability.

The processing load from DVMs, and therefore the sizing of the servers, is highly dependent on the workload and activities of the DVM users. For typical users, five DVMs per server CPU core are recommended, although eight or more DVMs may be deployed per CPU core for lighter workloads. More recent Intel Xeon and AMD server CPUs have more efficient native virtualization support, increasing the potential number of concurrent DVMs per CPU core and ultimately lowering costs.

Memory allocated to DVMs may be anywhere from 512 MB to 1 GB or more depending on the type of user workload and applications being used and the DVM operating system. It

is important not to under-allocate RAM to prevent individual DVMs from paging their virtualized memory to the DVM image file and thereby over-burdening the storage sub-system. To avoid this, more memory should be allocated to DVMs that are exhibiting significant levels of paging when possible. The total RAM on the virtualization server may be over-allocated to the supported DVMs, thus allowing the hypervisor itself to make more intelligent paging decisions than the Windows OS in any individual DVM can. Typically, 70-80% of the memory allocated to concurrent DVMs can be in the server's physical memory, with the rest being in the hypervisor's swap (page) file on disk.²

PHYSICAL INFRASTRUCTURE – STORAGE

Another key physical infrastructure component is storage, usually in the form of arrays of disks either directly attached to the servers running the DVMs (referred to as local storage) or more commonly as part of a shared Storage Area Network (SAN). Because the Windows OS reads and writes often to the virtualized disk drives presented to it by the hypervisor, the performance of the storage subsystem used by the servers is a critical factor in how well the virtual desktops perform and scale under load.

Availability can also be a critical factor as any DVM stored on local storage is at risk of not being available if the server it is stored on is unavailable due to a failure or maintenance. If this risk is acceptable, or there are alternate equivalent DVMs on other hosts, then local storage can be used to reduce infrastructure costs. If DVMs are unique, such as with DVMs that have been permanently assigned to users, and availability is a significant concern, then shared storage should be used.

The local disk sub-system or shared storage servers used to store DVM image files must deliver a sufficient number of IOPS (Input/Output Operations per Second) at a low enough latency to support an adequate response time. Disks in storage servers are usually configured in RAID arrays for hardware redundancy and performance reasons with non-parity disks storing data and parity disks storing information needed to reconstruct lost data in the event of a hardware failure.

High performance SAS disks rotating at 15,000 rpm will typically support 10 – 15 DVM images per non-parity disk. Less expensive disks, including standard desktop SATA drives, may be used if fewer or less demanding DVMs are deployed per disk. Parity disks in a RAID configuration do not contribute IOPS and should not be included in these scoping calculations. For larger SANs, large on-controller caches will often greatly improve performance although at a higher cost. Optimizing storage usually requires some empirical testing as the specifics of workloads and server configurations will determine what impact a particular storage configuration has on DVM performance.

In the future Solid-State Disks (SSDs) are expected to provide 10x-100x the IOPS of mechanical hard drives and overcome many of the storage limitations provided the underlying hypervisors know how to manage this new form of storage.

PHYSICAL INFRASTRUCTURE – LAN

Getting adequate user experience from virtual desktops depends on having low latency, high-bandwidth local-area network connections provided by standard 10/100 Mb/sec networks (i.e. Ethernet) between the servers running the hypervisor hosting DVMs and the endpoint devices.

Communications in the Pano System is handled by the Pano Direct Protocol® (PDP) implemented in the Pano Zero/Virtual Clients and the Pano Direct Service running in the DVMs. This protocol is purpose-built for VDI and is designed to make efficient use of the bandwidth available on a typical 100Mb/sec switched Ethernet LAN, delivering a user experience that is equivalent to or even better than a business PC.

In some cases where support of virtual desktops is needed in remote offices that are linked by wide-area networks (WANs), customers have been able to get adequate performance by using local on-premises hypervisor servers running just the DVMs used in

² For help configuring and sizing servers or storage for VDI deployments please see the [VDI Infrastructure Sizing Solution Brief](#)

the remote office, while still managing all of the remote DVMs and Pano Zero/Virtual Clients from a centralized Pano Controller and required DVM management tools connected over the WAN. Although there may be some delay in the initial login sequence, once the DVM is connected to the Pano Zero/Virtual Client all of the PDP traffic goes directly between them on the LAN, providing good response times.

