

## Zoom Phone Local Survivability (ZPLS)

<b>Zoom Phone Local Survivability (ZPLS)</b>	<b>1</b>
<u>New and Changed Information</u>	<u>2</u>
<u>Introduction</u>	<u>3</u>
<u>Design Considerations</u>	<u>4</u>
<u>Deployment Options</u>	<u>4</u>
<u>Signaling and Media</u>	<u>7</u>
<u>Zoom Client</u>	<u>8</u>
<u>Zoom Phone Local Survivability Module (ZPLS)</u>	<u>9</u>
<u>PSTN Integration</u>	<u>10</u>
<u>Session Border Controller (SBC)</u>	<u>11</u>
<u>Route Group for Survivability</u>	<u>13</u>
<u>Call Forwarding Local Survivability</u>	<u>14</u>
<u>Emergency Location Identification Number</u>	<u>17</u>
<u>End User Experience</u>	<u>18</u>
<u>Supported Features</u>	<u>18</u>
<u>Supported Devices</u>	<u>20</u>
<u>Administrator Tasks</u>	<u>22</u>
<u>Licensing</u>	<u>23</u>
<u>Deploy the OVA</u>	<u>23</u>
<u>Zoom Node Installation</u>	<u>25</u>
<u>ZPLS Installation</u>	<u>26</u>
<u>Registering Zoom Node</u>	<u>26</u>
<u>Verifying Agents</u>	<u>29</u>
<u>Adding the ZPLS Service</u>	<u>30</u>
<u>ZPLS Configuration</u>	<u>32</u>
<u>Role-Based Access Control</u>	<u>32</u>
<u>Enabling the Phone Site with ZPLS</u>	<u>33</u>
<u>Enabling Users for ZPLS</u>	<u>35</u>
<u>Session Border Controller (SBC)</u>	<u>35</u>
<u>Route Group Configuration</u>	<u>37</u>
<u>BYOC Numbers</u>	<u>39</u>
<u>ELIN Configuration</u>	<u>40</u>
<u>Call Forwarding Configuration</u>	<u>42</u>
<u>Routing Rules</u>	<u>44</u>
<u>Troubleshooting</u>	<u>45</u>
<u>Testing and Validation</u>	<u>45</u>
<u>Simulating a failover</u>	<u>47</u>
<u>Testing Mode</u>	<u>48</u>

## **New and Changed Information**

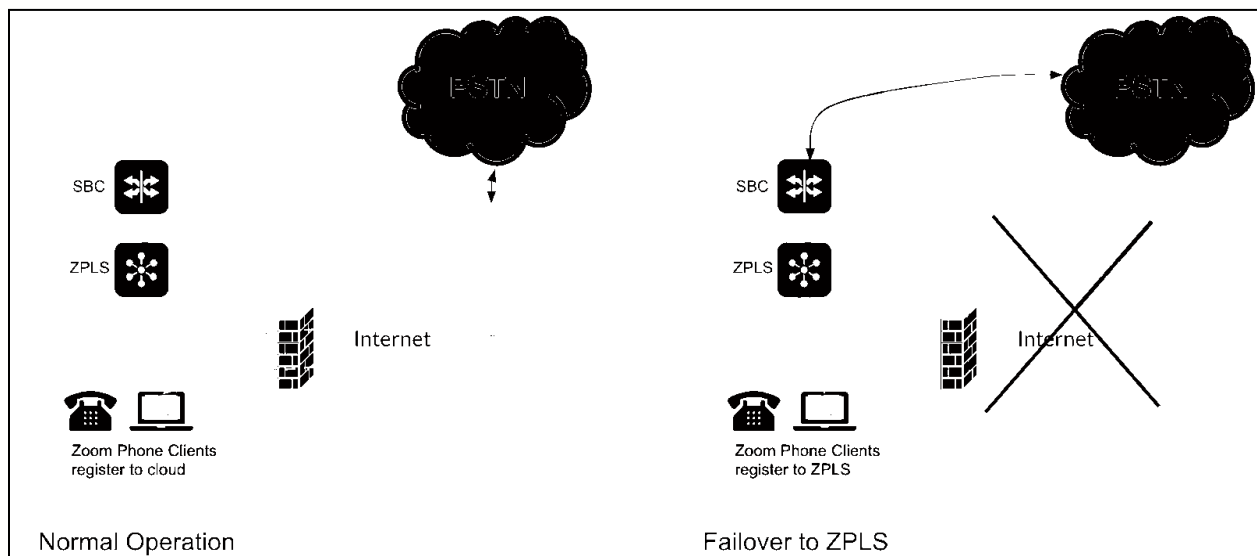
The following table provides an overview of the major changes to the features of Zoom Phone Local Survivability. The table does not provide an exhaustive list of all changes made to the guide.

<b>Feature or Change</b>	<b>Description</b>	<b>Link to view change</b>	<b>Date</b>
Initial Release of document for version 1.12.0.114			1/21/23

## Introduction

Zoom Phone is a cloud-based service that is dependent on IP connectivity to Zoom's datacenters. Customers that are using the Zoom Phone solution at corporate locations are encouraged to deploy redundant and reliable internet connectivity with sufficient bandwidth at each corporate office as a base requirement. Zoom Phone Local Survivability is not intended to be a permanent solution offering feature parity with the cloud service.

For certain business locations, maintaining telephony service in the event of an outage is critical. Zoom can offer a survivability solution of basic telephony services in order to provide an additional layer of protection to ensure business continuity. An outage can be the result of an internet service failure at a business location or a failure in multiple Zoom datacenters that prevent client devices from reaching Zoom Phone components.



The Zoom Phone Local Survivability (ZPLS) module leverages the platform and OS provided by Zoom Node and is distributed as a Linux-based appliance that is deployed on an on-premises VMware ESXi host. The ZPLS module does not affect the phone service during normal operations. Phone clients and devices in survivable Phone Sites register to the corresponding ZPLS module and are able to maintain a subset of Phone features when connectivity to the Zoom Phone cloud is lost. When connectivity to the Zoom Phone cloud returns, clients and devices re-register back to the cloud. During the outage neither the administrator nor end user is required to take any action to enable survivability- the failover and fallback process is seamless and automatic. Maintaining inbound PSTN numbers to Zoom-provided numbers requires an Administrator to enable a toggle from within the Zoom Web Administrator portal.

## Design Considerations

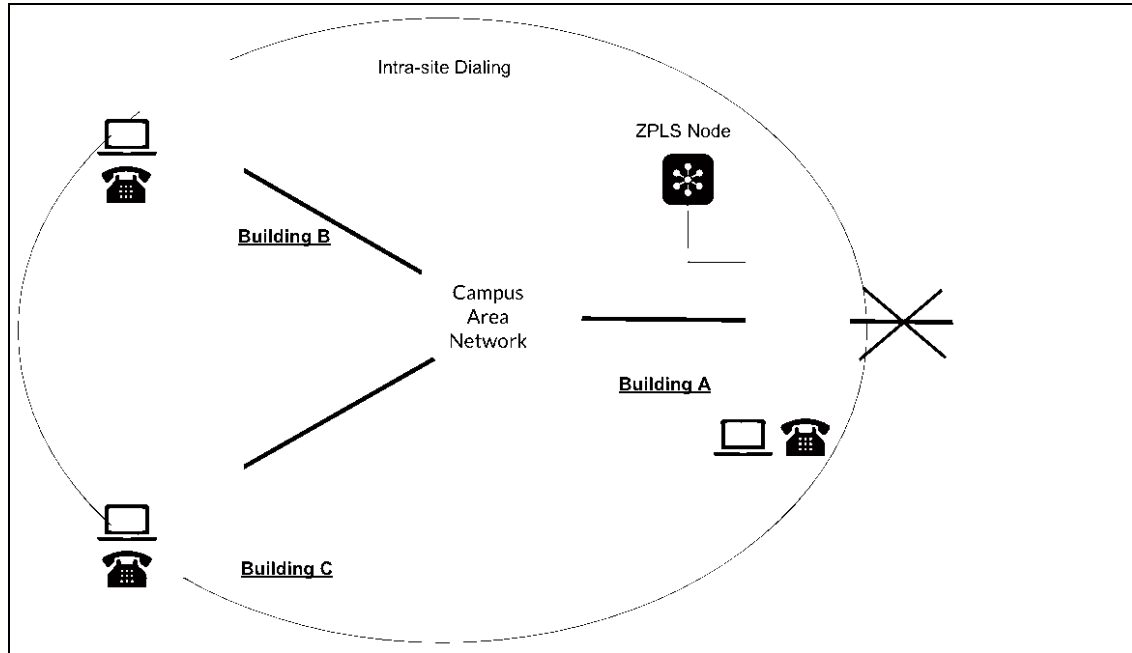
### Deployment Options

The survivability appliance will typically serve as a last choice continuity solution in strategic locations that house a large number of employees in a single location or campus. During normal operations, Zoom Phone clients communicate with Zoom Phone data centers directly bypassing the ZPLS module. The ZPLS module does not act as a SIP Proxy solution or Media Termination Point. During periods of outage when clients are unable to connect to the Zoom Phone data centers, supported clients and devices are able to register to a local ZPLS module in order to maintain internal dialing functionality and basic supplementary services. Optionally, PSTN connectivity can be maintained should an SBC(s) and appropriate Route Groups be provisioned. When normal operations have been restored, clients register back to the cloud and the ZPLS module returns to an idle state.

Critical to the design of when and where to deploy the ZPLS module(s) is the concept of Sites which can be viewed and added from the Admin portal under **Phone System Management > Company Info**. Sites within the Zoom Phone System is a configuration setting that enables customers to organize end users with shared characteristics into a single dialing domain. For example, SIP Registrar/Zone, a common access code, geographical location or default emergency address are possible reasons as to why users, devices and other constructs within the Phone System would belong to the same site.

