

ZENworks 2020 Update 1

TCP and UDP Ports

June 2020

The information in this document pertains to the default TCP and UDP ports used by ZENworks.

- ♦ [“Appliance” on page 1](#)
- ♦ [“Primary Servers” on page 3](#)
- ♦ [“Satellite Servers” on page 8](#)
- ♦ [“Managed Devices” on page 11](#)
- ♦ [“ZENworks Agent” on page 13](#)
- ♦ [“ZENworks Application” on page 13](#)
- ♦ [“Remote Management” on page 14](#)
- ♦ [“Remote Management - Using Join Proxy” on page 14](#)
- ♦ [“User Sources” on page 15](#)
- ♦ [“Databases” on page 15](#)
- ♦ [“ZENworks Reporting” on page 15](#)
- ♦ [“Legal Notice” on page 16](#)

Appliance

The following table contains information about the various ports that need to be configured for the ZENworks Appliance.

Item	Ports	Mandatory	Configurable	Firewall Requirement	Additional Details
TCP Ports	9080	Yes	No	Open TCP Port	Used by the monitoring tool to access the server.
	9443	Yes	No	Open TCP Port	Used to administer the appliance.
	8081	No	Yes	Open TCP Port	Kafka: Used by Kafka Schema Registry.
	9093	No	Yes	Open TCP port	Kafka: Used by Kafka

Item	Ports	Mandatory	Configurable	Firewall Requirement	Additional Details
	8083	No	Yes	Open TCP port	Kafka: Used by Kafka connect
	5433	No	No	Open TCP port	Vertica: Used by Vertica client (vsq, ODBC, JDBC) port. For information on all the ports that are to be open for Vertica's internal purposes, see Vertica documentation .
	5434	No	No	Open TCP port	Vertica: Used by Vertica intra and inter-cluster communication. Vertica opens the Vertica client port +1 (5434 by default) for intra-cluster communication, such as during a plan. If the port +1 from the default client port is not available, then Vertica opens a random port for intra-cluster communication. For information on all the ports that are to be open for Vertica's internal purposes, see Vertica documentation
	5450	No	No	Open TCP port	Vertica: used for Vertica Management Console. For information on all the ports that are to be open for Vertica's internal purposes, see Vertica documentation
	5444	No	No	Open TCP port	Vertica: used for Vertica Management Console. For information on all the ports that are to be open for Vertica's internal purposes, see Vertica documentation
	4804	No	No	Open TCP port	Vertica: Daemon to Daemon Connections. For information on all the ports that are to be open for Vertica's internal purposes, see Vertica documentation .
UDP Ports	5433	No	No	Open TCP port	Vertica: spread monitoring. For information on all the ports that are to be open for Vertica's internal purposes, see Vertica documentation .

Item	Ports	Mandatory	Configurable	Firewall Requirement	Additional Details
	4804	No	No	Open TCP port	Vertica: Daemon to daemon connections. For information on all the ports that are to be open for Vertica's internal purposes, see Vertica documentation .
	4803	No	No	Open TCP Port	Vertica: Daemon to daemon connections. For information on all the ports that are to be open for Vertica's internal purposes, see Vertica documentation .
	6543	No	No	Open TCP Port	Vertica: Monitor to daemon connection. For information on all the ports that are to be open for Vertica's internal purposes, see Vertica documentation .

Primary Servers

The following table contains information on the default ports used by the ZENworks Primary Server:

Item	Ports	Mandatory	Configurable	Firewall Requirement	Additional Details
Firewall Settings: TCP Inbound Ports	80 and 443	Yes	Yes	Open TCP Port	<p>Port 80 is for Tomcat non-secure port and Port 443 is for Tomcat secure port.</p> <p>Port 443 is used to transfer content from Primary Servers to other Primary Servers, Satellite Servers and managed devices.</p> <p>Port 443 is used to upload the collection data, such as inventory and system messages from the managed device to the Primary Server.</p> <p>Port 443 is also used for CASA authentication. Opening this port allows ZENworks to manage devices outside of the firewall. It is a good practice to make sure that the network is configured to always allow communication on this port between the ZENworks Server and ZENworks Agents on managed devices.</p> <p>If other services are running on ports 80 and 443, such as Apache, the installation program asks you for new ports to use.</p> <p>If you plan to use AdminStudio ZENworks Edition, it requires that the Primary Server is using ports 80 and 443.</p>
	998	Yes	No	Open TCP port	<p>Used by the Preboot Server (novell-pbserv).</p> <p>The Preboot Server (novell-pbserv) is used only with ZENworks Configuration Management.</p>
	7444	Yes	No	Open TCP port	<p>Used to view the system update status of servers and managed devices.</p> <p>IMPORTANT: This is a fixed port. During Installation and Upgrade ensure that this port is not blocked.</p>