Pano Remote and Pano Gateway use a different protocol, the Microsoft Remote Desktop Protocol (RDP), for a portion of its communications as the Pano Remote software runs on a Windows PC and has to deal with the potentially high latency and low bandwidth of WAN and Internet connections between it and the Pano Gateway server (see page 14 for more information).

HYPERVISORS

A fundamental software component supporting the Pano System is the hypervisor - either VMware's vSphere ESX/ESXi, Microsoft's Hyper-V or Citrix XenServer. These hypervisors host the DVMs, running virtualized Microsoft Windows XP or Windows 7 operating systems, along with other system VMs including the Pano Controller and Pano Maestro appliances.

Most of these hypervisors are referred to as class 1 or native, bare-metal hypervisors meaning that no server operating system is required to support them as they run directly on the server hardware without any other underlying software. The virtualization platform software, from VMware, Microsoft or Citrix, typically also includes an extensive toolset for managing hypervisor servers and provisioning their hosted virtual machines.

CONNECTION BROKER – PANO CONTROLLER

Pano Controller coordinates the management and administration of Pano Zero/Virtual Clients and DVMs with the virtualization platform software components. A self-contained software appliance that can be placed on any hypervisor server, Pano Controller enables IT staff to provisioning new DVMs for users, authorize users and user groups to access specific DVMs, and monitor the availability of running DVMs. Pano Controller also allows you to manage thresholds for available DVMs to ensure users don't need to wait when logging in while still conserving compute and power resources by shutting down unused DVMs.

Pano Controller has three distinct roles, any of which may be enabled for any particular Pano Controller VM during the initial setup process:

- **Zero Client Controller Role** – provides connection and management of Pano Zero/Virtual Clients including display of the client login screens and authentication with a directory service like Active Directory
- **Virtual Desktop Broker Role** – performs connection brokering between a user's Pano Zero/Virtual Client and their assigned DVMs, using an internal database of DVMs and user assignments.
- **Full Role** – this role is simply a combination of the above two roles.

ALTERNATE CONNECTION BROKERS

When running on the VMware platforms the Pano System is also compatible with VMware View Manager and the Pano Controller can integrate it as the primary connection broker. View Manager is typically used for very large VDI deployments (starting at 1,000 or more desktops) or when deploying hybrid populations of endpoints that mix Pano Zero Clients with thin clients. In these types of deployments, View Connection Server is used to authenticate users and determine which DVMs they are associated with, while Pano Controller is still used to discover Pano Zero Clients and start Pano DVMs as needed. Pano Controller provides a special VMware View Collection type (see page 12) to help identify which DVM connections are brokered by View Connection Server.³

When running on the Citrix platforms the Pano System uses Citrix XenDesktop as the primary connection broker. In this type of deployment, XenDesktop is used to

³ For more information see the [Using VMware View with the Pano System Solution Brief](#)

authenticate users and determine which DVMs they are associated with, while Pano Controller is still used to discover Pano Zero/Virtual Clients and provide the login screen. Pano Controller provides a special XenDesktop Collection type (see page 12).⁴

SCALABILITY/REDUNDANCY – PANO MAESTRO

Pano Maestro is a management front-end that provides both a summary monitor for groups of Pano Controllers and the ability to drill-down into each group's Pano Controller Console.