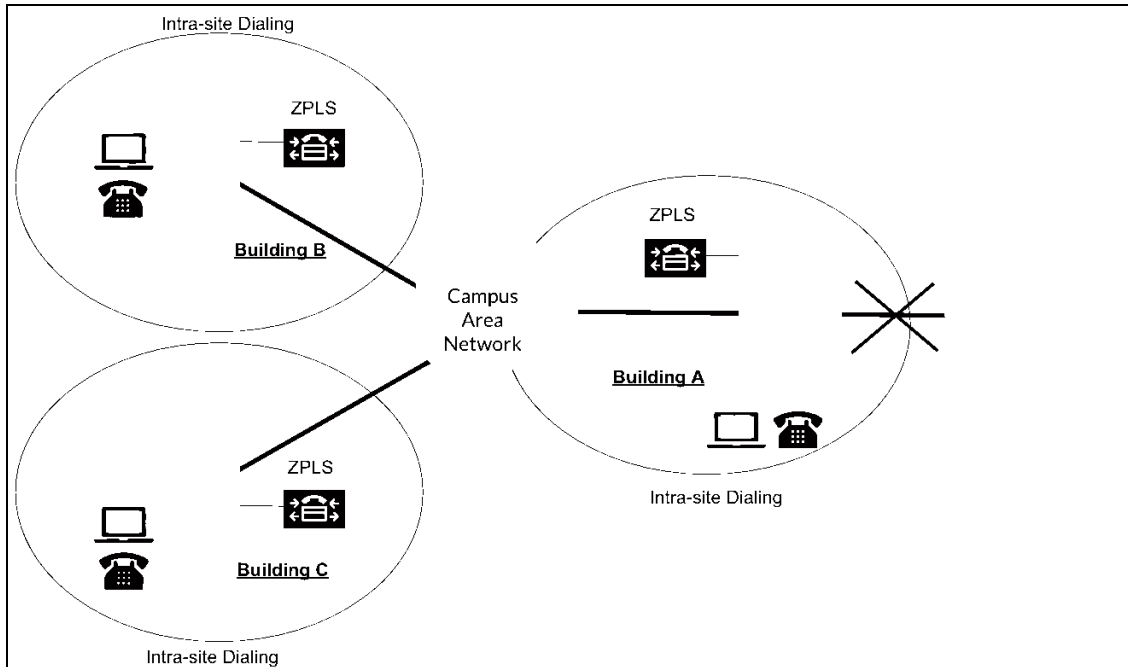
An important consideration before administrators deploy the survivability appliance is that each ZPLS module can only serve a **single** site as defined within Zoom Web portal and each administratively defined site can only leverage a single ZPLS module. In other words there is a 1:1 mapping between Zoom Phone Sites and ZPLS modules and therefore only intra-site calling is possible during while survivability mode is active.

Consider a campus environment at an educational or healthcare facility that contains multiple buildings or locations.



In the example above there are three buildings that comprise the campus. Internet breakout for all locations is centralized (Building A). A single ZPLS module has been deployed and should be located in the Building housing the majority of the users and devices where business continuity is most critical. In the event that the Zoom Cloud is inaccessible, the ZPLS module is able to provide service for all three buildings on the condition that the IP Connectivity within the Campus Network is still functional. Users at the three locations would need to have been provisioned into a single Phone System Site (in this example Site “ABC”) which is assigned to the ZPLS module. Internal dialing within the Site through short extension calling or contact dialing is supported. Optionally inbound and outbound PSTN calling is functional if SBC and Route Groups are enabled.

In the previous example the Campus Network was deemed to have sufficient reliability and resiliency to the point that each location did not warrant a separate (on-site) ZPLS module. Contrast this with a situation whereby the connectivity between locations is less robust.

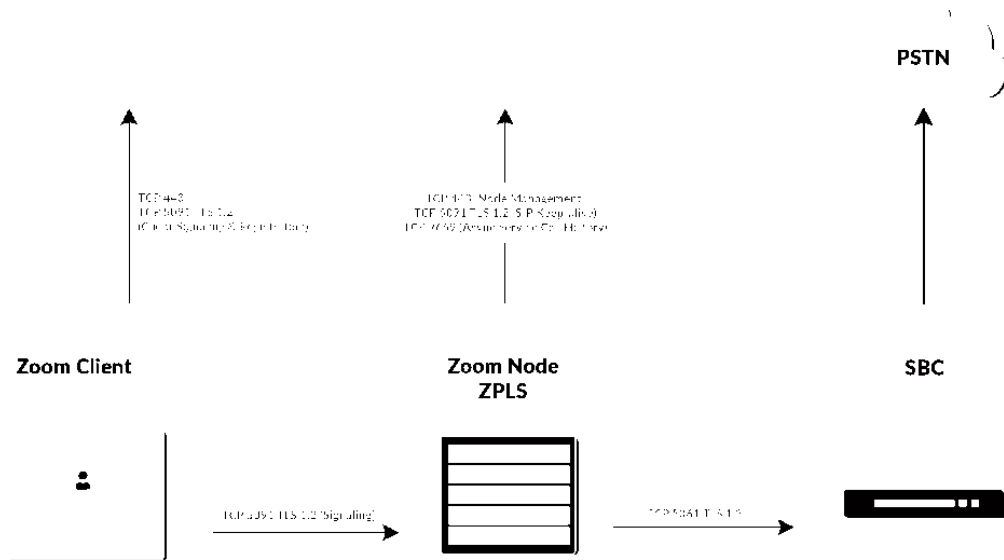


In the above scenario each campus building or location maps to its own Phone System Site that contains local users and devices along with a local ZPLS module. The advantage of this deployment model versus the one discussed earlier is that telephony service can be maintained in the event that the Campus Network suffers an outage. PSTN connectivity could also be maintained by provisioning the Survivability SBC's and PSTN trunks at each of the locations. The limitation of this deployment model is related to the reduced scope of the internal dialing domain since each ZPLS module has no awareness of other ZPLS modules that have been deployed in the network. While internal dialing within each location is supported, internal dialing between locations/buildings is not supported in this example.

Another consideration that affects optimal design is the static nature of the association of Zoom Phone constructs to a site. When users or devices are added to the Phone System, a "home" site is statically configured. Once a specific user roams outside of their home site to another location (e.g. their home office or a different building within the campus), Zoom does not dynamically adjust the site bound to the user. In the above example if a user based at Building A temporarily moves to Building B at the time of an outage, the client would attempt to connect to the ZPLS module provisioned at the configured site (Building A) as opposed to the local module at Building B. In this scenario survivability would still be dependent on the operational status of the Campus Network.

## Signaling and Media

This section details the high level interactions between all the necessary components required for Phone survivability to function.



The table below highlights the TCP and UDP ports utilized by Zoom Phone during normal operations when there is no disruption with connectivity to the cloud .

From	To	Destination Port	Purpose
ZP Client	ZP Cloud	5091 TCP/TLS	SIP Signaling traffic
ZP Client	ZP Cloud	443 TCP/TLS	Web traffic for client configuration settings
ZP Client	ZP Cloud	20000-64000 UDP	Secure RTP media traffic
ZP Client	ZP Cloud	390 TCP/TLS	Company Directory Search from Deskphones
ZPLS	ZP Cloud	5091 TCP/TLS	Connection for SIP Options Ping keepalive
ZPLS	ZP Cloud	443 TCP/TLS	Node / OS Management traffic
ZPLS	ZP Cloud	9669 TCP/TLS	Call History / CDR synchronization
SBC	ZP Cloud	5061 TCP/TLS	SIP Signaling traffic. Unless BYOC is being used this will only be used for SIP Options Keepalive when enabled within the admin portal.
SBC	ZP Cloud	20000-64000 UDP	Secure RTP media traffic when BYOC is being used for PSTN connectivity.

## ZOOM Phone

The table below highlights the TCP and UDP ports utilized by Zoom Phone when failover to ZPLS is active due to disruption with connectivity to the cloud .

<b>From</b>	<b>To</b>	<b>Destination Port</b>	<b>Purpose</b>
ZP Client	ZPLS	5091 TCP/TLS	SIP Signaling traffic
ZP Client	ZPLS	20000-64000 UDP	Secure RTP media traffic
ZPLS	SBC	5061 TCP/TLS	SIP Signaling traffic- can be modified in portal
ZPLS	SBC	20000-64000 UDP	Secure RTP media traffic

For further information related to the network and firewall settings see this support article:

<https://support.zoom.us/hc/en-us/articles/201362683-Zoom-network-firewall-or-proxy-server-settings>

### Zoom Client

In order for Zoom Clients to discover the ZPLS IPv4 address to use for registration in the event of an outage, the ZPLS must be bound to the Phone System Site and the User must be enabled for Phone Survivability. The Policy to determine which users are enabled for survivability is determined from the combination of Account, Group, Site and User Policy. This is especially useful if a Phone System Site contains more than 5000 users and devices (5000 being the maximum number of registered clients ZPLS can handle). Admins are able to selectively prioritize the clients that will survive during an outage as per the business needs.

Supported Clients and Devices maintain a keepalive mechanism (based on SIP REGISTER messages) to the Zoom Phone cloud. In the event of an outage the client continues to send keepalive messages in order to detect the return of the cloud service and initiate resumption of normal operations. Clients discover the appropriate failover ZPLS module from the Zoom Phone platform during the bootup process since the ZPLS Module is added as the tertiary SIP Registrar. The client will not be required to resolve the FQDN of the ZPLS Module since the ZPLS IPv4 address is discovered. When clients are offline and unable to connect to Zoom, the approximate time for failover to the ZPLS module is 3 minutes. When normal operations resume, the approximate time for fallback is 5 minutes.