Item	Ports	Mandatory	Configurable	Firewall Requirement	Additional Details
Firewall Settings: TCP Outbound Ports	80 and 443	Yes	Yes	Open TCP port	<p>Primary Server downloads patch license related information and checksum data over HTTPS (port 443), and the actual patch content files over HTTP (port 80). ZENworks Patch Management license information is obtained from the Ivanti licensing server (novell.patchlink.com), the patch content and checksum data is retrieved from an AKAMAI hosted content distribution network (novell.cdn.lumension.com). You must make sure that the firewall rules allow outbound connections to these addresses because the patch content distribution network is a large fault tolerant network of cache servers.</p> <p>Primary Server performs the ZENworks System Update Entitlement activation over HTTP (port 443) using the secure-www.novell.com (https://secure-www.novell.com) website. This rule can be turned off after successfully completing the entitlement activation.</p> <p>For more information, see the ZENworks System Updates Reference.</p> <p>Primary Server downloads system update related information and content over HTTP (port 443) using the you.novell.com (https://you.novell.com) website.</p> <p>For more information see Managing Update Downloads in the ZENworks System Updates Reference.</p> <p>NOTE: You must assign the Network Interface to the firewall zone. Firewall rules are applied to this zone for managing the ports used by ZENworks.</p>
	443 and 2197	Yes	No	Open TCP port	Used by ZENworks MDM Servers to communicate with the Apple Push Notification service (APNs).

Item	Ports	Mandatory	Configurable	Firewall Requirement	Additional Details
					Used for CASA authentication. It is a good practice to make sure that the network is configured to always allow communication on this port between the ZENworks Server and ZENworks Agents on managed devices when port 443 is busy.
	5550	Yes	Yes	Open TCP port	Used by Remote Management Listener by default. You can change this port in the Remote Management Listener dialog box in ZENworks Control Center. Remote Management is used only with ZENworks Configuration Management.
	5950	Yes	Yes	Open TCP port	Used by the Remote Management service, by default. You can change this port in the Remote Management Settings panel of the Remote Management Configuration page in ZENworks Control Center. Remote Management is used only with ZENworks Configuration Management.
	6789	Yes	Yes	Open TCP port	Used by ZooKeeper for incoming client connections.
	6790 and 6791	Yes	Yes	Open TCP port	Used by ZooKeeper as leader connection port and leader election port, respectively.
	7019	No	Yes	Open TCP port	Used by Join Proxy.
	7628	Yes	No	Open TCP port	Used by the ZENworks Agent for Quick Tasks. IMPORTANT: This is a fixed port. During Installation and Upgrade ensure that this port is not blocked.
	8005	Yes	No	Open TCP port	Used by Tomcat to listen to shutdown requests. This is a local port, and cannot be accessed remotely.
	9971	Yes	No	Open TCP port	Used by AMT Hello Listener to discover the Intel AMT devices. IMPORTANT: This is a fixed port. During Installation and Upgrade ensure that this port is not blocked.