Key functions performed by Pano Maestro include:

- **Scalability:** Binding together up to six Pano Controller instances as a group, sharing the load of client discovery and virtual desktop connection brokering.
- **Availability via Failover:** Pano Controller groups can be setup with primary and secondary instances to work in a redundant active/standby failover configuration. When the primary Pano Controller appliance fails or stops responding, the secondary Pano Controller appliance takes over.
- **Monitoring:** Provides a summary view of status for all managed Pano Controller Groups, including name and status of each primary, secondary, and auxiliary Pano Controllers in the group, and the roles (ZCC, VDB, Full) active in each.
- **Management:** provides a drill-down from the Summary view into the full management Console for each Pano Controller:
 - Opens a view into the Pano Controller Console management UI for the primary Pano Controller in each managed group.
 - Allows you to perform any management, monitoring, or provisioning tasks you could do directly within the Pano Controller's UI.
 - Works in a tabbed interface letting you open several Pano Controller Consoles at once and quickly switch between them and the Summary status view.
- **Licensing and Security:** Managing Pano System Licenses, proving a licensing service on your network. Pano Maestro can backup and restore configuration settings to quickly migrate or recover a setup. And it allows you to manage web security for the UI by configuring SSL certificates.

PLATFORM MANAGEMENT TOOLS

Pano Controller can work with the DVM management tools provided by the virtualization platform vendors, such as VMware vCenter Server, Microsoft System Center Virtual Machine Manager (SCVMM), and Citrix XenDesktop.

On the VMware platform vCenter Server (formerly called Virtual Center) provides highly scalable management of virtual machines. When used with Pano Controller, the vCenter console also enables administrators to configure many options that determine how the DVMs operate, including thresholds for resource usage, load balancing, and the cloning of DVMs from a specified template. Firewall settings and network configuration for access to DVMs are also set up in vCenter. Pano Controller and the Pano System can also be used without vCenter although with limitations, especially on the use of DVM collections.

A single instance of vCenter Server, which can also be installed on a virtual OS running on a hypervisor, is capable of managing multiple hosts and tens of thousands of DVMs. VMware also supports the use of Microsoft Cluster Services to provide redundancy via failover for vCenter Server.

Pano Controller can also be used with VMware View Composer, included with the Premier Edition of View, to optimize storage by having DVMs share a master image, eliminating redundant storage of OS and application files. This optimization, sometimes called deduplication, is typically used in larger deployments (over 1,000 DVMs) where the IT staff

⁴ For more information see the [Pano System on Citrix Solution Brief](#)

have a high level of VMware expertise to ensure that the savings in storage makes up for the extra work required during setup and provisioning of DVMs.

On the Microsoft virtualization platform, Pano Controller requires SCVMM to provide equivalent support for enhanced DVM provisioning and management. Integration between the two is done via a small software component, the Pano Connector for SCVMM.

DIRECTORY SERVICES / AUTHENTICATION

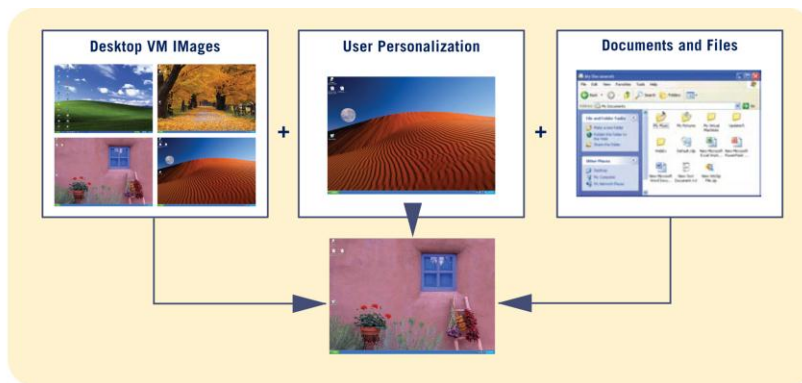
The user authentication performed by Pano Controller relies on a Directory Services server – supported servers and protocols include Microsoft Active Directory, Novell eDirectory, and OpenLDAP protocols. The Directory Services server is used to identify and authenticate users from the login screen displayed when the Pano Zero/Virtual Client starts up and connects to Pano Controller. The user identification provided as a user name and password not only confirms the user’s identity to Pano Controller but is also used to link users to their assigned DVM collections and groups (discussed below).

