



Network Port Diagram - Horizon View - Reference Sheet

Updated October 2013

Source: VMware KB 2061913

Reference for Port Diagram

Ref #	Source	Port	Target	Port	Protocol	Description
1	Security server	*	View Agent	4172	UDP	PCoIP (not SALSA20) if PCoIP Secure Gateway is used.
2	Security server	4172	View Client	*	UDP	PCoIP (not SALSA20) if PCoIP Secure Gateway is used.
3	Security server	500	View Connection Server	500	UDP	IPsec negotiation traffic.
4	Security server	*	View Connection Server	4001	TCP	JMS traffic.
5	Security server	*	View Connection Server	8009	TCP	AJP13-forwarded Web traffic, if not using IPsec or not using NAT.
6	Security server	4500	View Connection Server	4500	UDP	AJP13-forwarded Web traffic, when using IPsec through a NAT device.
7	Security server	*	View Agent	3389	TCP	Microsoft RDP traffic to View desktops.
8	Security server	*	View Agent	9427	TCP	Wyse MMR redirection.
9	Security server	*	View Agent	32111	TCP	USB redirection.
10	Security server	*	View Agent	4172	TCP	PCoIP (HTTPS) if PCoIP Secure Gateway is used.
11	View Agent	4172	View Client	*	UDP	PCoIP, if PCoIP Secure Gateway is not used.
12	View Agent	4172	View Connection Server or security server	*	UDP	PCoIP (not SALSA20) if PCoIP Secure Gateway is used.
13	View Client	*	View Connection Server or security server	80	TCP	<u>SSL (HTTPS access) is enabled by default for client connections, but port 80 (HTTP access) can be used in certain cases. See Notes and Caveats for TCP and UDP Ports Used by View.</u>
14	View Client	*	View security server	443	TCP	HTTPS access. Port 443 is enabled by default for client connections. Port 443 can be changed. <u>Connection attempts over HTTP to port 80 are redirected to port 443 by default, but port 80 can service client connections if SSL is off-loaded to an intermediate device. You can reconfigure the redirection rule if the HTTPS port was changed. See Change the Port Number for HTTP Redirection.</u>
15	View Client	*	View Connection Server	443	TCP	HTTPS access. Port 443 is enabled by default for client connections. Port 443 can be changed. Client connection attempts to port 80 are redirected to port 443 by default, but port 80 can service client connections if SSL is off-loaded to an intermediate device. Connection attempts to port 80 to reach View Administrator are not redirected. You must connect over HTTPS to reach View Administrator. <u>You can prevent HTTP redirection and force clients to use HTTPS. See Prevent HTTP Redirection for Client Connections.</u>

Ref #	Source	Port	Target	Port	Protocol	Description
16	View Client	*	View Connection Server or security server	4172	TCP	PCoIP (HTTPS) if PCoIP Secure Gateway is used.
17	View Client	*	View Agent	3389	TCP	Microsoft RDP traffic to View desktops if direct connections are used instead of tunnel connections.
18	View Client	*	View Agent	9427	TCP	Wyse MMR redirection if direct connections are used instead of tunnel connections.
19	View Client	*	View Agent	32111	TCP	USB redirection if direct connections are used instead of tunnel connections.
20	View Client	*	View Agent	4172	TCP	PCoIP (HTTPS) if PCoIP Secure Gateway is not used.
21	View Client	*	View Agent	4172	UDP	PCoIP, if PCoIP Secure Gateway is not used.
22	View Client	*	View Connection Server or security server	4172	UDP	PCoIP (not SALSA20) if PCoIP Secure Gateway is used.
23	View Connection Server	*	vCenter Server or View Composer	80	TCP	SOAP messages if SSL is disabled for access to vCenter Servers or View Composer.
24	View Connection Server	*	vCenter Server or View Composer	443	TCP	SOAP messages if SSL is enabled for access to vCenter Servers or View Composer.
25	View Connection Server	*	View Agent	4172	UDP	PCoIP (not SALSA20) if PCoIP Secure Gateway via the View Connection Server is used.
26	View Connection Server	4172	View Client	*	UDP	PCoIP (not SALSA20) if PCoIP Secure Gateway via the View Connection Server is used.
27	View Connection Server	*	View Connection Server	4100	TCP	JMS inter-router traffic.
28	View Connection Server	*	View Agent	3389	TCP	Microsoft RDP traffic to View desktops if tunnel connections via the View Connection Server are used.
29	View Connection Server	*	View Agent	4172	TCP	PCoIP (HTTPS) if PCoIP Secure Gateway via the View Connection Server is used.
30	View Connection Server	*	View Agent	9427	TCP	Wyse MMR redirection if tunnel connections via the View Connection Server are used.
31	View Connection Server	*	View Agent	32111	TCP	USB redirection if tunnel connections via the View Connection Server are used.
32	View Agent	*	View Connection Server instances	4001	TCP	JMS traffic.
33	View Composer service	*	ESXi host	902	TCP	Used when View Composer customizes linked-clone disks, including View Composer internal disks and, if they are specified, persistent disks and system disposable disks.
34	Security server	*	View Transfer Server	80	TCP	Local desktop check-out, check-in, and replication if tunnel connections are used and SSL is disabled for local mode operations.

Ref #	Source	Port	Target	Port	Protocol	Description
35	Security server	*	View Transfer Server	443	TCP	Local desktop check-out, check-in, and replication if tunnel connections are used and SSL is enabled for local mode operations.
36	View Client with Local Mode	*	View Transfer Server	80	TCP	Local desktop check-out, check-in, and replication if direct connections are used instead of tunnel connections, and SSL is disabled for local mode operations.
37	View Client with Local Mode	*	View Transfer Server	443	TCP	Local desktop check-out, check-in, and replication if direct connections are used instead of tunnel connections, and SSL is enabled for local mode operations.
38	View Connection Server	*	ESXi host	902	TCP	Local desktop check-out, check-in, and replication.
39	View Connection Server	*	View Transfer Server	80	TCP	Local desktop check-out, check-in, and replication if tunnel connections via the View Connection Server are used and SSL is disabled for local mode operations.
40	View Connection Server	*	View Transfer Server	443	TCP	Local desktop check-out, check-in, and replication if tunnel connections via the View Connection Server are used and SSL is enabled for local mode operations.
41	View Transfer Server	*	View Connection Server	4001	TCP	JMS traffic to support local mode.
42	View Transfer Server	*	ESXi host	902	TCP	Publishing View Composer packages for local mode.
43	View Transfer Server	*	Server that hosts the Transfer Server repository network share	445	UDP	Configuring and publishing View Composer packages to the Transfer Server repository network share.
44	Blast Client	22443	Connection Server/ Security Server	*	TCP	If you use VMware Horizon View HTML Access connect to View desktops on HTTPS port 22443 to communicate with the Blast agent.
45	Blast Client	*	Connection Server/ Security Server	8443	TCP	If you use VMware Horizon View HTML Access, the external Web client connects to a security server or connection server on HTTPS port 8443 to communicate with View desktops.
46	Connection Server	*	Active Directory/ Connection Server	389	TCP	This is used for replication with the Active Directory and/or other Connection Servers.
47	Source Connection Server	*	View Agent	22443	TCP	If you use VMware Horizon View HTML Access, connection servers and security servers connect to View desktops on HTTPS port 22443 to communicate with the Blast agent.