Item	Ports	Mandatory	Configurable	Firewall Requirement	Additional Details
Firewall Settings: UDP Ports	61491	Yes	No	Open TCP Port	Used for Diagnostics of ZENworks Loader Service. IMPORTANT: This is a fixed port. During Installation and Upgrade ensure that this port is not blocked.
	61492	Yes	No	Open TCP Port	Used for Diagnostics of the ZENworks JoinProxy Service. IMPORTANT: This is a fixed port. During Installation and Upgrade ensure that this port is not blocked.
	61495	Yes	No	Open TCP port	Used for Diagnostics of ZENworks Server Service. IMPORTANT: This is a fixed port. During Installation and Upgrade ensure that this port is not blocked.
	2645	Yes	No	Open TCP port	Default CASA port for authentication
	5502	Yes	Yes	Open TCP port	Used by the zen loader remote event module to notify configuration changes to other loader modules.
	67	Yes	No	Open UDP port	Used by proxy DHCP when it is not running on the same device as the DHCP server.
	69	Yes	No	Open UDP port	Used by the Imaging TFTP, but will not work across the firewall because it opens a random UDP port for each PXE device. The Imaging TFTP is used only with ZENworks Configuration Management.
	997	Yes	No	Open UDP port	Used by the Imaging Server for multicasting. The Imaging Server is used only with ZENworks Configuration Management.
	1761	No	No	Open UDP port	Used to forward subnet-oriented broadcast magic packets for Wake-On-LAN.
	4011	Yes	No	Open UDP port	Used for proxy DHCP when it is running on the same device as the DHCP server. Make sure that the firewall is configured to allow the broadcast traffic to the proxy DHCP service.

Item	Ports	Mandatory	Configurable	Firewall Requirement	Additional Details
	13331	Yes	No	Open UDP port	Used by the zmgpreboot policy, but will not work across firewall because it opens a random UDP port for each PXE device. The zmgpreboot policy is used only with ZENworks Configuration Management.
	6001	Yes	No	NA	Used for certificate activation. There is no firewall requirement for this port.
	31582	No	Yes	NA	Used when the Configure Action (novell-zenworks-configure) is running in the service mode. If this port is in use, a different port can be specified by configuring the <code>service.port</code> in the <code>novell-zenworks-configure-service.properties</code> file. There is no firewall requirement for this port.

Satellite Servers

This sections list the ports used by Satellite Servers:

- ♦ [“Windows Devices” on page 8](#)
- ♦ [“Linux Devices” on page 9](#)
- ♦ [“Macintosh Devices” on page 11](#)

Windows Devices

The following table contains information on the Windows Satellite Server Ports:

Item	Ports	Mandatory	Configurable	Firewall Requirement	Additional Details
Firewall Settings: Open TCP Ports	80	No	Yes	Open TCP Port	Used for content replication. Content is transferred between Satellite Servers and managed devices using this port. Used for content replication. Content is transferred between Satellite Servers and managed devices using this port. Used by the Collection Role to receive file uploads from managed devices. NOTE: Collection Role can be enabled over SSL if required.

Item	Ports	Mandatory	Configurable	Firewall Requirement	Additional Details
Firewall Settings: Open UDP Ports	443	No	Yes	Open TCP Port	Used for content replication. Content is transferred between Primary Servers and Satellite Servers using this port. Used for CASA authentication.
	998	No	No	Open TCP Port	Used by the Preboot Server (novell-pbserv). The Preboot Server (novell-pbserv) is used only with ZENworks Configuration Management.
	7019	No	Yes	Open TCP Port	Used by Join Proxy.
	67	No	No	Open UDP Port	Used by proxy DHCP when it is not running on the same device as the DHCP server.
	69	No	No	Open UDP Port	Used by the Imaging TFTP, but will not work across the firewall because it opens a random UDP port for each PXE device. The Imaging TFTP is used only with ZENworks Configuration Management.
	997	No	No	Open UDP Port	Used by the Imaging Server for multicasting. The Imaging Server is used only with ZENworks Configuration Management.
	4011	No	No	Open UDP Port	Used for proxy DHCP when it is running on the same device as the DHCP server. Ensure that the firewall is configured to allow the broadcast of traffic to the proxy DHCP service.
	1333 1	No	No	Open UDP Port	Used by the zmgpreboot policy, but will not work across the firewall because it opens a random UDP port for each PXE device. The zmgpreboot policy is used only with ZENworks Configuration Management.