Configuring Pano Desktop Virtual Machines

To simplify recovery and reconstruction of Pano DVMs in the event of corruption or malware infection, a few simple rules can be applied when building virtual machine templates. This approach relies on standard Windows capabilities and works by logically and, in some cases, physically segregating DVM components into four basic groups:

- **DVM Image:** A desktop virtual machine image running the Microsoft Windows XP or Windows 7 operating system along with whatever installed or streamed applications are needed for the DVM’s intended use. Typically a Windows Virtual Desktop Access (VDA) device-based subscription license is required to use Windows in a DVM.⁵
- **Pano Direct:** The Pano Direct Service device driver is installed in the DVM’s Windows OS to extend the virtualized system bus across the LAN to the Pano Zero/Virtual Client as well as providing local configuration capabilities. The VMware and Citrix platforms also require installation of their client tool software in each DVM.
- **User Profiles:** This standard Windows capability records the user’s personalization preferences for customizable aspects of the environment, including wallpaper, background colors, and display preferences. These profiles along with the folder redirection described next are sometimes referred to as User State Virtualization or just State Virtualization.
- **Folder Redirection:** Network drive mapping or redirection of the user’s Documents folder to a shared storage server file system. Because the DVM image does not store a user’s files internally, the file system for a given user must be mapped to it using folder redirection or by mounting network shared folders. In this way, even though the user’s files are external to the DVM, they appear to be local. Credentials obtained at login determine which folders/files are mounted or mapped for the user to access.

Figure 6:
Desktop Virtual Machine (DVM) components.



This separation makes it easy to reconstitute a user's DVM at any time. For example, if a user were to corrupt their DVM's OS by opening a virus-bearing e-mail, IT staff could delete the current DVM, and start a new one created with the same DVM image template, standard applications and drivers, user profile, and folder redirection as the original DVM—and the user would be ready to resume work.

This form of recovery can also be applied when an application becomes unreliable or misconfigured. In such cases, it is often easier just to provision a new DVM with the application software already installed rather than spend hours trying to diagnose and fix the problem. This is one of a number of ways that centrally managed virtual desktops can improve IT productivity while cutting user downtime.

With Windows policies the personalization of the DVM can be limited to a fixed set of options (such as wallpaper and display preferences) or extended in essentially any manner, such as user-specific software bundles or access to special devices.

Managing Pano Desktop Virtual Machines

One significant advantage of using systems purpose-built for virtual desktops over generalized OS virtualization tools is their customized support for time saving features used to provision and manage different types of DVMs.

In the Pano System DVMs are typically generated from a template that the IT staff has preconfigured. These templates are generally tailored to provide a DVM with all the necessary software for a particular user role, such as a member of the accounting department. Once this template has been configured, tested, and validated, it is stored in the vCenter inventory. DVMs are then cloned from this template to rapidly provision new users or workstations.

These templates and the clones made from them can be more easily managed as a group, known as a collection. A key characteristic of a DVM collection is the method by which users or devices are mapped to DVMs. Mappings are determined by two basic methods: by user and by device.

There are three main types of User Based DVM collections supported by Pano Controller – Pooled Desktops, Permanently Assigned Desktops, and Existing Desktops:

- A **Pooled Desktops collection** consists of a group of identically configured DVMs running on the virtualization server. When a user logs into the Pano Zero/Virtual Client, authentication credentials identify which group the user belongs to and with which pool of DVMs the group is associated. The user is then assigned to a DVM in that pool, the personalization and file systems are attached, and the DVM is issued to the user. In a typical deployment, such as in a call center, a pool has some number of DVMs in use and a few hot spares running on the server, so that a desktop can be provisioned quickly at login. Additional DVMs for the pool are typically powered off and can be turned on automatically when needed. Pooled desktops collections have several key benefits:
 - The mapping of the user to the DVMs is not persistent in a pooled collection. As a result, sites can achieve a higher utilization level because they can allocate hardware resources based on the average number of active users rather than the total number of possible users. Therefore, if a site has 100 users but they work in several different shifts, it needs to size the environment only to the number of expected concurrent users.
 - Since all logins build a new desktop from the DVM pool, the ability to phase in patches and updates from a new “gold image” is possible. However typically DVMs are used, and then returned to the pool, rather than being built for each login. To overcome this, administrators can “refresh” the pool, so that users are assigned DVMs from the updated pool upon next login.