## Zoom Phone Local Survivability Module (ZPLS)

Zoom recommends deploying the appliance on an internal LAN with a static IPv4 consistent with the customer's network designs. This appliance needs to be accessible to the Zoom Phone devices and desktop clients. In some circumstances the enterprise DMZ network can be used but network administrators will need to ensure communication through the enterprise firewall.

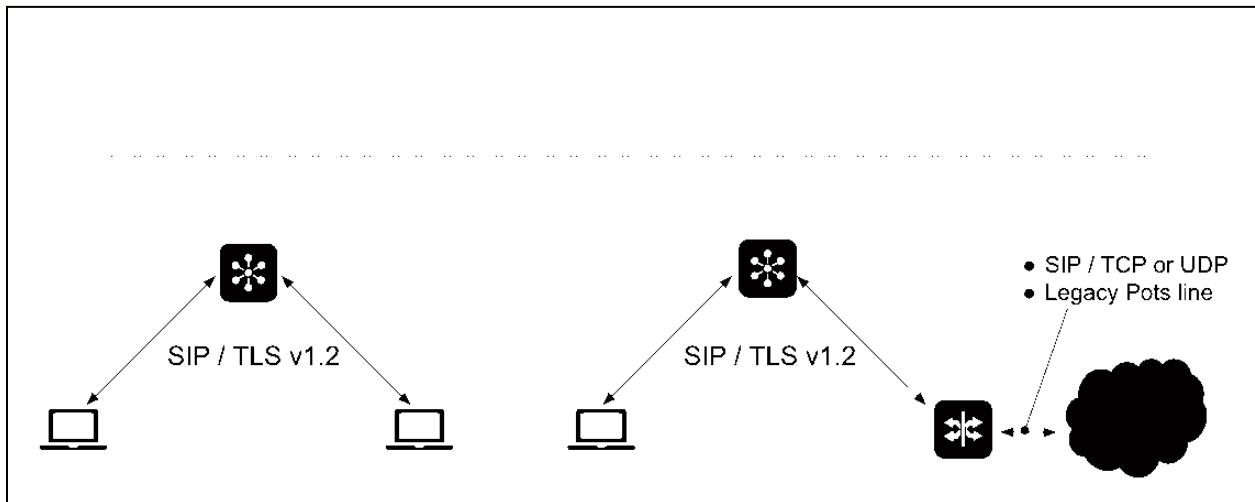
The ZPLS module must be configured when the Zoom Cloud is available and not during an outage. In order to synchronize user and device configuration, the module first needs to establish an https session with the Cloud. Zoom Node includes end-to-end Auto-PKI through DigitCert thus removing the burden of certificate generation and renewal from the customer. Administrators are required to adjust corporate firewall policy in order to enable ZPLS outbound initiated, stateful communication to the appropriate Zoom networks. The module imports relevant configuration required to successfully authenticate any user or device belonging to the site that has been enabled for survivability. This includes the security token required for authentication of users and devices within the site. The ZPLS module is assigned to a Phone System Site. Subsequent configuration changes within a site (e.g. new users or devices created or existing users or devices modified) are propagated to the ZPLS module every 10 hours.

The ZPLS module maintains a keepalive to the Zoom Cloud using the Options Keepalive mechanism. In the event that client devices within a site provisioned for survivability lose connectivity, supported clients and devices will register to the ZPLS module using SIP over TLS v1.2 providing that *both* the client devices *and* ZPLS module have detected the failure. The clients use SIP Digest Authentication in order to register to the ZPLS Module. Internal calling between extensions that have registered to the ZPLS module are subsequently supported. Secure RTP (SRTP) media sessions can be established however it must be noted that the media flows through the module and is not point to point (E2E).

## PSTN Integration

For Inbound and Outbound PSTN Connectivity customers will need to provide a Session Border Controller (SBC) that maintains operational PSTN Connectivity either through a legacy TDM/analog connection or SIP Trunk leveraging a cellular or alternate connection (e.g. DSL, carrier-provided circuit). It is possible that any SIP Trunks deployed at the SBC are dependent on the same internet service that is undergoing an outage that has caused the ZPLS module to enter survivability mode. In this situation customers should consider a tertiary connection that is dedicated for inbound/outbound PSTN calls

The figure below depicts the signaling and media path for active internal and external calls. Media offload is not supported in any scenario. Media packets are anchored or hair-pinned through the ZPLS module. Transcoding or transrating of audio codecs is not supported and all parties involved in an active call are required to support the same codec and sampling rate. Supported codecs are Opus, G711ulaw, G711alaw and G729.



TLSv1.2 must always be supported on any SBC being used for Survivability.

Upon restoration of cloud services, the ZPLS module will upload CDR records for any calls that were made during the offline period. These logs will be marked as calls that were completed while survivability mode was active.

## Session Border Controller (SBC)

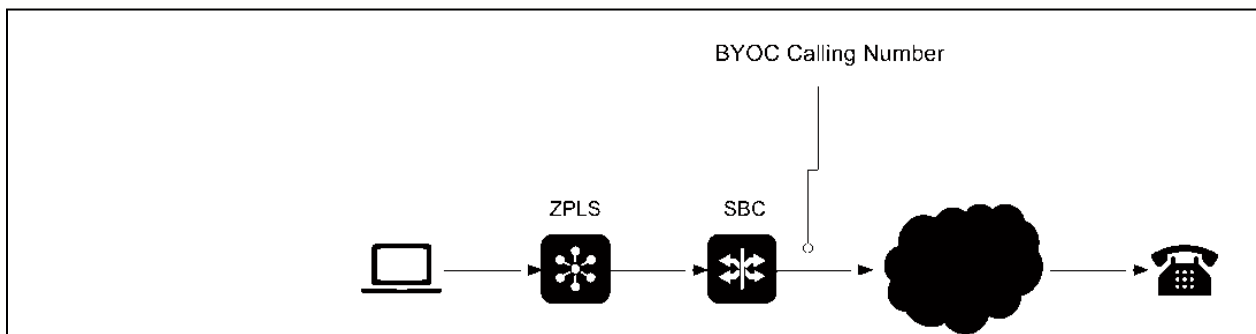
Any Session Border Controller (SBC) that is certified by Zoom for Bring Your Own Carrier (BYOC) connectivity can also be used for Zoom Phone Local Survivability. If BYOC is being used for PSTN connectivity, there is no need to deploy a separate SBC for the purposes of survivability.

Zoom recommends assigning a static IPv4 private IP address to the SBC. The SBC communicates to the ZPLS module on TLS port 5061 for secure SIP and UDP port range 20000-64000 for secure media.

Whenever possible ZPLS will attempt to route calls originating from registered Zoom clients locally. Calls are only forwarded by ZPLS to the SBC if the destination contained within the Request URI field of the incoming SIP Invite does not match a registered extension. A registered extension is the short extension without site code, the long extension with site code, the assigned Zoom Native Number and the assigned BYOC number. If the incoming SIP invite does not match any locally registered extension on ZPLS, the SIP Invite is forwarded to the SBC.

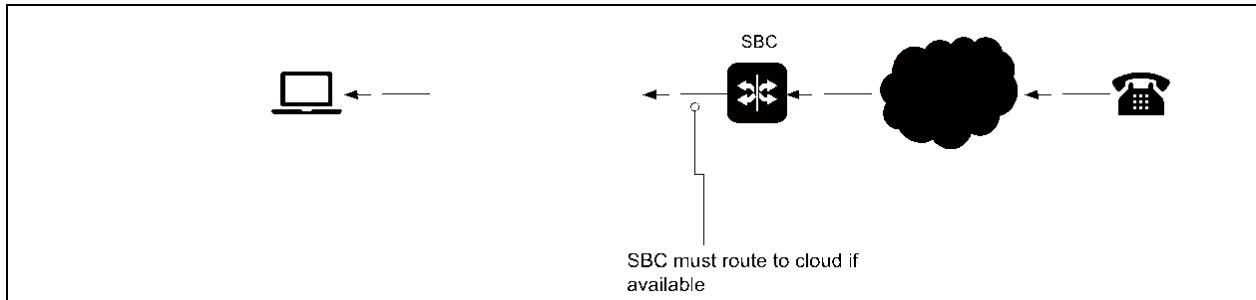
In order for ZPLS to discover the IP address of the SBC used for survivability, a Route Group that is designated for survivability should be assigned to the Phone System Site at the time as the ZPLS module assignment to Site. The SBC contained with the survivability Route Group is leveraged by the ZPLS module for off-net calls.

During an outage, outbound calls from ZPLS-registered devices will contain the BYOC Calling Number.



It is possible PSTN destinations place calls back to the Zoom client using the BYOC number (for example from Recent Call History) instead of the primary Zoom-provided PSTN number. If the resolution of the issue causing the outage is complete and the client has registered back to the cloud, the SBC should not forward the call onto the ZPLS module but instead pass the call onto the cloud.

## ZOOM Phone



For this reason the SBC must be able to establish TLS and UDP connectivity back to the Zoom Phone cloud (in addition to the ZPLS module). When adding the SBC into the Zoom portal, both the private IP address the ZPLS will use to communicate with the SBC in addition to a Public IPv4 address can be defined. Customers should ensure the SBC is either provisioned with a dual-NIC SBC and configured with a private and public IPv4 address, or ensure that static 1:1 NAT rules are in place on the edge firewall in addition to opening up of the required ports.

In summary, the SBC used for survivability must establish a TLS connection to the Zoom Cloud *and* the ZPLS Module. Options Keepalive should be enabled when adding the SBC - admins will see multiple sets of Options keepalive (between the SBC and ZPLS module and between the SBC and each Zoom Phone Datacenter).

In order to establish TLS connectivity to both ZPLS and Zoom cloud, the DigitCert root and intermediate certificates should be installed on the SBC. ZPLS uses DigitCert-signed auto-generated certificates so the same set of root/intermediate certificates used for BYOC will suffice for ZPLS.

