

This PDF was generated on February 2024 and was current at the time of download. To check for the latest version please visit <https://techzone.omnissa.com/resource/horizon-8-frequently-asked-questions-faqs>

# Horizon 8 Frequently Asked Questions (FAQs)

Omnissa Horizon

## Table of contents

|                                               |    |
|-----------------------------------------------|----|
| Horizon 8 Frequently Asked Questions (FAQs)   | 3  |
| Overview                                      | 3  |
| Audience                                      | 3  |
| Getting Started with Horizon 8                | 4  |
| Architecture                                  | 5  |
| Installation                                  | 6  |
| Configuration                                 | 7  |
| Scalability, Availability, and Infrastructure | 9  |
| External Access                               | 10 |
| Authentication                                | 11 |
| Profile Management                            | 12 |
| Security and Encryption                       | 13 |
| User Experience                               | 15 |
| Display Protocol, Multimedia, and Graphics    | 16 |
| Image Management                              | 18 |
| End-User Capacity                             | 19 |
| Unified Communications Support                | 20 |
| Printing and Peripherals                      | 21 |
| Administrative and Troubleshooting            | 22 |
| Summary                                       | 24 |
| Changelog                                     | 24 |
| About the Author and Contributors             | 24 |
| Feedback                                      | 24 |

## Horizon 8 Frequently Asked Questions (FAQs)

### Overview

The [Horizon 8](#) Frequently Asked Questions (FAQs) document provides answers to some of the most popular Horizon 8 FAQs. Explore this FAQ to gain valuable insights into the functionality, deployment, and optimization of this powerful virtual desktop and application delivery platform.

### Audience

This Horizon 8 FAQs document is intended for existing or prospective Horizon 8 IT administrators.

### Getting Started with Horizon 8

#### What is Horizon?

Horizon is a modern platform for running and delivering virtual desktops and apps across the hybrid cloud. For administrators, this means simple, automated, and secure desktop and app management. For users, it provides a consistent experience across devices and locations.

For more information, see the following:

- [What is Horizon 8?](#)

#### What is Horizon Client?

Horizon Client is software that allows you to connect your Horizon virtual desktop to a device of choice, giving you on-the-go access from any location. Clients are available for Windows, Mac, iOS, Linux, Chrome and Android. For more information, see [Horizon Clients](#) in the documentation.

#### How do you create VDI in Horizon?

Horizon allows you to set up and manage a virtual desktop infrastructure (VDI). This is achieved by creating and provisioning desktop pools for centralized management. For more information, see the [Evaluation Guide for Horizon 8](#).

#### How does Horizon work? Is it a VPN?

Horizon operates by running remote desktops and applications in data centers or the cloud, delivering them to users as a managed service. It provides flexible deployment options across private and public cloud infrastructures. Although Horizon is not a virtual private network (VPN), it employs a unified access gateway (UAG) for secure remote access. While it supports remote access via a VPN, one is not typically required. Horizon includes the display protocol, Blast Extreme, which provides users with a graphical interface to a remote desktop or published application.

For more information, see:

- [What is Horizon 8?](#)
- [Blast Extreme Display Protocol in Horizon](#)

#### What are the Horizon Control Plane Services?

The Horizon Control Plane simplifies and automates management with cloud services that connect entitlements and unify management across Horizon environments, on-premises, and in the cloud. For more information, see [Horizon Control Plane](#) in the Reference Architecture.

#### How can I evaluate Horizon?

The [Evaluation Guide for Horizon 8](#) walks you through a series of practical exercises and helps you to evaluate some of the key features of Horizon.

#### How often are major updates published?

For core Horizon components, major updates are published three to four times per year. For updates to on-premises and customer-managed components, customers should follow version compatibility guidance, and components are subject to our lifecycle policy for support.

#### What type of language support does Horizon offer?

The Horizon Client, HTML access, and remote desktops – as well as documentation – are available in English, Japanese, French, German, Simplified Chinese, Traditional Chinese, Korean, Spanish, and Brazilian Portuguese. If you use non-English keyboards and locales, you can use an IME (input method editor) that is installed in the local client system to send non-English characters to a published application. This process varies by client platform.

#### What about Horizon Cloud Service – next-gen? What is that?

Horizon Cloud – next-gen delivers a cloud-native, hybrid, and multi-cloud desktop and app virtualization platform while still providing security and not sacrificing end-user experience.

For more information, see the following:

- [What is Horizon Cloud Service – next-gen?](#)

### Architecture

#### What is the Horizon architecture?

Horizon maintains validated design documents which are tested and updated regularly, for full Horizon virtual desktop deployment and Horizon Apps published application deployment. Additional documentation on scaling requirements is also published.

- During the design phase of the deployment engagement, we will work with your organization's stakeholders to define the use cases, performance requirements, and other factors that will drive the solution design, then help create the full architecture and bill of materials required.
- Horizon supports multiple architecture options based on customer requirements and infrastructure standards. To achieve single-site or multi-site architecture, customers may choose to deploy Horizon using the pod and block approach described in the published reference architecture. During the discovery phase of implementation, we will work with you to determine the appropriate architecture for the Horizon deployment based on criteria such as decentralization and scalability.