This approach has a limitation compared to other types of DVM collections – a user's sessions and changes are not persistent, so some users may feel restricted by not

having the ability to fully customize their desktop or install applications that are not part of the application set for the pool.

- A **Permanently Assigned Desktops collection** consists of a group of DVMs in which the user-DVM link is persistent. As in a pooled collection, DVMs in a permanently assigned collection are created from a template, but once created the cloned desktop is assigned to only one user. In this type of a collection, personalization can extend beyond profiles, such as permitting users to install new software and extensively customize their Windows configuration. This is possible because users are always assigned to their specific DVM. This approach provides important flexibility to knowledge workers who have individual application preferences or who need the ability to install or update their own software or utilities – allowing them to manage their computing environment just as they might on a traditional physical PC.

This collection type has two caveats: Allowing users to make these changes to their environments also permits them to inadvertently install malware or corrupt applications, although these DVMs can be sometimes be fixed by rolling them back if a previous snapshot was made by the administrator. In addition, updates and patches must be implemented on an individual basis.

Permanently assigned desktop DVMs may be deployed on local storage to reduce infrastructure costs. However, in the event that a server hosting those DVMs becomes unavailable, the corresponding users will be unable to access their Pano desktops until service has been restored or an administrator has intervened to assign alternate desktops to the users. Depending on the deployment model, the delays this might produce may be an acceptable risk.

Permanently assigned desktops may also be deployed on shared storage (on a SAN) to ensure higher availability. In the event that a server storing those DVMs unavailable, the DVMs can be migrated to other servers in the cluster either manually or automatically.

- An **Existing Desktops collection** consists of unique DVM configurations that individual users might already be using before a transition to virtual desktops. By gathering these unique DVMs in their own collection, Pano Controller is capable of managing and administering them as a group. One disadvantage is that, similar to a permanently assigned desktops collection, the DVMs in an Existing Desktops collection must be managed individually.

There are additional **VMware View** and **XenDesktop** User Based collection types that can be used when the Pano Controller is set up with either Citrix XenDesktop or VMware's View Manager. Credentials that users input through the Pano client login screen are then passed directly to XenDesktop or View Manager to be authenticated and have the appropriate DVM identified. When using this collection type, Pano Controller does not start the DVM – instead the platform connection broker handles these tasks.⁶

In addition to these User Based collection types, Pano Controller supports three Device Based DVM collection types to simplify the administration of specialized virtual desktops:

- An **Automatic Login collection** type allows you to set up Pano endpoints and their corresponding DVMs to act like kiosks without the administrative burden of managing multiple accounts and passwords. Rather than displaying the Pano client login screen, the Pano endpoint automatically connects and logs on to the associated DVM using a specified account name and password that is the same for all DVMs in the collection.
- A **Different Accounts w/ Automatic Login collection** allows you to set up Pano Zero/Virtual Clients and their corresponding DVMs to act like kiosks. This collection type is best when you wish to create a set of kiosks of fixed-use workstations and want to have a unique user name and password assigned to each DVM. Rather than displaying the Pano client login screen, the Pano Zero/Virtual Client automatically

⁶ For more information see the [Using VMware View with the Pano System Solution Brief](#) or the [Pano System on Citrix Solution Brief](#)

connects and logs into the associated DVM using a saved account name and password. This collection type relies on a user group that has the individual saved account names as members and these accounts must exist in the directory service being used – local user accounts are not supported.

- A **Windows Login collection** allows you to set up a Pano endpoint and a corresponding DVM to act like a general-purpose Windows computer. This collection type is useful if you require users to use biometric devices (such as a fingerprint scanner) for authentication. Rather than displaying the Pano client login screen, the Pano Zero/Virtual Client automatically connects to the DVM and then requires the user to login to the Windows OS prior to using the DVM.