Zoom recommends admins configure the SBC to route incoming calls from the PSTN SIP Trunk to the Zoom Phone data centers as the first and second choice with the ZPLS acting as the tertiary path. Calls from ZPLS into the SBC should be routed to the PSTN SIP Trunk.

## Route Group for Survivability

A Route Group is a Zoom Phone construct that contains a source Zoom data center and one or more premise-based SBC IPv4 addresses. Zoom is able to establish a secure SIP Trunk between the source data center and SBC(s) once the provisioning has completed and a TLS connection is established. For additional resiliency a backup Route Group can be provisioned—typically this contains the same list of premise-based SBCs but from a different Zoom data center.

Prior to adding the Route Groups for survivability, Admins should ensure all SBCs have been defined within the Zoom Admin portal. Admin will then be required to add a minimum of two Route Groups for the purposes of survivability:

- The first Route Group will be set to type “*Survivability*”. The IPv4 address contained in the “Survivability Public/Private IP” section of the SBC configuration will be used for this survivability Route Group. This IPv4 address will be learnt by the ZPLS module once this Route Group is assigned to the appropriate Phone System Site. The assignment of the survivability Route Group to the Phone System Site must be completed at the same time as the ZPLS module. If the Options Ping mechanism is enabled on the Route Group, ZPLS will begin sending the Options Method to the SBC’s survivability IP address.

**Note:** the survivability Route Group has no option for source Zoom data center or Region and no option for backup Route Group. The ZPLS module is the sole entity that communicates with the SBC IPv4 address contained within this Route Group and at this time there is no option to add multiple SBCs.

- The second Route Group required is of type BYOC-P (Bring Your Own Carrier Premise) and is required by Zoom in order to handle inbound and outbound calls from/to BYOC numbers when survivability is no longer active (normal operations). The “Public IP Address” section of the SBC is used for this Route Group. When Options Ping is enabled, the Zoom Phone data centers within the configured SIP Zones will initiate the Options keepalive mechanism.

All Route Groups, Trunks and SBCs that are leveraged by ZPLS must be configured within the Zoom Web Admin portal prior to any failover occurring.

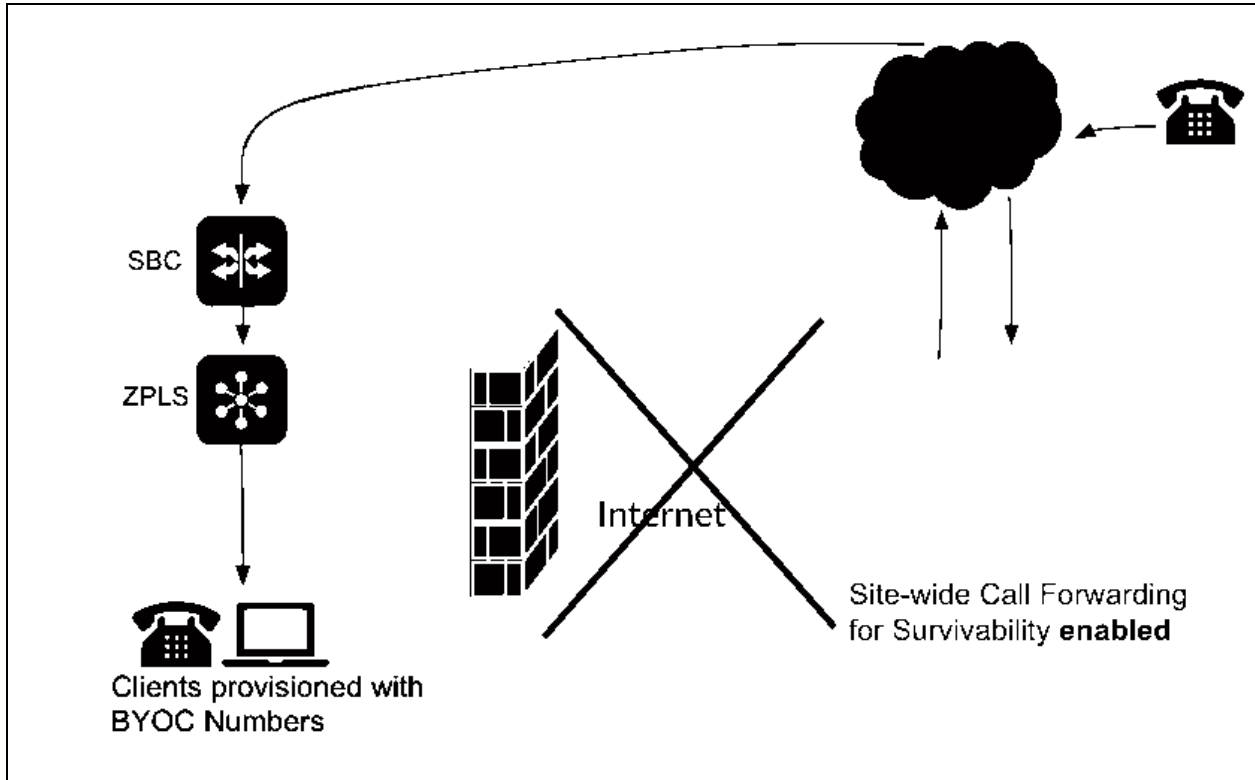
### Call Forwarding Local Survivability

This section applies to customers leveraging the Zoom Native PSTN solution for PSTN connectivity. Currently PSTN numbers obtained through Cloud Peering (BYOC-Cloud) cannot be rerouted during an outage. Customers using a premise-based BYOC solution are not required to forward numbers- failover in this instance can be achieved by adding a tertiary route to the ZPLS module on the premise-based SBC.

Zoom-provided PSTN numbers continue to be routed into the Zoom Cloud in the event of an outage. Zoom will attempt to route an incoming call to a registered client or device depending on the configured Call Handling rules within User Settings. If the Called Party is located within a customer premises that is undergoing an outage, the Zoom desktop client and any hardware phones or appliances will be unavailable from the perspective of the Zoom Cloud.

For Sites that have been enabled for survivability, Administrators are able to invoke Call Forwarding in order to re-route Zoom-provided PSTN numbers to BYOC numbers that are bound to the PSTN trunk attached to the survivability SBC. If Call Forwarding for survivability is enabled, Zoom will reroute incoming PSTN calls back out to the PSTN towards the survivability SBC and eventually the ZPLS module and registered client. The Administrator can provision the call forwarding logic ahead of time and manually enable it during an outage. This allows customers the flexibility to purchase numbers directly from Zoom while still being able to answer calls directly at a site that has lost connectivity to the cloud.

An overview of the Call Forwarding solution is detailed below.



- (1) A PSTN caller initiates a call to a Zoom-provided number.
- (2) The call arrives into the Zoom Phone cloud- Call Forwarding for Survivability has been enabled by the Administrator since the destination site is undergoing an outage. This forwarding logic is defined by the administrator prior to any outage occurring. In essence the forwarding logic consists of rules whereby Zoom Native numbers are forwarded to BYOC numbers that are associated with the SIP Trunk defined in step (4) below. Call forwarding can be invoked in bulk or on a per-extension basis.

**Note:** If Call Forwarding for Survivability is not enabled, the action defined under the Overflow for that particular extension is invoked.

- (3) Since Call Forwarding logic has been invoked, Zoom does not attempt to route the call to any registered client- instead the call is rerouted to the PSTN with the destination or Called Party Number set to the BYOC number.
- (4) The SIP Trunk that connects the Survivability SBC to the PSTN must be functional during any outage otherwise the call to the BYOC number will fail.
- (5) The survivability SBC must be reachable to/from the ZPLS module during the outage. and must be defined and added into a survivability Route Group prior to any outage occurring. The survivability Route Group is assigned to the Phone System Site within the web portal. The SBC must be configured to route known BYOC numbers to the ZPLS module and external calls made from ZPLS should be routed to the PSTN provider.
- (6) Clients that failover and register to the ZPLS module should be assigned a BYOC number if there is a requirement to receive external calls. Clients that are not provisioned with a BYOC number will be unable to receive PSTN calls but may still register to the ZPLS module with an internal extension. The Local Survivability Mode policy toggle of the User / Common Area must be enabled in order for clients to register to the ZPLS module.

At this time the following limitations apply:

- Zoom-provided (Native) numbers assigned to Users, Common Areas, Auto Receptions (AR), Shared Line Groups (SLG) and Call Queues (CQ) can be forwarded to BYOC numbers provisioned on customer-managed survivability trunks. For the purposes of this document the nomenclature of the number being forwarded is referred to as the **Source Number**.
- At least one BYOC number must be added and assigned to a Zoom Phone user within the survivability site. During normal operations the user will be assigned at least three numbers: (a) the internal extension with site code prepended, (b) the Zoom Native PSTN number and (c) the BYOC PSTN number. For the purposes of this document the nomenclature of the target number used for the call forward is referred to as the **Destination Number**.
- Logic to forward Source numbers to Destination numbers is provisioned by Administrators from within the portal. A source number can only be forwarded to a single destination number. Multiple source numbers can be forwarded to the same destination number.
- The forwarding should be left in the disabled state until such a time when an outage has occurred- at this time Administrators will be required to access the portal to enable the



forwarding logic. Administrators can enable call forwarding rules for the entire site or for individual source numbers.

- Forwarding for survivability applies only to incoming PSTN calls and not for calls originated by other Zoom extensions that are registered to the cloud. Calls originating from internal Zoom-registered extensions will be subject to the treatment defined by the “*When a call is not answered*” section of the Call Handling rules within the destination User Settings.
- When forwarding for survivability is enabled, Zoom will not attempt to route the call to a cloud-registered endpoint. For example, if the user successfully registers the mobile client to the Zoom cloud when call forwarding for survivability is enabled, incoming PSTN calls will not alert the mobile client since the forwarding logic takes precedence.
- If call forwarding for survivability is disabled, incoming PSTN calls will be treated according to the Call Handling logic for each individual user. If no phone client is registered to the cloud, callers will be subject to the treatment defined by the “*When a call is not answered*” section of the Call Handling rules within User Settings.