For more information, see [Horizon 8 Architecture](#) in the Reference Architecture.

#### Describe the server infrastructure required for the system, i.e. server counts, functionality, specifications.

The server infrastructure required for Horizon typically consists of:

- Connection Server: This is the core component of the Horizon infrastructure and acts as a broker between virtual desktops and remote clients. It manages user authentication, and session management, and provides access to virtual desktops and applications. A typical deployment would require at least two Connection Servers for high availability.
- Unified Access Gateway (UAG): This is a virtual appliance that enables secure remote access from an external network to a variety of internal resources, including Horizon-managed resources.
- vSphere - This is the infrastructure platform Horizon 8 leverages to provide virtual machines and applications to end-users. It offers a world-leading hypervisor and administrative console to manage and monitor virtual machines.

For a full list of components, see [What Is Horizon 8?](#) and [Horizon 8 Architecture](#).

### Installation

#### How is Horizon deployed?

Horizon is a modern platform for secure delivery of virtual desktops and apps. Supported by the Horizon Universal License, our hybrid Horizon VDI and app deployment options deliver flexibility across deployment options: on-premises, private cloud, and public clouds.

- In a multi-cloud architecture, organizations can place pods of Horizon desktops and apps in one or more public or private clouds.

For more information, see [Horizon Configuration](#) in the Reference Architecture.

#### What network and internet connectivity speeds and bandwidth requirements are needed?

Network and connectivity requirements will depend on several factors, as detailed in our documentation.

Because these factors can vary widely, many organizations monitor bandwidth consumption as part of a pilot project. As a starting point for a pilot, plan for 150 to 200Kbps of capacity for a typical knowledge worker.

#### Provide details on the database engine installation, i.e., versions, redundancy, permissions, backups, maintenance, data sizes, and so on.

The event database stores information about Horizon 8 events as records in a database rather than in a log file. You configure an event database after installing a Connection Server instance. You can use Microsoft SQL Server, Oracle, or PostgreSQL database reporting tools to examine events in the database tables.

For details, see [Configuring Event Reporting in Horizon Console](#) in the documentation.

## Configuration

### Can Horizon support antivirus deployment in the environment?

Yes, Horizon supports the use of antivirus software in a Horizon environment and has published guidance on changes that can be made to improve virtual machine performance without unduly compromising system security. For details, see [Antivirus Considerations in a Horizon Environment](#).

### Does Horizon support persistent virtual desktops?

Yes. There are several ways to create persistent desktops in Horizon:

- You can create automated pools of full-clone virtual machines.
- If you already have virtual desktops or physical desktops created, you can import them into Horizon as persistent desktops using the manual desktop pool with a dedicated assignment.

For more information, see [Horizon Configuration](#) in the Reference Architecture.

### Can Horizon assign virtual desktops to specific endpoints (e.g. Thin-Clients or PCs) instead of assigning virtual desktops to users?

With kiosk mode, administrators can set up unattended clients that can obtain access to their desktops from Horizon.

A client in kiosk mode is a thin client or a lock-down PC that runs Horizon Client to connect to a Connection Server instance and launch a session.

- End users do not typically need to log in to access the client device, although the published desktop might require them to provide authentication information for some applications. Sample applications include medical data entry workstations, airline check-in stations, customer self-service points, and information terminals for public access.

### How are Horizon desktops delivered to end users?

Desktops can be delivered in instant-clone (non-persistent) as well as dedicated (persistent) desktops. Common desktop types (i.e., knowledge workers, call center workers, contractors, and so on) can be grouped and administered via desktop pools, which share a common gold image for efficient provisioning. Users can gain entitlements to desktop(s) or applications in an automated fashion through techniques like directory memberships.

For more information, see [Horizon Configuration](#) in the Reference Architecture.

### Can Horizon restrict or allow local client drive access to the server?

Restrict or allow end users to share folders and drives on the local client system with remote desktops and published applications using the client drive redirection feature.

- If Blast is enabled, files and folders are transferred across a virtual channel with encryption.
- Using Dynamic Environment Manager, Horizon smart policies can be created to add conditions that must be met for client drive access to be allowed. For example, you can configure a policy that deactivates the client drive redirection feature if a user connects to a remote desktop from outside your corporate network.

### Does your solution block screen capture or keyloggers on the client endpoint?

Configure Screen-capture Blocking settings to allow/deny a user to take screenshots of the virtual machine or published application. Supported on Windows and macOS clients.

Configure Key Logger Blocking either per user or per device for Windows and macOS clients.

### What branding options are available to use with your software?

For on-premises and IaaS-hosted pods, customize the look and feel of your Horizon Service Center for administrator users by using an External Style Sheet.

Override some or all of the elements in the default style sheet by specifying your own in the System section of the Configuration tab. For example, you can change the colors of the top banner, replace the logo, change the font, and so on.

### Can Horizon display watermarks to protect from unauthorized reproduction and distribution?

Configure Horizon to display a digital watermark that shows traceable information which can deter people from unauthorized activity. The watermark can be displayed on the following remote sessions:

- Published applications and applications running on a desktop pool
- Virtual desktops and RDS hosts
- Nested mode
- Multiple monitors
- Primary session in a collaborative session
- Screen capture applications and the Print Screen key operated from the client system and within the remote desktop include the watermark.