DVM collections provide valuable systems management benefits, especially in pooled desktops collections as desktops can be upgraded on the IT department’s schedule without interfering with users. In addition, it is easier to contain virus outbreaks, because IT can easily delete infected DVMs and provide fresh replacement DVMs to the pool. With other collection types, IT can also manually remove infected DVMs and replace them with uninfected snapshots of the DVMs.

Putting it all Together

To illustrate how the major components of the Pano System work together, this section recaps what happens when a user logs in and connects to a Pano desktop virtual machine on the server from a Pano Zero/Virtual Client or the Pano Remote software.

At start-up or when the Pano Button is pressed, the Pano Zero/Virtual Client searches for and connects to a Pano Controller running on the local network. Pano Controller then displays the Pano login screen on the Pano’s attached monitor. After the user enters their user name and password, those credentials are authenticated using the directory services server attached to Pano Controller. The corresponding entry determines which group the user is in and which collections of DVMs they can select.

Users can use the login screen’s Options dialog to access a number of other choices to troubleshoot DVM problems without involving IT staff. These options, which can be enabled or disabled on collection basis, include:

- Power on – load the DVM if it is not already active on the hypervisor server
- Restart Windows – equivalent to a warm boot of the DVM
- Reset Power – does a cold restart (power off, power on) of the DVM
- Trash Desktop – marks the DVM as not usable and needing attention from IT (only available for DVMs in Permanently Assigned Desktops collections)

The last option is typically used when a user suspects that their DVM OS or applications are corrupted or infected with malware. After flagging a DVM as Trashed, the user can get a new DVM (cloned from the collection’s template) upon their next login allowing them to continue working without waiting for assistance from IT.

Figure 7:
Choosing a DVM in the Pano login Options dialog.



If users have been assigned multiple DVMs, they can select which DVM they wish to connect to from the Desktop drop-down menu (see Figure 7 below). For example they might have been assigned both a Windows XP and a Windows 7 DVM during a transition period between the two. Or they might have access to both a permanently assigned desktop, such as a physician having an office PC used for email and filing reports, and one or more DVMs in a task or group-associated desktop pools, such as clinical care or nursing workstation in various hospital wards.

Once the login process has started and the virtual desktops are “powering” up, the user can monitor its progress both via changes in the color of the

Pano Button light and via the Pano login screen red-yellow-green status indicators.

If the user is remotely connecting to the DVM via Pano Remote (described in more detail on page 14) the process is similar with a few key differences. Instead of the Pano Zero/Virtual Client connecting to Pano Controller, the Pano Remote software on the USB key is launched and displays the login screen. The user credentials are passed over the wide-area-network (WAN) like the Internet from the user's computer using the Microsoft RDP protocol to Pano Gateway where they in turn passed on to Pano Controller. From there on the process is much like that with the Pano Zero Client – just the final leg of the connection from Pano Remote to the DVM is different as it uses RDP and SSL to provide secure, reliable communications over the external WAN leg.

Once a DVM is selected and “powered up” on a hypervisor server by Pano Controller, communications are then run directly from the DVM to the Pano Zero/Virtual Client, without any involvement by Pano Controller. During the session the user's keystrokes are encrypted and sent over the local area network to the Pano Direct Service in the DVM running on the hypervisor server. The send-transit-response cycle is so quick the user cannot tell that anything other than a local PC is in use. Mouse clicks and any I/O from a USB peripheral are sent in the same way to the DVM although USB peripheral data is not encrypted. The Pano Direct Protocol used between the Pano Zero/Virtual Client and Pano Direct Service running in the DVM optimizes the use of network bandwidth by only sending the minimum number of bits necessary to update the screen display on the attached monitors.

A heartbeat connection to Pano Controller is monitored in case the Pano Zero Client is disconnected from the DVM. This feature helps users suspend the connection to a running DVM and then change rooms or even buildings and be able to reconnect to the DVM and resume working at the point at which they disconnected. The user's DVM remains running across disconnects, so that a break in connection or a transition from one Pano Zero/Virtual Client to another does not end the user session.