### Emergency Location Identification Number

Administrators are able to designate a single Emergency Location Identification Number (ELIN) to a Phone System Site for situations when emergency services numbers have been called by ZPLS-registered extensions during an outage. This ELIN must be a BYOC-P number that is terminated on a PSTN trunk that is located at the failover SBC/gateway. When the user makes an emergency call during Survivability mode, the user’s direct number, if one is available, will be replaced with the ELIN that is designated at the site level. This allows users who do not have a direct number to call emergency services and be reachable for callback from the emergency operator. When the Public Service Answering Point (PSAP) calls the ELIN, the system is designed to route this call back to the original user who made the emergency call. The system continues to route callbacks to the ELIN for up to 2 hours. Once the administrator has assigned a BYOC number as the designated ELIN for a particular site, the BYOC number cannot be assigned to any user or other Zoom Phone entity.

Zoom does not take responsibility for updating BYOC carriers of physical addresses that correlate to each ELIN- customers should ensure emergency addresses are correctly mapped to the appropriate physical address.

## End User Experience

### Supported Features

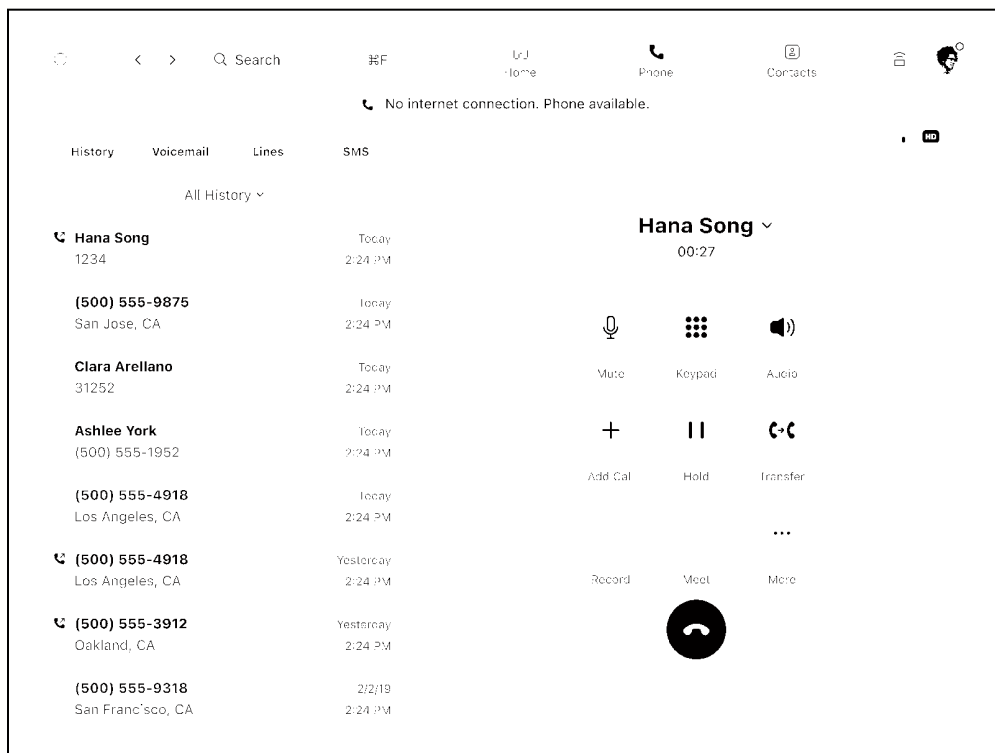
End user functionality during periods of cloud service disruption will always be limited when compared to the feature set offered under normal operations- the majority of the features Zoom Phone customers enjoy are dependent on the components deployed in the cloud. With that in mind, the table below details the supported functionality during periods of outage when clients are offline.

<b>Functionality in Survivability Failover Mode</b>	
<b>Supported</b>	<b>Not Supported</b>
Internal Extension Dialing	Add/Remove Contact
Dial By Name	Inter-ZPLS Module calling
Contact Search/Calling (the client learns the first 25000 contacts)	URI dialing
Dial From Call History (Call History in failover is uploaded to Zoom when service resumes)	Voicemail
Inbound / Outbound PSTN (assumes SBC and survivable PSTN connectivity)	Speed Dial
Hold/Resume	Call Forwarding
Mute/Unmute	Call Handling rules based on business/closed/holiday hours
DTMF (RFC 2833)	Escalate to multiparty conference (more than 3 participants)
Consult Transfer	Escalate to Meeting
Blind Transfer	Call Queue
Call Park	Auto Receptionist
Adhoc 3-party Conference	Delegation/Shared Line Appearance
	Shared Line Group
	Monitoring (Barge/Monitor/Whisper)
	Pickup
	Intercom
	Nomadic e911 calling

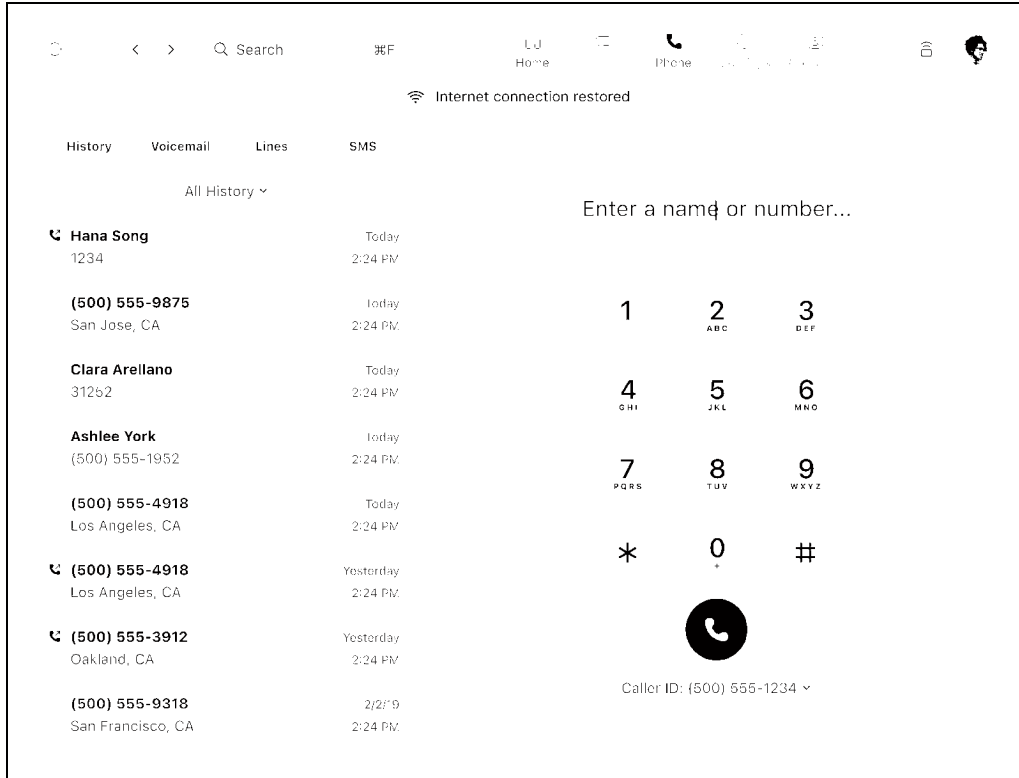
	Switch to Carrier
	End to end encrypted calling

Zoom does not support checkpointing of active calls when access to the cloud is lost. Users involved in an active call will hear a Fast Busy tone at the time when the client can no longer reach the Zoom Phone cloud and will need to wait for the failover process to the ZPLS Module to complete before manually re-establishing the call.

The process of failover and fallback is transparent to the End User. They are not required to close and relaunch the client or reboot hardware devices and there is no trigger required to initiate the failover. Users will see the following banner indicating that they are operating in failover mode.



The screenshot below shows the Zoom Client once it has reconnected to the Zoom cloud.



## Supported Devices

The Zoom Windows Desktop Client is supported from version 5.10.7.

The Zoom Mac OS Desktop Client is supported from version 5.11.

The Zoom Mobile Client is not supported.

The list of supported hardware devices is as follows:

- Poly UCS 6.4.2.3336 or later version,
- Poly CCX series + 7.1.1
- Poly Trio series + 7.0.1
- AudioCodes MP-1288 + Firmware Version 7.20A.258.663
- AudioCodes MP-112/114/118 + Firmware Version 6.60A.364
- AudioCodes MP-124 + Firmware Version 6.60A.364
- Yealink SIP series
  - CP920
  - CP925
  - T21P, T23G, T27G, T29G
  - T31G, T31P, T33G
  - T40G, T41P, T42G, T46G, T48G

## ZOOM Phone

- T42S, T46S, T48S
- T43U, T46U, T48U
- T53W, T54W, T57W, T53
- Yealink Android series
  - CP960
  - CP965
  - T56A, T58A
  - T58W
  - VP59
- Yealink DECT series
  - W56P
  - W60P
  - W70B
  - W80DM
  - W90DM

## Administrator Tasks

Zoom supports installation of the ZPLS module as a Virtual Machine running on a supported release of the VMWare ESXi hypervisor. Zoom distributes to licensed customers a prepackaged OVA file for installation. During the creation of the virtual machine, customers are able to customize the hardware specification for the Virtual Machine using one of two supported reference configurations as shown below.

	Configuration Option 1	Configuration Option 2
Hardware Specs	8 CPU 16 Gb RAM 80 Gb HDD	16 CPU 16 Gb RAM 80 Gb HDD
Total number of registrations	2000	5000
Total number of concurrent calls	240 calls	480 calls
Calls per second (CPS)	2	4
Registrations per second (RPS)	45	90

Similar to the End User experience, it is not necessary for the administrator to perform any action to initiate failover or fallback.