### Scalability, Availability, and Infrastructure

#### How do you scale Horizon deployments?

Horizon scales independently, depending on the required number of supported users. Physical and virtual servers are added to the server pools to scale horizontally. Virtual resources are added to the infrastructure to scale vertically.

See [Scalability and Availability](#) in the Reference Architecture.

#### Can your solution enable access to physical desktops as well?

Although best known for its myriad benefits when implementing virtual desktops and application servers, Horizon also offers the option to broker access to physical machines. This provides an excellent and familiar experience for employees.

Brokering to physical machines can be implemented either with an existing Horizon environment or with a new one. With minimal components required, this solution can be implemented quickly.

For more information, see [Using Horizon to Access Physical Windows Machines](#).

#### How does Horizon eliminate boot storm when all users log in at once on shift?

Horizon includes Instant Clones for provisioning virtual machines from a powered-on primary image that shares both disk and memory. Instant Clone uses the same technology leveraged in vMotion that will duplicate the VM in memory and include it in a Horizon pool in an average of 1 second per VM thus limiting the amount of IOPS required on disk since there is no “boot time” removing the boot storm concern.

When a user logs out of the desktop, that desktop always gets deleted and recreated as a fresh image from the latest patch. This process creates a staggered approach to patching, thus eliminating “boot storms,” reducing storage IOPS, and creating less of a load on the vCenter Server.

In addition, all the installers for the various Horizon components, agents, and client software can be run from the command line, with switches for various installation options.

#### Does Horizon support load balancing?

Load balancing applies to multiple components differently. We can load-balance end-users to resources, then load-balance once the user is brokered or when using shared desktops and applications (RDSH).

- Load-balancing Connection Servers:

We recommend that multiple Connection Servers be deployed in a load-balanced replication cluster. This ensures that user load is evenly distributed across all available servers and a single namespace can be used by end-users.

The load balancer serves as a central aggregation point for traffic flow between clients and Connection Servers, sending clients to the best-performing and most available Connection Server instance.

For details, see [Load Balancing Connection Servers](#) in the Reference Architecture.

- Load-balancing platform infrastructure:

Admins can configure load balancing for RDSH server farms through the Horizon Console.

For details, see [Configuring Load Balancing for RDS Hosts in Horizon Console](#) in the documentation.

#### Does Horizon have High Availability/Disaster Recovery?

Horizon can be deployed in either a failover model or a multi-environment model to achieve high availability and support your overall disaster recovery plan. The published reference architecture addresses multi-site options for both active/passive and active/active models enabled through Horizon Cloud Pod architecture.

For details, see [Multi-site Architecture](#) and [Providing Disaster Recovery for Horizon](#).

## External Access

Describe how Horizon allows end users to access resources and applications.

In the Horizon Console, set up authentication for users and groups to control access to apps and desktops.

Configure entitlements to control which remote desktops and apps your users can access.

For details on the communication flow, see [Internal Connections](#) and [External Connections](#) in [Understand and Troubleshoot Horizon Connections](#).

Describe Role-Based Access Control for administrators.

You can use Unified Access Gateway to enforce least-privilege access. Unified Access Gateway ensures that connections to virtual apps and desktops are always from trusted, authenticated, and authorized users, who are restricted to using managed and compliant devices.

Describe the mobile functionality supported by the system, i.e. mobile OS, mobile apps, mobile hardware.

The solution supports access via mobile devices - including a range of form factors such as tablets and handheld devices - with Horizon Clients available for iOS and Android, as well as Windows and Linux. These clients are developed to support mobile OS and hardware features such as biometric identification, display pivot, external monitors, client-side soft keyboards and touchpads, gestures, unity touch, and more.

For more information, see [Horizon Clients](#) in the documentation.

Does Horizon support IPv4 and IPv6?

Horizon supports IPv6 as an alternative to IPv4. A Horizon pod must be either IPv6 only or IPv4 only. However, connections from both IPv4 and IPv6 client devices to the same Horizon pod are supported through Unified Access Gateway.

### Authentication

#### Can Horizon use Entra ID for identity verification authentication?

Yes - Microsoft Entra ID (formerly Azure AD) can be used for Horizon user authentication in two ways:

- Using Workspace ONE Access (included in entitlement) - Directly with the Unified Access Gateway performing third-party SAML authentication with an Entra ID Enterprise application added from the Entra ID Gallery
- Then either True SSO can be used on Horizon for a seamless end-user experience, or the user can enter an AD password, whichever the customer prefers.

Beyond Horizon, Workspace ONE acts as a single point of entry for all end-user apps and desktops and can use Entra ID as an identity service.

Workspace ONE integration with Microsoft goes beyond authentication, allowing customers to use managed device data such as device compliance state in the Entra ID conditional access policies. The integration gives you the ability to set different conditional access policies for individual Office 365 applications.

#### Does Horizon provide SSO?

Horizon provides a True SSO (single sign-on) feature that allows users to log in with third-party identity provider credentials and access a virtual desktop or published application without having to supply their AD credentials. With True SSO, a user can log in using a non-AD method (for example, RSA SecurID credentials), and once authenticated, the user can launch any entitled desktop or application without being prompted for a password. True SSO uses SAML (Security Assertion Markup Language) to send the User Principal Name to the identity provider's authentication system to access AD credentials. Horizon then generates a unique, short-lived certificate for the Windows login process.