Finally, when the user logs out, the DVM may shutdown depending on the power management policy of the collection. At that point, pooled desktops are returned to the pool for use by another user. If, while the user is logged on, the load on one server node begins to detrimentally affect performance, the server may begin migrating DVMs to a different node (if VMware DRS is being employed). To completely terminate the user's DVM connection, the user must log out of the DVM. Administrative policies at a site can also be configured to force disconnect or logout after a certain period of idle time.

The Pano Zero Client

The Pano Zero Client is the heart of the Pano System, consisting of a compact purpose-built desktop virtualization hardware endpoint that sits on the user desk and connects the display, input devices and other USB peripherals to the DVM running on the hypervisor server. It is a true zero client because in contrast to thin client and PC endpoints it contains no CPU, no storage, and no operating system or software. As a result, it

consumes very little power — about 6.5 watts when fully active with dual displays and under 0.2 watts when in sleep mode — and is tamper-resistant and never stores any data locally, eliminating the risk of data loss from equipment theft. More importantly, it requires no endpoint management software, no patch management, no firmware upgrades, and no local OS licensing fees or updates – both significantly reducing virtual desktop deployment costs and improving on-going IT productivity.

Figure 8 shows the rear of the Pano Zero Client and the various jacks it contains for connecting desktop peripherals. These include a DVI-I video port (which can be converted to VGA with

Figure 8:
Ports and connectors
on the rear of the
Pano Zero Client.



the included adapter), a second monitor port (connects to a second DVI monitor with an optional Dual Monitor Cable), an RJ-45 Ethernet jack, four USB connectors, plus an analog audio port for headphones and speakers.⁷

In contrast to most thin clients, the Pano Zero Client itself contains no USB or other drivers. Instead, the Pano System utilizes only the native drivers in the Windows OS running in the connected DVM and simply handles communications between the DVM operating system and the ports on the Pano Zero Client, much like a PC system bus or chipset.

This approach improves performance when displaying video or other multimedia and also greatly simplifies deployments since most types of USB devices work on a Pano without any specialized support – unlike thin clients, vendors do not have to write or supply special drivers to allow peripherals like scanners or printers to connect to the endpoint – instead standard Windows drivers can be used.

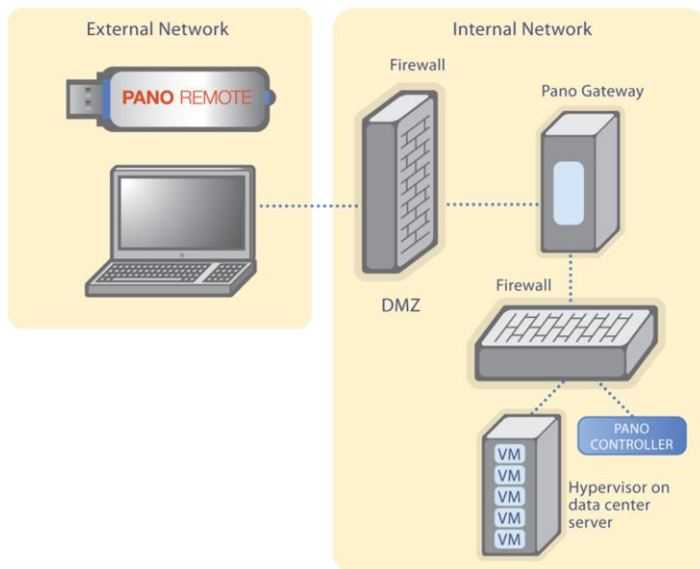
The Pano Zero Clients also includes a single user interface element, the Pano Button®, located on the front corner of the top. The Pano Button serves both as an indicator of the connection status, glowing steady blue when successfully connected to a DVM, and as a button that allows the user to interrupt the Device-DVM connection and return to the Pano login screen and connect to another DVM. Pressing the Pano Button can act almost as a virtualized equivalent of the Ctrl-Alt-Del used to regain control of a physical PC but it never causes the DVM to reboot or restart, preserving whatever work and applications are open so you can log back in to resume work.