**Note:** When the number of endpoints within a site enabled for survivability exceeds 5000, ZPLS will process the first 5000 registrations on a first come first served basis. Customers are advised to use the Zoom Phone Policy setting “**Local Survivability Mode**” in order to prioritize which users support survivability failover. This policy can be defined at the Account, Site, Group or User level.

## Licensing

There are two licenses that must be installed prior to configuring ZPLS:

- Zoom Node License
- Zoom Phone Hybrid License

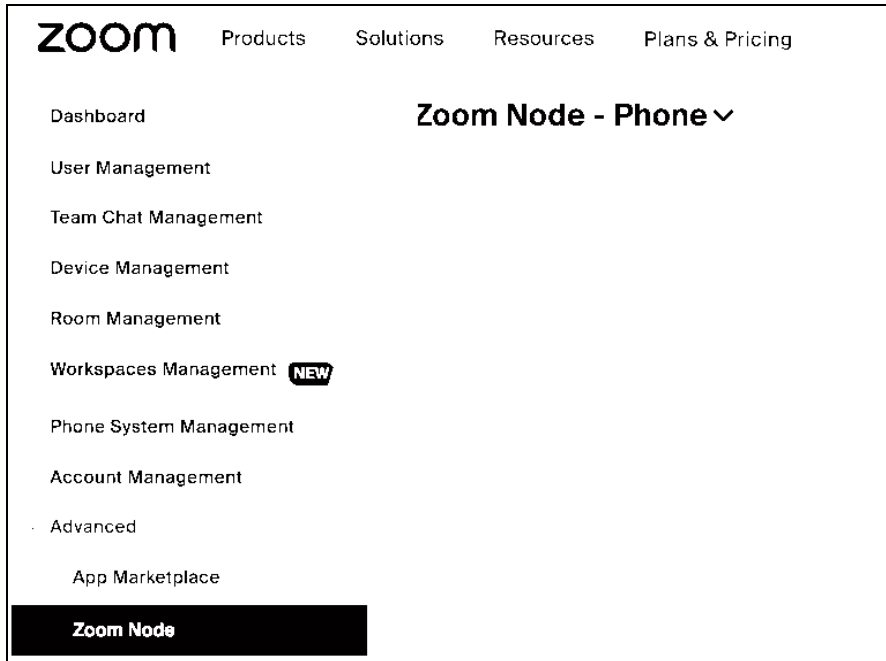
Administrators are able to verify that the correct licenses have been provisioned by accessing the Zoom Administrator Web Portal and navigating to **Account Management > Billing** and verifying active licenses are in place as shown in the screenshot below.

The screenshot displays two active licenses in the Zoom Administrator Web Portal. The first license is for Zoom Node, and the second is for Zoom Phone Hybrid. Both are active and associated with a Zoom account.

License Name	City	Subscription Period	Service Effective Date	Status	Billing Account	Next Invoice Date	Next Invoice Amount
Zoom Node	100	Monthly	Dec 1, 2021	Active	Zoom	Dec 31, 2030	\$0.00
Zoom Phone Hybrid	100	--	Mar 23, 2022	Active	Zoom	Expires on Dec 31, 2030	\$0.00

## Deploy the OVA

Administrators are able to download the Open Virtual Appliance (OVA) file from the Zoom Administrator Web Portal by navigating to **Advanced > Zoom Node** and ensuring that **Zoom Node- Phone** is selected in the pulldown menu in the upper left hand corner of the portal as shown in the screenshot below.



Administrators should then select the **Node** tab followed by clicking **Add Nodes**. A popup window will appear with the option to download the latest version of the OVA file. The size of the OVA is between 4-5 GB.

**Note:** If the Zoom Node option is not visible in the portal then it is likely that the logged in user does not have privileges to view this option. An account owner or admin can add the required roles to users by navigating to **User Management > Roles > <RoleName>** and scrolling down to the **Zoom Node** section and selecting **Zoom Phone Local Survivability > View/Edit** options.

Once the download of the OVA template is complete, the Virtual Machine can be deployed by following the steps detailed below. VMWare ESXi 7.x hypervisor was used for the purposes of this document, steps may differ between versions of vSphere or hypervisor.

1. Navigate to your ESXi host address
2. Select **Host -> Virtual Machines**
3. Right click on Virtual machines and select **Create/Register VM**
4. Select the option **Deploy a virtual machine from OVF or OVA file**
5. Enter a name for the virtual machine and browse the local computer for the .ova file that was downloaded.
6. Select the default network mappings unless the deployment environment has other requirements. Click **Next**.



**Note:** For production deployments only 'Thick' provisioning is supported. There are no hard requirements for IOPS at this stage.

7. Review the information and click **Finish**. Once the deployment is completed successfully, power on the virtual machine and open the console of this virtual machine.

### Zoom Node Installation

The following steps are required to install Zoom Node which ZPLS leverages for cloud connectivity and management.

1. Navigate to the console of the virtual machine that was deployed in the previous step.
2. The Zoom Node virtual machine will boot up and when completed, a screen will be shown to set up the default password. The default admin user is "**zoom-setup**". This username/password will be used for the virtual machine setup from the console.
3. When prompted, enter a default password for the **zoom-setup** user.

```
Please reset the initial password of user [zoom-setup].
```

```
Password rule:
```

```
Must be at least 8 digits of characters long
```

```
Must contain at least one number, one symbol,
```

```
one upper-case character and one lower-case character
```

```
New password:
```

4. You will then be prompted to configure the hostname of the Virtual Machine. There is no requirement for reverse DNS PTR record lookup.

```
Current Hostname: [localhost.localdomain]
Do you want to change the hostname right now? [yes]:
Please input the new hostname:
```

5. If DHCP is not available, there will be a prompt to set an IP address, Default Gateway and DNS server.

**Note:** SSH is not enabled on Zoom Node OS. Direct access is available through the virtual console only.

## ZPLS Installation

Once the IP address, hostname and default password are set, the module can be associated with the correct Zoom account by generating an activation code in the cloud and entering this code on the console of the Node.

## Registering Zoom Node

The Server should be added within the Zoom Administrator Web Portal by navigating to **Advanced > Zoom Node** and selecting the **Nodes** tab.

**Zoom Node - Phone** Services **Nodes** Agents Dashboard Alerts

Confirmed Nodes **Unconfirmed Nodes** Groups

A Zoom Node OS update is available and will be installed within 7 days. Update Postpone

Search Node

Name	IP Address	MAC Address	Services	Creation Time	Zoom No
------	------------	-------------	----------	---------------	---------

The Admin should then select **Add Nodes**.

Services **Nodes** Agents Dashboard Alerting Logs Settings Documentation


nstalled within 7 days. Update Postpone

**Add Nodes**

Select **Generate code**. Copy this code and save it to be used in the next step. Ensure the code is used prior to the defined expiration period, otherwise a new code will need to be generated.

## Add Nodes

- Download the image below.



**ZoomNodeOS.ova** 4.7G

version 1.0.1 (20221123071515) file based on July 26, 2022

↓ Download

3-A2e5-10f3lx-re1-hewlettdeloid-0000300-a380-c7ee81-020037004c-07000098000e

- After configuring the IP address, generate and copy the code to install the Node Agent.

Code Expiration:

15

↑ ↓

minutes

[Generate Code](#)

- After installation completed and confirm the node, you will see the agent status on Agent tab page. You can continue to install services on Services page.

[Close](#)

Navigate to the virtual machine console, and select option 3 - **Register Zoom node**. Input the code that was copied from the Zoom admin portal in the previous step and enter it here:

```

Let's get started configuring your server for Zoom Node.

1. Please login to the Zoom configuration portal at https://zoom.us.
2. Select Advanced->Zoom Node and add a server.
3. Copy and paste your code into the prompt below.(Esc and Enter to back out)

Registration Code [nws.zoom.us]:
    
```

**Note:** This will install required components. Once the components have been downloaded and installed, navigate to the administration portal to check the status.

After approximately 5 minutes following entering the activation code within the CLI of the Node, the admin will be required to navigate to **Advanced > Zoom Node > Zoom Node - Phone > Nodes > Unconfirmed Nodes** from within the Zoom Administrator Web Portal. Ensure that the node hostname defined on the CLI matches what is listed on the web portal.

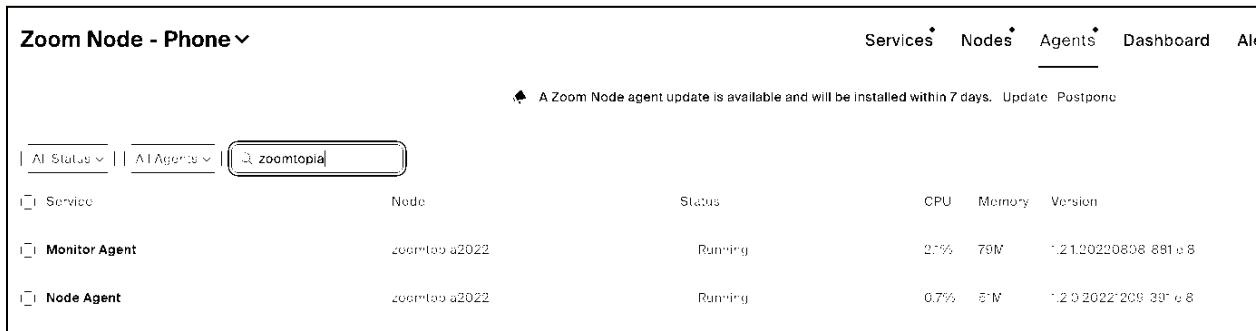


Name	IP Address	MAC Address	Start/End Time	
zoomtopia	10.0.240.101	8c:8e:9d:00:00:00	2/15/2022	Confirm Remove

Click **Confirm** to move this server into the **Confirmed Servers** tab.