For more information, see [Setting up True SSO](#) in the Reference Architecture.

#### Describe how your solution supports Network Access Control (NAC) or device authentication to ensure only authorized thin client devices are permitted to access the virtual desktop environment.

Horizon supports Network Access Control (NAC) or device authentication to ensure only authorized thin client devices are permitted to access the virtual desktop environment. This is achieved through a feature called Client Certificate Authentication.

Client Certificate Authentication is a method of authentication that uses digital certificates to verify the identity of thin client devices before allowing them to connect to the virtual desktop environment. Each thin client device is issued a unique digital certificate that is used to authenticate the device when it connects to the virtual desktop environment. This ensures that only authorized thin client devices are allowed to access the virtual desktop environment, providing an additional layer of security.

#### Does Horizon provide Active Directory (or LDAP) for authentication Windows Server versions?

Horizon supports Active Directory on Windows Server 2012R2 and above.

Horizon supports certain Active Directory Domain Services (AD DS) domain functional levels.

- Configure domains and trust relationships
- Create an OU for remote desktops
- Creating OUs and groups for kiosk mode client accounts
- Create groups for users
- Create a user account for the vCenter server

## Profile Management

Can Horizon manage the environment settings through group policy templates or a built-in policy manager?

Create Horizon smart policies in Dynamic Environment Manager.

When you define a Horizon smart policy, you can add conditions that must be met for the smart policy to take effect.

For example, you can configure a policy that deactivates the client drive redirection feature if a user connects to a remote desktop from outside your corporate network.

Besides smart policies, Dynamic Environment Manager allows administrators to manage many Windows environment settings, and application-specific templates are available to manage application profile settings.

Can Horizon customize user personas?

As part of the Horizon platform, Dynamic Environment Manager provides for user personalization and dynamic policy configuration for virtual desktops, session-based desktops, and RDSH-published applications. Dynamic Environment Manager can deliver persistent personal settings within the virtual desktop across any endpoint. Contextual policies for user profile management ensure that IT can map policy settings that tie directly to the end user's device and location. These can include authentication, security settings, printer mapping, and more.

Dynamic Environment Manager Agent starts at login when configured for user accounts, or at machine startup when configured for computer accounts. The agent imports policy settings, including application and user environment settings, from a configuration share. It also optionally loads personalization settings from a user profile archives share. You can use the provided AD Group Policy Object (GPO) administrative templates to enable and configure the agent, though a NoAD mode of configuration is also an option.

Horizon enables simplified app provisioning through App Volumes. You can bundle applications and data into specialized read-only containers called packages. You can assign packages to users, groups, computers, or organizational units, and deliver applications through them. Using the App Volumes Manager, you can create, provision, assign, update, edit, delete, and manage packages.

Describe the process for backing up, restoring, and resetting users' application settings and user preferences.

Dynamic Environment Manager provides for user personalization and dynamic policy configuration for virtual desktops, session-based desktops, and hosted (RDSH-published) applications.

Dynamic Environment Manager requires a network file (SMB) share to store system and user settings. This is the responsibility of the customer, and it is recommended that it be located as close as possible to the Horizon pods.

Customers manage the backup of this for High Availability and Disaster Recovery purposes.

Describe the granularity of accessing/resetting users' application settings and user preferences.

Use the Horizon Remote Desktop Features and GPOs to configure remote desktop features installed with Horizon Agent on virtual desktops or an RDS host. Configure policies controlling the behavior of desktop and application pools, machines, and users.

For details see [What is Horizon 8?](#) and [Horizon Group Policies](#) in the Reference Architecture.

Can Horizon automatically provision apps for users based on device type, user type, and other profiles?

Built on a modern management and monitoring platform, App Volumes provides reliable application delivery and user environment management with powerful workflows. Provision applications faster, deliver context-aware user policy and isolate apps as needed, enabling "follow-me" applications and user settings for a personalized and consistent user experience.

### Security and Encryption

Does Horizon 8 use cryptographic protection that is FIPS 140-2 certified?

Horizon can perform cryptographic operations using FIPS (Federal Information Processing Standard) 140-2 compliant algorithms. You can enable the use of these algorithms by installing Horizon in FIPS mode.

- Not all Horizon features are supported in FIPS mode. Also, Horizon does not support upgrading from a non-FIPS installation to a FIPS installation.

For details, see the following:

- [Installing Horizon 8 in FIPs Mode](#)
- [Federal Information Processing Standard \(FIPs\) 140-2 & 140-3](#)

Describe the security functions or configurations available in your VDI platform.

Horizon supports security configurations across solution components, including:

- Required system and database login accounts.
- Configuration options and settings that have security implications.
- Resources that must be protected, such as security-relevant configuration files and passwords, and the recommended access controls for secure operation.
- Location of log files and their purpose.
- External interfaces, ports, and services that must be open or enabled for the correct operation of Horizon.

Is Horizon data encrypted?