Remote Access to Virtual Desktops

PANO REMOTE

Pano Remote™ is an option in the Pano product line that allows Pano users to reach their Pano DVMs from a remote location over a WAN like the Internet. Pano Remote lets users temporarily access their Pano virtual desktops when they are away from the office, whether working in the evening or when travelling by simply plugging a special secure USB key into any Microsoft Windows PC. No software installation is required and nothing is done to or left on the hosting PC.

Figure 9:
Pano Remote provides secure access to Pano virtual desktops from any Windows desktop or laptop.



Pano Remote provides access to any of the Pano DVMs assigned to the user, either in a window (at a resolution set by the user in the login screen) or using the full screen. Administrators can set policies in Pano Controller to allow or restrict access to local printers and drives along with controlling transfer of data on the clipboard between the virtual and host operating systems. Pano Remote is delivered already installed on a USB key and can be used with Microsoft Windows XP, Vista or 7 on the remote host desktop computer.⁸

PANO GATEWAY

Pano Gateway is a communication portal bundled with Pano Remote that provides secure connections from external networks. It acts as a plug-in to Microsoft Windows Server 2008 Remote Desktop Services Gateway (formerly called Terminal Services) to provide

⁷ For more information please see the [Pano System data sheet](#).

⁸ For more information please see the [Pano Remote data sheet](#).

secure access from external networks like the Internet as shown in Figure 9.

Pano Gateway does not require the use of VPN software or hardware to communicate with Pano Remote users, but instead uses standard secure protocols and ports (RDP via HTTPS/Secure Sockets Layer) to connect to Pano Gateway and in turn to the virtual desktops on VMware, Citrix or Hyper-V hypervisor servers inside the data center. The RDP protocol, while not delivering an optimal user experience, ensures a reliable connection even over WANs like consumer-level Internet DSL or cable modems. This also simplifies the configuration of firewalls and security policies while still ensuring that critical servers hosting DVMs would not needlessly be exposed to potential security risks.

Pano Remote can help you inexpensively extend your Pano virtual desktop deployment to larger populations of transient users, such as guest users, users needing limited and intermittent access to a virtual desktop or to mobile workers. Anywhere and anytime they can find a Windows PC with a network connection, they can reach their Pano virtual desktop.

Benefits from the Pano System

The Pano System and the Pano Zero Client delivers the benefits of virtualization to the desktop. It makes it possible for IT staff to deploy, manage, secure and support desktops entirely from within the data center — including provisioning, monitoring, trouble-shooting, backups and updates — and it removes the many inconveniences, costs, productivity drains and security threats of having traditional PCs at user's desks.

Zero clients by design can't store data locally, eliminating security risks from the loss or theft of the devices — lacking a processor they also present no opportunity for malware infection. And without fans or failure-prone hard drives they can have life spans many times that of typical PCs in harsh environments, reducing both costs and user downtime.

Virtual desktops can also help you meet goals for reducing your environmental footprint by cutting desktop energy use to just a few percent of the energy consumed by PCs, often saving enough to recoup endpoint capital expenses in the first year or two.

For More Information

For more detailed information on setting up and managing the Pano System, along with detailed help in optimizing your virtual desktop deployment can be found in the online help available at help.panologic.com.

For more information on the Pano System or to obtain a Starter Kit please visit www.panologic.com or call us at 650-454-8940.

Pano Logic, Inc.
2000 Seaport Blvd, Suite 200
Redwood City, CA 94063

This document was updated in May 2012 and is specific to the features and capabilities of Pano System 6.0 [WP-PSTA-110211]

© Copyright 2009, 2010, 2011, 2012 Pano Logic, Inc.

Pano, Pano Logic, Pano Button, Pano Direct Protocol, and Pano Direct Technology are registered trademarks of Pano Logic, Inc.

Pano Gateway, Pano Controller, Pano Maestro, Pano Remote, Pano Direct Service, Pano System, Pano Virtual Client, and Pano Zero Client are trademarks of Pano Logic, Inc.