

This PDF was generated on October 2024 and was current at the time of download. To check for the latest version please visit
<https://techzone.omnissa.com/resource/omnissa-horizon-blast-extreme-display-protocol>

Omnissa Horizon Blast Extreme Display Protocol

Omnissa Horizon

Table of contents

Omnissa Horizon Blast Extreme Display Protocol	3
Introduction to Horizon Blast Extreme	3
Horizon Blast Extreme Benefits	4
Security Features	5
Components of Horizon Blast Extreme	6
Configurable Components	6
Client-Side Components	6
Agent-Side Components	7
Log File Locations for Client and Agent Components	7
Horizon Blast Extreme Network Connections	8
Internal Connection	8
Tunneled Connection	8
External Connection	8
Deployment	9
Omnissa Horizon Software Requirements	9
Software Requirements for Physical Desktop Machines	9
Port Requirements	9
Configuration and Optimization	9
Summary and Additional Resources	10
Additional Resources	10
Changelog	10
Authors and Contributors	10
Feedback	10

Omnissa Horizon Blast Extreme Display Protocol

Introduction to Horizon Blast Extreme

Display communication protocols provide end users with a graphical interface to a remote desktop or published application. Omnissa Horizon® Blast Extreme is a display protocol built by Omnissa to deliver an immersive, feature-rich experience for end users across devices, locations, media, and network connections. Horizon Blast Extreme is included with [Omnissa Horizon® 8](#) and [Omnissa Horizon® Cloud Service](#), which provide the latest generation of Horizon desktop virtualization and remote application-delivery software.

This guide provides a technical description of the Horizon Blast Extreme display protocol, including its benefits, limitations, and deployment options, for administrators who are considering using Horizon Blast Extreme in their organization today.

This guide is intended for IT administrators and evaluators who are at least somewhat familiar with Omnissa Horizon® VDI. Readers should also have a solid understanding of desktop and application virtualization, as well as a good working knowledge of networking and supporting infrastructure, covering topics such as Active Directory, Group Policy, and supporting technologies.

Horizon Blast Extreme Benefits

Horizon Blast Extreme provides

- End-users access to their personalized virtual desktops or remote applications from company laptops, their home PCs, thin client devices, Macs, tablets, or smartphones.
- A consistent user experience across devices and locations while keeping corporate data compliant and securely stored in the data center.
- Ability to meet performance requirements for visually demanding applications when used with certain GPU-based hardware acceleration in the host.
- Broad client support, including Windows, Linux, Mac, Android, iOS, Chrome, and web (HTML Access) clients.
- Ability to use either the TCP or the UDP network transport.
- Intelligence to determine and accommodate varying network conditions.
- Flexibility with regard to configuration methods, which include using Windows Group Policy or Horizon Smart Policies included with [Omnissa Dynamic Environment Manager](#).
- Option to simplify setup, including opening only one port (TCP 443) on front-end firewalls when [Omnissa Unified Access Gateway](#) is used as the secure gateway.

For a detailed list of Horizon Blast Extreme features, see the [Horizon Omnissa Blast Extreme](#) topic in the [Horizon Overview and Deployment Planning](#) guide.

Security Features

Horizon Blast Extreme includes the following security features to support Horizon:

- AES (Advanced Encryption Standard) encryption – All TCP and UDP connections use TLS to encrypt communication. TLS version and encryption defaults are routinely updated to reflect current best practices. Horizon Blast Extreme is secured by AES-128 encryption by default. You can, however, change the encryption cipher to AES-256.
- Security certificates – For external connections, Horizon Blast Extreme can use the security certificate on the Unified Access Gateway appliance. Horizon Blast Extreme can also use the certificate thumbprint of the Blast Secure Gateway or virtual desktop. A certificate thumbprint is a cryptographic hash of a certificate.
- SHA-256 signatures – Horizon Blast Extreme uses the latest security algorithms, including SHA-256.
- Dual IPv4/IPv6 support – When using Horizon Blast Extreme, Unified Access Gateway can be used to bridge between IPv6 Omnissa Horizon Clients and an IPv4 backend and agents. The Horizon Clients can use either IP version 4 or 6. Horizon Blast Extreme must be on TCP 443 only (as described previously for port sharing).
- FIPS support – FIPS-ready libraries are available for Unified Access Gateway appliances.
- Common Criteria – Horizon 8.7 (2209) and later versions are certified for Common Criteria compliance by the National Information Assurance Partnership (NIAP).
- Port sharing – If you use a Horizon Unified Access Gateway virtual appliance for connections from outside the corporate network, by default the connection uses TCP port 8443 and optionally UDP port 8443. It is possible to configure the Blast External URL on the Unified Access Gateway appliance to use port sharing on TCP port 443 so that no additional ports need be opened on the front-end firewall.

Components of Horizon Blast Extreme

Display protocols must be able to efficiently provide the best user experience for various types of screen content, including text, still images, streaming video, 3D rendering, and audio. Horizon Blast Extreme was built to handle even the most demanding graphical workloads, including medical imaging and designing geographic information systems (GIS) applications used for analyzing large data sets, creating maps, and visualizing scenarios of the outside world, in both 2D and 3D.