## Verifying Agents

Navigate to the **Agents** tab to ensure that the **Node Agent** and **Monitor Agent** are running before proceeding. It may take a few minutes for both to become available.

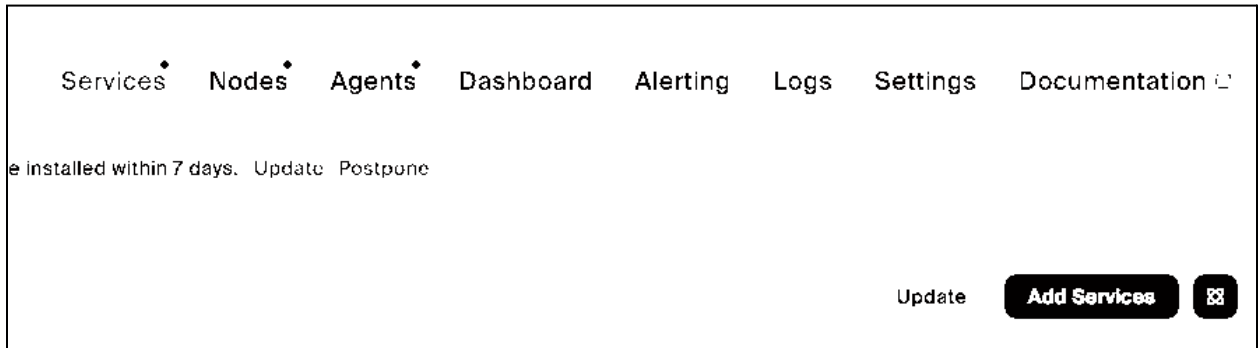


A Zoom Node agent update is available and will be installed within 7 days. Update Postpone

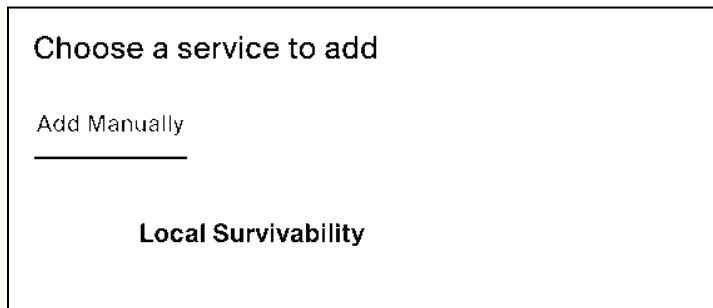
Service	Node	Status	CPU	Memory	Version
Monitor Agent	zoomtopia2022	Running	2.1%	79M	1.2.1.20220808-881-e8
Node Agent	zoomtopia2022	Running	0.7%	81M	1.2.0.20221208-391-e8

## Adding the ZPLS Service

From the Zoom Administrator Web Portal the administrator should navigate to **Advanced > Zoom Node > Zoom Node - Phone -> Services** and Select **Add Services** on the top right hand corner of the screen.



Select **Local Survivability** as the component.



Select the server where the Local Survivability Module needs to be installed and IPv4 address. The remaining fields can be set as default unless the customer is wishing to use their own CA-signed certificates and not the Auto-PKI mechanism that Zoom provides natively.

### Add Local Survivability

Install on a node \*

Internal IP \*

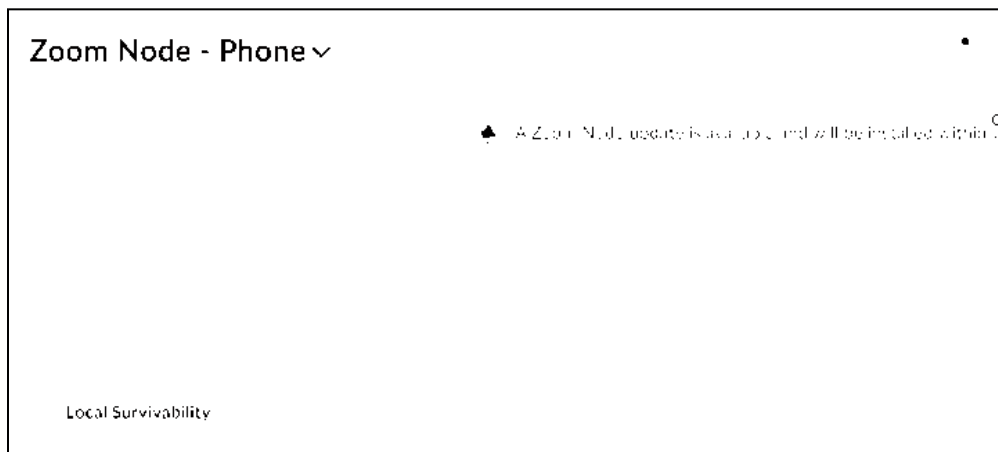
  

Internal domain

Mask vanity name from the domain("zoom")      Add prefix

Click **Add**. Note: the options to “Mask vanity name” and “Add prefix” are used for other Zoom Node services but not ZPLS.

Installation of the module and associated components will begin and the progress can be monitored on the admin portal,



Click the checkbox and Start the services and within a minute the services will display as “Running”.

Zoom Node - Phone		Services	Nodes	Agents	Dashboard			
<input type="text" value="Search"/>								
<input type="text" value="A Services"/>		<input type="text" value="A Status"/>						
Selected 1 Services		Update	Rollback	Start	Stop	Restart	Delete	
<input checked="" type="checkbox"/>	Service		Node		Status	CPU	Memory	Version
<input checked="" type="checkbox"/>	Local Survivability		zoomtopia_zps		Running	0.8%	62M	1.12.0.114

## ZPLS Configuration

### Role-Based Access Control

In order to configure the Zoom Node and ZPLS services, Administrators will need to be provisioned with the appropriate role within the Zoom web portal.

In order to configure and assign the role to Administrators who will be required to provision the ZPLS server navigate to **User Management > Roles** and click **Add Role** in the top right hand corner of the web page. The following permission must be enabled:

User and Permission Management	integration or connector.		
Account Management	<b>Contact Center Mobile SDK</b> Enable users to view and edit permission for downloading a Contact Center experience onto mobile.		
Device Management			
Zoom Rooms Management	<b>Zoom Node</b> Set up servers and services and configure them		Entire Account
Workspaces Management	<b>Hybrid Meeting</b> Manage hybrid multimedia route and zone controller proxy		
Team Chat Management			
Whiteboard	<b>Zoom Phone Local Survivability</b> Set up servers & service for zoom phone survivability mode	<input checked="" type="checkbox"/>	Entire Account
Billing			
Dashboard	<b>Zoom Mesh</b> Set up Zoom Mesh, view dashboard, and configure mesh details		
Reports			
Advanced Features	<b>Hybrid</b> Setup token and list proxy Zone Controller		
Zoom Phone			
AI Management	<b>Device Policy Management</b>		



Alternatively this permission could be applied to an existing role that is already in place.

If a new role is being created then you must ensure that the appropriate members are added by clicking **Role Members**.



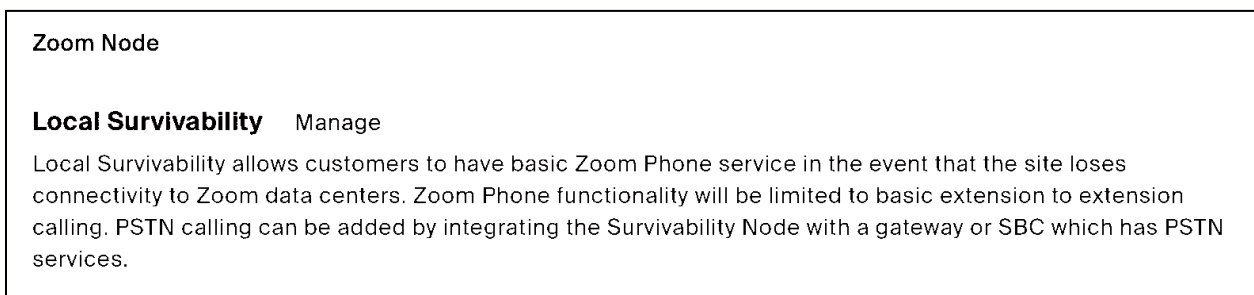
## Enabling the Phone Site with ZPLS

**Note:** If failover PSTN connectivity is required during an outage then Administrators can skip the steps defined within this section and instead move onto the next section.

Associating the ZPLS module and survivability Route Group to the appropriate Site should be done at the same time- this is covered in the [Route Group Configuration](#) section.

Once the Zoom Phone Local Survivability Module has been installed, the Local Survivability module should be associated with a specific Site (or Account in the case of single site deployments).

The ZPLS module to the appropriate Phone Site. Administrators should navigate to **Phone System Management > Company Info > Account Settings > Zoom Node** and select the **Manage** hyperlink that is next to **Local Survivability**.



The appropriate ZPLS server should then be assigned to the Site that requires survivability. Click **“Assign to”**.

Company Info > Account Settings > Local Survivability

### Local Survivability

Search by Service display name

Status (All) Site (All)

Display Name	Server	Service	Status	Version	Assigned to
Local Survivability	_zpls	Local Survivability	Running	1.12.0.114	-- Assign to

The appropriate **Site** should then be selected and then the Admin should click **Ok**.

### Assign Local Survivability

Display Name Local Survivability

Server zpls

Assign to (( San Jose Site

Route Group (optional)

Cancel **OK**

Navigate to **Phone System Management > Company Info > Sitename > Settings > Zoom Node** and verify the assignment and also ensure the services are running.