In general, devices will connect via a Horizon Client, installed on an endpoint or as a native mobile application (e.g., iOS). Client software is available from app stores or from Horizon for iOS, Android, Chrome, Windows, Linux, and macOS so that users can access published applications from any device. An HTML Access web client is also available, and it does not require installing any software on client devices. By default, SSL (HTTP over SSL) encrypted client authentication is supported by the Horizon Connection Server.

- When clients connect to a remote desktop or application with the PCoIP or Blast Extreme display protocol from Horizon Clients can connect through the applicable Secure Gateway component on a Horizon Connection Server instance or Unified Access Gateway appliance. This connection provides the required level of security and connectivity when accessing remote desktops and applications from the Internet.
- Unified Access Gateway appliances include a PCoIP Secure Gateway component and a Blast Secure Gateway component, which offers the following advantages:
- The only remote desktop and application traffic that can enter the corporate data center is traffic on behalf of a strongly authenticated user.
- Users can access only the resources that they are authorized to access.
- The PCoIP Secure Gateway connection supports PCoIP, and the Blast Secure Gateway connection supports Blast Extreme. Both are advanced remote display protocols that make more efficient use of the network by encapsulating video display packets in UDP instead of TCP.
- PCoIP and Blast Extreme are secured by AES-128 encryption by default. You can, however, change the encryption cipher to AES-256.

What user data is collected by your solution? Is any of this data publicly accessible?

For full details on the types of data collected, and how we process and collect data, refer to the Privacy datasheets on [Trust Center for Horizon Privacy](#).

How does Horizon restrict users from installing software on the virtual environment to prevent the use of unauthorized and malicious software?

Protecting any [Horizon environment](#) from unauthorized or malicious software is critical, as such threats can compromise

both the virtual environment and the underlying host systems.

If proper security controls are not implemented, session breakout can occur where users may gain access to unintended system functions or resources through application dialogs such as Command Prompt, Notepad, or other creative methods. This risk originates from the default operating system permissions granted to the user in single and multi-session environments including RDSH server environments. These behaviors are not unique to any one platform, and hence industry best practices recommend a [defense-in-depth strategy](#) to limit exposure.

Recommended best practices include:

**Application Allow-list or Application Access Control:** Administrators can also use application allow-listing to restrict the types of software that can be accessed or installed in the virtual environment . This involves creating a list of approved applications that users can install or access while blocking all other applications. For more detail see the following articles relevant to Windows Operating Systems: [Application Control for Business](#) and [App Software Restriction Policies](#) .

**User Permissions and Environment Lockdown:** Omnissa enables administrators to control user permissions and restrict access to specific applications and features. [Dynamic Environment Manager](#) and [Workspace ONE UEM](#) can be used to limit access to dialogs, system tools, and shell components that may enable breakout attempts.

**Virtualization-based Security:** To minimize threats due to persistence and enhance security, use of non-persistent resources (e.g. RDSH host VMs, single user VMs) should be configured to reset frequently. Applications can also be delivered to VMs dynamically by using [App Volumes](#), allowing for a streamlined and minimal base image with a reduced attack surface.

**Anti-virus and Anti-malware Protection:** Implement security measures within a Horizon environment by using anti-malware tools in the base image or directly on virtual machines and RDSH hosts where applicable. This ensures consistent protection against threats inside user sessions. Also, you should monitor for any signs of unauthorized software execution or breakout attempts.

## User Experience

Can users disconnect their sessions, without losing what they have open, and pick it up in a different set? (For example, shared environments, different devices, and so on)

Administrators can set a duration of time for a user to remain logged into their session even after a session has been abandoned/disconnected, meaning the desktop remains available for that period of time, allowing a user to reconnect and resume their session as it was prior to the disconnect.

For security purposes, a Horizon administrator can set timeouts that log a user off or lock the session after a period of inactivity. This timeout applies to VDI Desktop Assignments, as well as both session-based desktop and published application connections.

New session IDs are created each time a user or administrator logs out of the solution fully.

Are monitor configurations connected at the client endpoint supported? Does Horizon dynamically adjust for changes in endpoint monitor configuration?

Horizon supports using multiple monitors with a remote desktop.

If Horizon Client uses all monitors, when you maximize an application window, the window expands to the full screen of only the monitor that contains it.

If you use two monitors, the monitors are not required to be in the same mode. For example, if you are using a laptop connected to an external monitor, the external monitor can be in portrait mode or landscape mode.

Monitors can be placed side by side, stacked two by two, or vertically stacked only if you are using two monitors and the total height is less than 4096 pixels.

Additional considerations apply for 3D rendering, 4K resolution, specific display protocols, and vGPU.

Due to the number of variables in your end users' environments that can affect their graphical user experience — such as network conditions, bandwidth consumption, workload intensity, and so on — testing is recommended so that you can identify the usability, cost, and performance mix which best meet your specific business requirements.

Does Horizon allow applications to appear in the start menu or on the local desktop providing a familiar application access experience for users?

Horizon enables admins to create shortcuts for entitled applications that appear in the Windows Start menu, on the Windows desktop, or both.