Configurable Components

Various components of a display protocol can be configured to address the different types of screen content and differing network speeds that end users are likely to encounter. These components include the transport protocol and display protocol codec:

- Transport protocol – Horizon Blast Extreme supports two transport protocols to carry the display traffic between clients and the Horizon infrastructure: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
- Display protocol codec – A codec is used to encode and decode the screen content transferred by Horizon Blast Extreme. Depending on the type of client device Horizon Blast Extreme supports the following codecs: H.264, HEVC (H.265), AV1, Adaptive, and the BlastCodec. The image formats used by these codecs employ compression to reduce the size of the content before it is transferred across the network.

For details about the various display protocols, see the product documentation topic [Summary of Codec Options](#).

Omnissa Horizon Blast Extreme uses client-side components, installed with [Omnissa Horizon Client](#), as well as agent-side components, installed on virtual desktops, physical desktops, and RDSH servers that host published applications and desktops.

Client-Side Components

Optimized for the mobile cloud, Horizon Blast Extreme supports a broad range of client devices, including Windows, Linux, Mac, Android, iOS, Chrome, and web (HTML Access) clients. On the client side, you can configure which codec or codecs to use for encoding and decoding the screen content transferred by Horizon Blast Extreme.

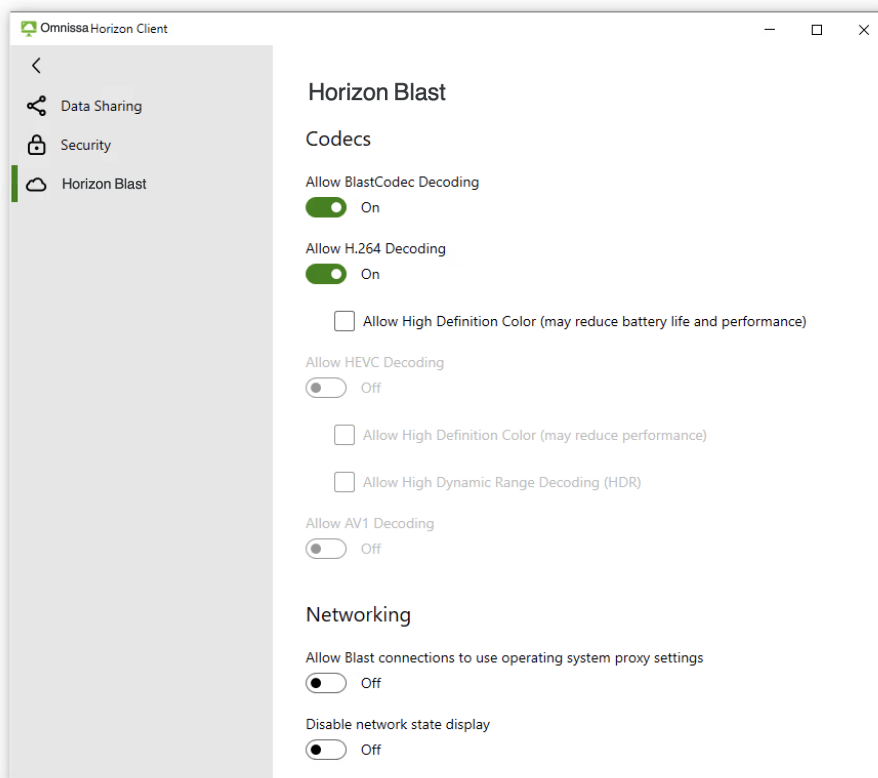


Figure 1: Horizon Blast Extreme Settings on Horizon Client for Windows

Note: Different types of client devices support different features of Horizon Blast Extreme. To find out which Horizon Blast Extreme settings are available for a specific client platform, see the Horizon Client user guide for that platform, available from the [Omnissa](#)

[Horizon Client Documentation](#) page.

Agent-Side Components

The client-side settings work in conjunction with the agent-side settings, which administrators can configure, as described in [How to Configure Horizon Blast Extreme](#), in the *Omnissa Blast Extreme Optimization Guide*.

Three Horizon Blast Extreme components are built into the Horizon Agent, which administrators install in virtual desktops and Microsoft RDSH servers:

- The Blast service (VMBlastS.exe) manages user sessions, proxies incoming TCP connections, and prepares the Blast Worker process.
- The Blast Worker process (VMBlastW.exe) captures the screen and handles everything within the session.

Log File Locations for Client and Agent Components

Log files related to Horizon Blast Extreme can be found in the following locations:

- Windows client: To collect logs on a Windows client, use the log collection feature included in Horizon Client. See [View and Collect Logs on Horizon Windows Client](#).
- Mac client: To collect logs on a Mac, use the log collection feature included in Horizon Client. See [Collecting Support Data](#).
- Horizon Agent: Logs reside in a subdirectory of the <Drive>:\ProgramData\ directory.

This directory contains logs for the three Horizon Blast Extreme components:

- Blast-Service.log
- Blast-Worker-SessionId<#>.txt
- Blast-Proxy.log

For more information about the entries in these log files, see [How to Verify Configuration](#) in the *Omnissa Blast Extreme Optimization Guide*.