Linux Devices

The following table contains information on the Linux Device Ports:

Item	Ports	Mandatory	Configurable	Firewall Requirements	Additional Details
Firewall Settings: Open TCP Ports	80	No	Yes	Open TCP port	Used for content replication. Content is transferred between Satellite Servers and managed devices using this port. Used for content replication. Content is transferred between Satellite Servers and managed devices using this port. Used by the Collection Role to receive file uploads from managed devices. Collection Role can be enabled over SSL if required.
	443	No	Yes	Open TCP port	Used for content replication. Content is transferred between Primary Servers and Satellite Servers using this port. Used for CASA authentication.
	998	No	No	Open TCP port	Used by Preboot Server (novell-pbserv). The Preboot Server (novell-pbserv) is used only with ZENworks Configuration Management.
	7628	Yes	No	Open TCP port	Used by the Adaptive Agent.
	7019	No	Yes	Open TCP port	Used by Join Proxy.
Firewall Settings: Open UDP Ports	67	No	No	Open UDP port	Used by proxy DHCP when it is not running on the same device as the DHCP server.
	69	No	No	Open UDP Port	Used by the Imaging TFTP, but will not work across the firewall because it opens a random UDP port for each PXE device. The Imaging TFTP is used only with ZENworks Configuration Management.
	997	No	No	Open UDP port	Used by the Imaging Server for multicasting. The Imaging Server is used only with ZENworks Configuration Management.
	4011	No	No	Open UDP port	Used for proxy DHCP when it is running on the same device as the DHCP server. Ensure that the firewall is configured to allow the broadcast traffic to the proxy DHCP service.

Item	Ports	Mandatory	Configurable	Firewall Requirements	Additional Details
	13331	No	No	Open UDP Port	Used by the zmgpreboot policy, but will not work across the firewall because it opens a random UDP port for each PXE device. The zmgpreboot policy is used only with ZENworks Configuration Management.

Macintosh Devices

The following table contains information on the Macintosh Device Ports:

Item	Ports	Mandatory	Configurable	Firewall Requirements	Additional Details
Firewall Settings: Open TCP Ports	80	No	Yes	Open TCP port	Used for HTTP non-secure port.
	7628	Yes	No	Open TCP port	Used by the Adaptive Agent.
	443	No	Yes	Open TCP port	Used for content replication. Content is transferred between Primary Servers and Satellite Servers using this port.

Managed Devices

- ♦ [“Windows” on page 11](#)
- ♦ [“Linux” on page 12](#)
- ♦ [“Macintosh” on page 12](#)

Windows

The following table lists the ports used by the Windows managed devices:

Item	Ports	Mandatory	Configurable	Firewall Requirements	Additional Details
Firewall Settings: Open TCP Ports	7628	Yes	No	Open TCP Port	In order to view the status of the ZENworks Adaptive Agent for a managed device in ZENworks Control Center, ZENworks automatically opens port 7628 on the device if you are using the Windows firewall. However, if you are using a different firewall, you must open this port manually. Port 7628 must also be opened on the device if you want to send a Quick Task to the client from ZENworks Control Center.

Item	Ports	Mandatory	Configurable	Firewall Requirements	Additional Details
	5950	No	Yes	Open TCP Port	<p>For Remote Management where the ZENworks Adaptive Agent is running, the device listens on port 5950.</p> <p>You can change the port in ZENworks Control Center (Configuration tab >Management Zone Settings > Device Management > Remote Management).</p> <p>Remote Management is used only with ZENworks Configuration Management.</p>

Linux

The following table lists the ports used by the Linux managed devices:

Item	Ports	Mandatory	Configurable	Firewall Requirements	Additional Details
Firewall Settings: Open TCP Ports	7628	Yes	No	Open TCP Port	You must assign the Network Interface to the firewall zone. Firewall rules are applied to this zone for managing the ports used by ZENworks.
	5950	No	Yes	Open TCP Port	<p>For Remote Management where the ZENworks Adaptive Agent is running, the device listens on port 5950.</p> <p>You can change the port in ZENworks Control Center (Configuration tab >Management Zone Settings > Device Management > Remote Management).</p> <p>Remote Management is used only with ZENworks Configuration Management.</p>
	5951	No	Yes	Open TCP Port	<p>Used by Remote Management for linux remote login.</p> <p>You can change the port in ZENworks Control Center (Configuration tab >Management Zone Settings > Device Management > Remote Management).</p>

Macintosh

The following table lists the ports used by the Macintosh managed devices:

Item	Ports	Mandatory	Configurable	Firewall Requirements	Additional Details
Firewall Settings: Open TCP Ports	7628	Yes	No	Open TCP Port	You must assign the Network Interface to the firewall zone. Firewall rules are applied to this zone for managing the ports used by ZENworks.