## Display Protocol, Multimedia, and Graphics

### Does Horizon support the latest GPU, NVIDIA GPU, and vGPU?

Horizon offers three types of graphics acceleration:

- Virtual Shared Graphics – Share a GPU across multiple virtual desktops.
- Virtual Shared Pass-through Graphics – Share a GPU across multiple virtual desktops, without using the proprietary 3D driver.
- Virtual Dedicated Graphics Acceleration – Provides each user with unrestricted, fully dedicated access to one of the host's GPUs (also called GPU pass-through).

### What multimedia support does Horizon have?

Horizon supports multiple display protocols – including PCoIP and Blast Extreme – with built-in features that adapt to network conditions automatically, delivering the best experience possible.

- Horizon with Blast Performance includes an array of offerings to optimize audio and video across formats such as HTML5, QuickTime, and Windows Media, as well as applications such as Skype, Cisco WebEx, and more.
- Blast Extreme Performance- Enable power users and designers to collaborate with global teams in real time with immersive 2D and 3D graphics seamlessly rendered on any device, accessible from any location with Blast 3D, built on the broadest virtualized graphics capabilities in the industry, including hardware-accelerated graphics with NVIDIA GRID vGPU technology.
- Deliver an immersive, feature-rich user experience for end users, across devices, locations, media, and network connections with Blast Performance. Bring secure, workstation-class performance and rich 2D and 3D graphics from the cloud to remote and mobile workers with Horizon with Blast 3D.

### Does Horizon provide lossless image quality?

Horizon supports "build to lossless" using the Blast display protocol (also available for PCoIP); this encoding approach provides a highly compressed initial image that progressively builds to a full lossless state.

### What options are there to control/tune frame rate if required?

Frame rate control and tuning can be set for the Blast Extreme display protocol using GPO or Dynamic Environment Manager (DEM) policies. Policies set by DEM can be set on a contextual basis.

- Control how PCoIP renders images during periods of network congestion. The Minimum Image Quality, Maximum Initial Image Quality, and Maximum Frame Rate values interoperate to provide fine control in network-bandwidth constrained environments.

### Does Horizon have a seamless and resizable application window?

Configure the display window size through the Horizon Client, via URI, group policy, or command line.

### Does Horizon support mechanisms to reduce network bandwidth utilization per user/policy?

Yes - With Smart Policies, you can use the Bandwidth profile policy setting to configure a bandwidth profile for PCoIP or Blast sessions on a per-user basis.

If you use the PCoIP or the Blast Extreme display protocol, you can adjust several elements that affect bandwidth usage. Configure the image quality level and frame rate used during periods of network congestion. For session bandwidth, you can configure the maximum bandwidth, in kilobits per second, to correspond to the type of network connection, such as a 4Mbit/s Internet connection. The bandwidth includes all imaging, audio, virtual channel, USB, and PCoIP or Blast control traffic.

### Describe the typical frame rate.

Configure policies and behaviors for the Blast display protocol, including settings such as:

- Audio playback
- Image Quality
- Max Frame Rate
- Max Session Bandwidth



## Image Management

How does Horizon handle image management, creation, updates, and modifications for virtual machines?

- To create an image, you use vSphere to create the VM, and then you install the Windows OS, Tools, Horizon Agent, and optionally the other agents for Dynamic Environment Manager and App Volumes. You can then install any other applications you choose, perform various optimization tasks, and finally take a VM snapshot that you will select when creating an instant clone desktop pool or RDSH server farm. To update or modify VMs, because instant clone desktop pools share a base image, you can quickly deploy updates and patches by updating the parent virtual machine.
- The push image feature allows you to make changes to the parent virtual machine, take a snapshot of the new state, and push the new version of the image to all users and desktops on a rolling basis. When a user logs off an instant clone virtual desktop, Horizon deletes the instant clone and creates a fresh new instant clone from the latest version of the image, and the new clone is ready for the next user to log in.

## End-User Capacity

### Which desktops does Horizon support?

Horizon provides a single platform for delivering hosted Windows applications and shared desktop sessions from Windows Server instances using Microsoft Remote Desktop Services (RDS), virtual desktops, and ThinApp packaged applications. Horizon supports both Windows- and Linux-based desktops, including RHEL, Rocky, Ubuntu, CentOS, and NeoKylin.

### Can Horizon provide support for published applications?

Provide end users with published Windows-based applications via RDS hosts, by using the same Horizon Client that they previously used for accessing remote desktops, and they use the same Blast Extreme or PCoIP display protocol. Alternatively, users can access published desktops and apps via the HTML Access web client, if they do not want to install the Horizon Client software on their device.

To provide a published application, install the application on an RDS host, or create App Volumes packages and assign them to computer or group accounts for RDS hosts. One or more RDS hosts make up a farm, and from that farm, administrators create application pools in a similar manner to creating desktop pools. Using this strategy simplifies adding, removing, and updating applications; adding or removing user entitlements to applications; and providing access from any device or network to centrally or distributed application farms.

### Can Horizon run two different versions of the same application, as application virtualization, without any conflict from the underlying operating system (OS) of the VDI?

App Volumes supports easy maintenance of multiple versions of a single app, including markers to identify and assign current versions while preserving the ability to assign older versions for specific purposes.

### How does Horizon deliver applications to end-users?

Horizon supports apps on a wide range of platforms, including Windows and Linux, as well as Remote Desktop Services (RDS) hosted apps, packaged apps with ThinApp, and software-as-a-service (SaaS) apps.