The next section describes the workflow of connections made between the client and agent components.

Horizon Blast Extreme Network Connections

Horizon Blast Extreme can provide the best remote display experience, regardless of whether the user is inside or outside of the corporate network.

The following sections describe internal and external connections in a Horizon 8 deployment. For information about network connections in a Horizon Cloud environment, see [Horizon Cloud Service - next-generation Network Ports Diagrams](#).

Internal Connection

With an internal connection, the client, the Horizon 8 server, and the virtual desktop or RDSH server are all inside the corporate network. For a diagram of internal connections, see Figure 3: Blast Extreme Internal Connection in the [Internal Connection](#) section of the [Network Ports in Horizon 8](#) guide.

Tunneled Connection

With a tunneled connection, the client, the Horizon 8 server, and the virtual desktop or RDSH server are all also inside the corporate network, but the clients might be on a different subnet from that of the virtual desktops or RDSH servers (where the agent is installed), and you do not want to open ports between the clients and agents directly. Tunneling traffic through the Connection Server allows for ports to be open between the Connection Server and the client, and between the Connection Server and the agent, but not between the client and the agent.

For a diagram of tunneled connections, see Figure 13: Blast Extreme Tunneled Connection in the [Tunneled Connection](#) section of the [Network Ports in Horizon 8](#) guide.

External Connection

With an external connection, the client is connecting from outside the corporate network to the Unified Access Gateway. This gateway then directs the traffic to the correct port and location on the Horizon 8 Connection Server and agent.

For a diagram of external connections, see Figure 8: Blast Extreme External Connection in the [External Connection](#) section of the [Network Ports in Horizon 8](#) guide.

Deployment

To set up the Horizon environment for Horizon Blast Extreme, administrators open various firewall ports, the details of which are provided in the guides referenced in the earlier chapter [Horizon Blast Extreme Network Connections](#), in this guide.

In Horizon 8 environments, administrators can also select Horizon Blast Extreme as the default display protocol or as a possible protocol choice for end users:

- When creating desktop pools or server farms, in the Remote Display Settings, for Default display protocol, you can select Omnissa Horizon Blast, and you can specify whether users can choose the protocol. For Windows desktops, see the applicable section in [Desktops and Applications in Omnissa Horizon 8](#). For Linux desktops, see the applicable section in [Linux Desktops and Applications in Omnissa Horizon 8](#).
- To configure the remote display protocol at the global entitlement level, see [Cloud Pod Architecture in Omnissa Horizon 8](#).

In Horizon Cloud Service environments, the only display protocol used is Horizon Blast Extreme.

Omnissa Horizon Software Requirements

For Horizon 8 deployments, we strongly recommend using the latest version of the following components:

- Connection Server
- For external connections: Unified Access Gateway
- Horizon Client
- Horizon Agent

For specific system requirements, see the [Omnissa Horizon Documentation](#) page.

Software Requirements for Physical Desktop Machines

Horizon Blast Extreme is supported on physical desktop machines. See the product documentation topics [Prepare a non-vSphere Machine For Omnissa Horizon 8 Management](#) and [Worksheet for Creating a Manual Desktop Pool](#).

Port Requirements

For details about port requirements for connectivity between the various components and servers in a Horizon deployment, see the [Network Ports in Horizon 8](#) guide and the [Horizon Cloud Service - next-generation Network Ports Diagrams](#).

Also see the product documentation topics [Firewall Rules for Horizon Connection Server](#) and [Firewall Rules for Horizon Agent](#).

Configuration and Optimization

For information about administrator settings, end-user settings, and various optimization strategies, see the [Omnissa Blast Optimization Guide](#).

Summary and Additional Resources

Now that you have learned about the benefits and features of Horizon Blast Extreme and have seen how easy it is to configure in your Horizon environment, we hope that you will take advantage of this adaptive and purpose-built display protocol.

Additional Resources

[Omnissa Blast Extreme Optimization Guide](#)

[Omnissa Horizon Documentation](#)

[Omnissa Horizon Clients Documentation](#)

[Network Ports in Horizon 8](#)

[Horizon Cloud network ports diagrams](#)

[Omnissa Knowledge Base](#)

Changelog

The following updates were made to this guide.

Date	Description of Changes
2024-10-15	
2021-04-27	Incorporated various recent suggestions from reviewers.
2020-12-21	Updated product documentation links to use Horizon 8 documentation.
2020-04-22	Update for Horizon 7 version 7.10.
2017-07-31	Update for Horizon 7 versions 7.1 and 7.2.
2016-10-10	Initial publication date.

Authors and Contributors

[Graeme Gordon](#) is a Senior Staff Architect, Technical Marketing, Omnissa.

[Caroline Arakelian](#) is a Senior Technical Marketing Manager, Technical Marketing, Omnissa.

[Chris Halstead](#) co-authored the original version of this white paper. Chris is a Senior Staff Adoption Product Manager, Omnissa.

Feedback

Your feedback is valuable.

To comment on this paper, contact End-User-Computing Technical Marketing at tech_content_feedback@omnissa.com.