ZENworks Agent

The following table lists the ports that need to be configured for ZENworks Agent

Item	Ports	Mandatory	Configurable	Firewall Requirements	Additional Details
Firewall Settings: Open TCP ports	135, 139, 445, 593	Yes	No	Open TCP Ports	Since the Remote WMI connection establishes an RPC connection with the target Windows device, these TCP ports must be allowed by the Windows Firewall of the target device for the WMI discovery technology. Ports 139 and 445 are also required to access the Print Spooler.
Firewall Settings: Open UDP ports	161,162	Yes	No	Open UDP Ports	These are the default ports used by SNMP.
(Optional) Firewall Settings: Open TCP and UDP ports	42, 137	No	No	Open TCP and UDP ports	These are the default WINS replication ports.
(Optional) Firewall Settings: Open TCP ports	515	No	No	Open TCP ports	This is the default port to access the Print Server.

ZENworks Application

The following table lists the ports that need to be configured for ZENworks Application

Item	Ports	Additional Details
Firewall Settings: Open TCP Ports	7268	This is the default port for communication between the ZAPP UI and the ZENWorks agent service.
	7269	This is the default port for websocket communication between the ZENWorks agent service and the ZAPP UI using the WebSocket protocol.

Remote Management

- ♦ [“Windows Devices” on page 14](#)
- ♦ [“Linux Devices” on page 14](#)

Windows Devices

The following table lists the ports that need to be configured for Remote Management Ports of Windows devices:

Item	Ports	Additional Details
Firewall Settings: Open TCP Ports	5950	By default, the Remote Management service runs on this port.
	5550	Remote Management Listener runs on this port.
	5750	By default, the remote management proxy listens on this port.

Linux Devices

The following table lists the ports that need to be configured for Remote Management Ports of Linux devices:

Item	Ports	Additional Details
Firewall Settings: Open TCP Ports	5950	By default, the Remote Management service runs on this port.
	5951	Remote Management service for Remote Login runs on this port.
	5750	By default, the remote management proxy listens on this port.

Remote Management - Using Join Proxy

The following table lists the ports that need to be configured for Remote Management using Join Proxy:

Item	Ports	Additional Details
Firewall Settings: Open TCP Ports	7019	By default, the port on which the Join Proxy listens for a connection.

User Sources

The following table lists the ports that need to be configured to access the User Source.

Item	Ports	Additional Details
Firewall Settings: Open TCP Ports	636	Default SSL port while configuring the User Source.
	389	Default non-SSL port while configuring the User Source.

NOTE: If the LDAP server is listening on a different port, you must ensure that the port is opened for the Primary Servers and Authentication Satellite Servers to talk to the LDAP Server.

Databases

The following table lists the ports that need to be configured for the databases.

Item	Ports	Additional Details
Firewall Settings: Open TCP Ports	1433	Default port for the Microsoft SQL database.
	1521	Default port for the Oracle database.
	54327	Default port for the embedded and PostgreSQL

NOTE: You can change the default port number if there is a conflict. However, you must ensure that the port is opened for the Primary Server to talk to the database.

ZENworks Reporting

The following table lists the ports that need to be configured for ZENworks Reporting:

Item	Ports	Mandatory	Configurable	Firewall Requirements	Additional Details
TCP Ports	443	Yes	No	Open TCP port	Port used by the Primary Server in the Management Zone.
	636	No	Yes	Open TCP port	Default SSL port while configuring the User Source.

Item	Ports	Mandatory	Configurable	Firewall Requirements	Additional Details
	389	No	Yes	Open TCP port	Default non-SSL port while configuring the User Source.
	25	Yes	No	Open TCP port	Default port on which the SMTP server listens during the configuration of the outbound email server settings to send email notifications and reports.
	9080	Yes	No	Open TCP port	Port used to enable the Ganglia monitoring tool to access the server.
	9443	Yes	No	Open TCP port	Port used to administer the appliance and configure ZENworks Reporting.
	9005	Yes	No	NA	Used by Tomcat to listen to shutdown requests. This is a local port, and cannot be accessed remotely.

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.novell.com/company/legal/>.

Copyright © 2008 - 2020 Micro Focus Software Inc. All Rights Reserved.