- Windows apps can be installed either in the base image or via App Volumes packages.
- Horizon includes a wizard-driven app publishing process that includes selecting the users who are entitled to an application or app pool. The wizard lists both natively installed apps and App Volumes applications in the same list, simplifying the pool creation and user entitlement process.
- Using Dynamic Environment Manager and App Volumes, the applications can maintain unique configurations across versions and in alignment with a user's permission. Conditional Policies, for example, can allow the configurations to occur based on a set of criteria that you dictate towards one user versus another using the same application.

## Unified Communications Support

### Does Horizon use unified communications technology?

Horizon supports customers who want to utilize softphones and unified communications technology. The strategy for utilizing unified communications technology with virtual desktops is dependent on the vendor, however, most involve utilizing supported versions of their products that allow for offloading the VoIP workload to ensure efficient communication between endpoints. Support fully optimized unified communications and real-time audio-video (RTAV) with Blast Live Communications. Real-time audio-video allows Horizon users to run Skype, WebEx, Microsoft Teams, and other online conferencing applications in their remote sessions. With Real-Time Audio-Video, webcam and audio devices that are connected locally to the client system are redirected to the remote sessions. This feature redirects video and audio data with a significantly lower bandwidth than can be achieved by using USB redirection.

### Does Horizon support session collaboration?

With Session Collaboration, multiple users can view and modify the same desktop which can be very useful in healthcare, design, engineering, and education organizations for peer reviews, design iterations, and training. The desktop owner can invite multiple additional users to collaborate in real-time on his or her desktop and do so with a great user experience for all users.

### Does Horizon support voice, video, and collaboration?

Horizon has released Media Optimization for Microsoft Teams to deliver exceptional experiences for end-users, offloading audio, video, and screen-sharing to the endpoint.

Microsoft Teams media processing takes place on the client machine instead of the virtual desktop.

### How does Horizon support Skype for Business?

Horizon offers optimized support for Microsoft Skype for Business through a Virtualization Pack. The solution delivers exceptional audio and video either directly between endpoints for one-to-one collaboration or offloads it to a central Multipoint Control Unit (MCU) for multiparty conference calls or meetings.

The optimized solution delivers a better user experience and avoids increased data center infrastructure traffic, which can lead to chokepoints and performance issues.

## Printing and Peripherals

### Does Horizon support printing?

Print from a remote desktop to any local or network printer available on the client computer with Integrated Printing.

- Support client printer redirection, location-based printing, and persistent print settings.
- The location-based printing feature of Integrated Printing maps printers that are physically near client systems to remote desktops.
- Location-based printing is supported on the following remote desktops and applications.
- Remote desktops that are deployed on single-user machines, including Windows desktop and Windows Server machines.
- Published desktops and published applications that are deployed on RDS hosts, where the RDS hosts are virtual machines or physical machines.
- Available for Windows, Mac, Linux, mobile client devices, and browser-based clients.

### Does Horizon support specialty printing such as label or barcode printers?

Use local printer redirection for specialized printers such as barcode printers and label printers connected to the client.

The virtual printing feature allows end users on some client systems to use local or network printers from a remote desktop without requiring that additional print drivers be installed in the remote desktop operating system. The location-based printing feature allows you to map remote desktops to the printer that is closest to the endpoint client device.

With virtual printing, after a printer is added to a local client computer, that printer is automatically added to the list of available printers on the remote desktop. No further configuration is required. Users who have administrator privileges can still install printer drivers on the remote desktop without creating a conflict with the virtual printing component.

### Is peripheral support available?

Administrators can configure peripheral connection options for printers, disk volumes, cameras, scanners, serial devices, and USB devices. A virtual desktop can accommodate up to 128 USB devices. You can also redirect certain locally connected USB devices for use in published desktops and applications.

### Does Horizon support peripherals such as drawing tablets, and signature pads?

Horizon supports human interface devices (HID) such as tablets through USB forwarding.

### Can Horizon restrict USB devices?

Deactivate USB redirection for all desktop pools, for specific desktop pools, or specific users in a desktop pool.

### Does Horizon use smart cards?

Horizon supports smart card authentication directly through the connection server, or via SAML assertion passed from a third-party solution such as a load balancer. Smart cards are supported on Horizon clients for Windows devices, macOS, Linux, and Chrome endpoints.

## Administrative and Troubleshooting

### Does Horizon have a centralized console for management and administrator tasks?

Horizon Console is the web interface for Horizon through which you can create and manage virtual desktops and published desktops and applications.

This single administration console provides detailed levels of control, allowing you to customize the end-user experience, access, and personalization to support corporate policy.

As an administrator, you have centralized control, efficiency, and security by storing desktop data in the data center.

Using the Horizon Console, you can manage your desktop and application pools and farms, segment the type of access given to end-users based on an enhanced role-based access mechanism, and do cross-pod management from any browser, using the Cloud Pod Architecture (CPA). You are provided with a rich feature set and an enhanced user experience, including:

- Standard and customer role-based access
- Desktop and application pools and farm creation
- Restyled dashboard
- Smart card authentication- RDSH load balancing
- VM Hosted Apps (for Windows multi-session VMs)
- Image scale-out- Cloud pod architecture

For customers with a Universal License, the Horizon Universal Console gives you access to several additional Horizon Control Plane Services, including license management, infrastructure monitoring, connection component status, and capacity.

Depending on which optional components are used, other consoles are required. For App Volumes, a separate App Volumes Manager console is used. For Dynamic Environment Manager, a separate Dynamic Environment Manager Management console is used.

### Does Horizon's administrator console define the scope and role of administrative functions for compliance and control?

The Horizon Cloud console enables role-based access control for administrators through the Cloud Console, with a range of options to help support customer access management:

For on-premises and IaaS-hosted pods, Horizon also includes built-in role-based delegated administration for control over who can use Horizon Console and what tasks those users are authorized to perform. Horizon Console presents the combination of a role, an administrator user or group, and an access group as a permission. The role defines the actions that can be performed, the user or group indicates who can perform the action, and the access group contains the objects that are the target of the action. Selectively assign administrative rights by assigning administrator roles to specific Active Directory users and groups, with additional settings for permissions, privileges, access, and more.

### How easy is it to find information while using Horizon?

Within the Horizon Console (on-premises), administrators can search console data with the additional ability to select filtering criteria that are related to the objects you are searching for.

Within the Horizon Universal Console, you can search within either users or VMs. After you select a search of users or VMs, enter your search term into the search text box. When you have entered at least three (3) characters in the search text box, names that begin with those characters are displayed. You can continue entering more characters to narrow down the results. With the VMs search, you can search for RDS server VMs in farms and VDI desktop VMs that are provisioned in your Horizon Cloud tenant environment.

### Does Horizon provide detailed audit records for all associated components?

Horizon creates log files that record the installation and operation of its components (Horizon Agent, Published Applications, Connection Server, Horizon Services). Data includes usage of the system (for example, login times, and audit information tracking changes to service configuration and operations; data about the end users' usage of the system, for example, login times, application and desktop launches, RDSH performance data, RDSH hostname, and client IP address).

The event database stores information about events that occur in the Horizon Connection Server host or group, Horizon Agent, and View Administrator, and notifies you of the number of events on the dashboard.

In addition to monitoring events in Horizon Console, you can generate Horizon events in Syslog format so that the event data can be accessible to analytics software.

Within the Horizon Cloud Next-Gen Console, access activity logs covering Admin event logs and system events, as well as End User logs, which can be exported to CSV for storage and analysis.

### Does Horizon offer APIs?

Horizon enables automation and reporting through a growing collection of RESTful APIs- Categories of API endpoints include:

- Authentication and authorization
- Configuration of Horizon components
- Entitlements for apps and desktop pools
- External data retrieval
- Inventory data
- Monitoring of Horizon services

### Can Horizon record the user's session to track all the user's activities?

Horizon supports session recording through the Recording feature, which allows administrators to record desktop sessions to monitor user behavior on a Windows desktop.

When enabled, Recording starts automatically upon user login and alerts the user that the session is being recorded.

Recordings are stored as MP4 and can be downloaded to play in a local player or viewed in the Recording web console.

### Can Horizon provide a consolidated view of the entire VDI to identify potential bottlenecks in performance?

Use Horizon Console to view information about global entitlements, pods, sites, and home sites.

Horizon Console displays monitoring information about Connection Server instances, the event database, gateways, datastores, vCenter Server instances, domains, and sessions in a Cloud Pod Architecture environment.

### Is it possible to uniquely identify a user with a session at any given time?

The Help Desk feature allows the administrator to type in the name of the user and bring up a user card that contains information about the sessions launched by the user. Administrators can also use the Desktop sessions report that provides administrators with a history of all the sessions a particular user has launched over a pre-defined period (e.g., Past 24 hrs., 7 days, 15 days, and so on).

### Is help desk support available?

Horizon Help Desk Tool enables help desk staff to take quick actions to help get the user up and running again with a simple interface that provides performance and configuration information.

- View resource consumption for CPU and memory, along with latency information
- Provide remote user assistance actions, including:
  - Sending a message to the user,
  - Launching Microsoft Remote Assistance to actively help the user in session,
  - Disconnecting and resetting the VM.
- Administrator actions through the Help Desk Tool are captured in the Event Log.
- For organizations that have deployed the Horizon Universal Console, administrators can access help desk information for users accessing cloud-connected pods. This can include information on current sessions, assignments, desktops, applications, and activities.

Summary

This Horizon 8 FAQ document covered everything from initial setup to advanced configurations and troubleshooting. Topics included installation, configuration, scalability, security, user experience, and administrative tasks.

Changelog

The following updates were made to this guide:

| Date       | Description of Changes |
|------------|------------------------|
| 2024/02/26 |                        |

About the Author and Contributors

This document was created by:

- Brittany Coleman, Content Strategist, Omnissa
- [Gina Daly](#), Technical Marketing Manager, Omnissa
- [Rick Terlep](#), Staff Technical Marketing Architect, Omnissa

Feedback

Your feedback is valuable.

To comment on this paper, contact End-User-Computing Technical Marketing at [euc\\_tech\\_content\\_feedback@omnissa.com](mailto:euc_tech_content_feedback@omnissa.com).