Company Info > San Jose Site > Settings > Local Survivability

## Local Survivability

Display Name	Local Survivability
Server	zpls
Site	San Jose Site Unbind
Route Group	--
Status	Running Last sync time: Jan 10, 2023 at 7:05 AM ⓘ
Version	1.12.0.114
IP Address	192.168.2.73
Testing Mode	<input checked="" type="checkbox"/>

## Enabling Users for ZPLS

Based on the hardware specification of the server, the maximum number of Users and Devices that can register to a single ZPLS module is restricted to 2000 or 5000 Users/Devices. Zoom is looking to increase this number at some point in the future. Today, Administrators have flexibility in selecting and prioritizing which users and devices are enabled for Survivability by configuring the Zoom Phone Policy setting **Local Survivability Mode**. Only those users and devices that have this policy enabled will attempt to register to the ZPLS module in the event of an outage.

Administrators are able to configure the policy within the the web portal in four different places:

1. Account-wide
2. Site-wide
3. Group-wide
4. Per user or device

## Session Border Controller (SBC)

If PSTN connectivity in failover mode is desired, customers will be required to set up Survivability Route Groups and SBCs from within the Zoom Administrator Web Portal prior to any outage occurring.

In multi-site environments, the SBC can be added within Site Settings or Account Settings from **Admin > Phone System Management > Company Info**. The assumption made within this

document is that a multi-site environment is being used and therefore all the remaining steps are contained within Site Settings.

A SIP Trunk must be established between the SBC and the ZPLS module. The SBC will need to have the DigitCert root and intermediate certificates installed to establish TLS connectivity to both the ZPLS module (as well as the Zoom cloud).

Adding the SBC within the Administration portal does not directly create the SIP Trunk between the ZPLS module and SBC. The SBC needs to be associated with a Survivability Route Group which is then associated with the appropriate Site/Account- only at this stage is the ZPLS module made aware of the IP Address details of the SBC that is used for external call routing.

From the Zoom Administrator Web Portal the admin should navigate to **Phone System Management > Company Info > "Site\_Name" > Routing > Session Border Controllers**. Click **Manage** and select **Add** and then populate the following fields:

- Enter a **Display Name** that describes the SBC being added.
- Enter the **Public IP address** and **Port Number** of the SBC. This is the Public IPv4 address assigned to the SBC (either physically assigned or via static 1:1 NAT on the customer firewall). This field is used to establish a SIP Trunk from the cloud to the external IPv4 address of the SBC for BYOC purposes as discussed in [this section](#).
- Enable **Bring Your Own PBX- Premises** to ensure the BYOC numbers can be routed under normal conditions.
- Enable **OPTIONS Ping Status**- this will enable Admins to verify the SIP Trunk between the SBC and (a) the ZPLS module and (b) Zoom cloud is in service.
- Enable **In Service**
- **Enter a Survivability Public/Private IP Address** and **Port Number** of the SBC- this field is used to establish a SIP Trunk between the ZPLS module and SBC. Zoom recommends using a private IPv4 address to avoid routing through the firewall and possibly adding complex route reflection rules. The IP Address defined here will be pushed to the ZPLS module once the Survivability Route Group (defined in the next step) is added to the Site.

### Add a new SBC

Name:

Public IP Address:

Private IP Address:  
This field is required

Region:

Enable Survivability:

Enable BYOC:

Enable SIP Trunk:

Enable SIP Trunk:

Enable SIP Trunk:

Enable SIP Trunk:

Enable SIP Trunk:

Public IP Address:

Private IP Address:  
This field is required

Cancel

## Route Group Configuration

Two Route Groups should be created at the Account or Phone Site in order to ensure PSTN connectivity is functional with the survivability solution:

1. A Route Group is needed for assignment to the specific Phone System Site that is enabled for survivability - the *Survivability Public/Private IP Address* defined within the SBC is pushed to the ZPLS module. Upon entering failover mode, ZPLS will send external calls to the SBC IP Address contained within the Survivability Route Group. This Route Group does **not** contain a “Region” since the purpose of this Route Group is to establish a connection to the ZPLS module.
2. At least one additional Route Group is required for routing incoming calls to BYOC numbers during normal conditions. In this instance a SIP Trunk is created between the Zoom Phone SIP Zone(s) contained within the Region(s) and the SBC *Public IP Address*. Backup Route Groups are possible with this BYOC Route Group but not the survivability Route Group.

## Survivability Route Group

From the Zoom Administrator Web Portal the admin should navigate to **Phone System Management > Company Info > “Site\_Name” > Routing > Route Groups.**

1. Click **Add** and select the **“Or, add a new route group”** link.
2. Enter a **Display Name** for the Route group.
3. Change the Type to **Survivability**.
4. Click on **Add** and select the **Session Border Controller** that was added in the previous steps
5. Click **Save**

The screenshot shows a form for adding a new route group. The 'Display Name' field is filled with 'ZPLS-RG'. The 'Type' dropdown menu is set to 'Survivability'. The 'Session Border Controller' dropdown menu is set to 'All'. The 'Add' button is highlighted in blue. There are 'Cancel' and 'Save' buttons at the bottom right of the form.

Assign this Route group to the Local Survivability Module

6. Navigate to **Company Info > Account Settings > Zoom Node** and click **Manage**

The screenshot shows the 'Zoom Node' settings page. The 'Local Survivability' section is expanded, showing a 'Manage' button. The 'Zoom Node' section is also visible, with a 'Zoom Node' label.

7. Select the server and click **“Assign to”** and select the Site (this may have been previously configured) and Route Group that was created in the previous steps.

Company Info > Account Settings > Local Survivability

## Local Survivability

Display Name: Local Survivability | Status (All) | Site (All)

Display Name	Server	Site	Status	Weight	Assign to
Local Survivability	Local Survivability	Mumbai	Enabled	10.5	--

Assign to

The selected Server should be assigned to a specific Site and when PSTN connectivity is required the survivability Route Group should also be assigned.

### Assign Local Survivability

Display Name: Local Survivability

Server: Mumbai, India

Assign to: Mumbai Site (Mumbai)

ZPLS-RG

Cancel **OK**

## 8. Click **Ok**

At this stage the ZPLS module for the specified Site will attempt to establish TLS connectivity to the Survivability IP Address/Port and in addition invoke the Options keepalive mechanism if enabled (which is recommended for troubleshooting purposes).

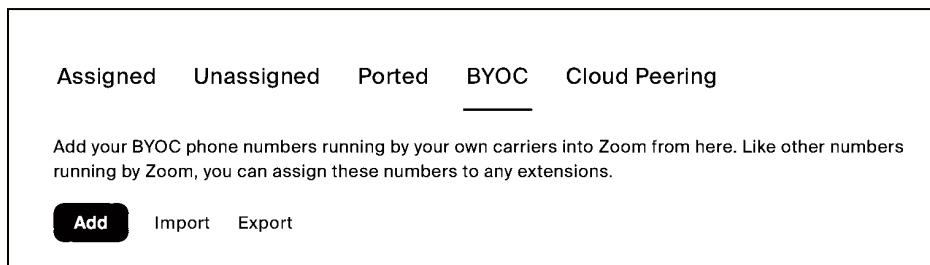
## BYOC Numbers

In order to invoke Call Forwarding for Survivability of Zoom Native Numbers to users and devices located within site undergoing an outage, BYOC numbers associated with the PSTN connection attached to the survivability SBC must be acquired. The number of BYOC extensions required is determined by the number of unique extensions needed during a failover. For example, if 100 users require a Direct Inward Dial service during an outage, 100 extensions must be acquired from the BYOC provider and subsequently 100 Zoom Native numbers can be forwarded to the aforementioned 100 BYOC numbers.

**Note:** Zoom Native numbers can **only** be forwarded to BYOC numbers *assigned* to users within the Site that is being configured for Call forwarding Local Survivability.

In addition to Call Forwarding, a single BYOC number is required for emergency services support. This unique BYOC number can be configured as the Emergency Location Identification Number (ELIN) for the specific Site and must not be assigned to any user or Zoom Phone entity

In order to add BYOC Numbers from the Zoom Administrator Web Portal the admin should navigate to **Phone System Management > Phone Numbers** and select the **BYOC** tab. From here BYOC numbers can be added or imported from CSV.



Once the BYOC numbers have been added to the Site enabled for survivability, they must be assigned to users that will be enabled for survivability (the exception being the BYOC number dedicated as the ELIN for the Site). This can be done by switching to the **Assigned** tab and subsequently assigning the BYOC numbers to users. At this stage users will be configured with a Zoom-provided PSTN number and in addition an BYOC carrier-provided PSTN number. In the event of a failover, only the BYOC carrier-provided PSTN number will be functional.

### ELIN Configuration

Each Site can be configured with a single Emergency Location Identification Number (ELIN). The purpose of ELIN is covered earlier in [this section](#).

From the Zoom Administrator Web Portal the admin should navigate to **Phone System Management > Company Info > "Site\_Name" > Zoom Node** and under the section for Emergency Location Identification Number (ELIN) click **Add Number**.



Zoom Node	<b>Emergency Location Identification Number (ELIN)</b>
Hours	Assign a number that will be used as outbound caller ID when calling emergency services while in Survivable mode
Call Park	
Security	Add Number

From the pulldown menu, the number that will be used as the Calling Number when a user within the Site has dialed the emergency services should be selected. This must have previously been added as a BYOC number within the Site and remain unassigned.

Zoom Node	<b>Emergency Location Identification Number (ELIN)</b>
Hours	Assign a number that will be used as outbound caller ID when calling emergency services while in Survivable mode
Call Park	
Security	4080 Edit

Under **Phone System Management > Phone Numbers** admins are able to view the ELIN as a number assigned to Local Survivability.

Assigned								Unassigned	Ported	BYOC	Cloud Peering
Main Company Number : +13213500357											
Add											Customer
Import											Export
4080											
Number Type (All)											
Assigned to (All)											
Status (All)											
Site											
Assign SMS/MMS											
Disable SMS/MMS											
Number											
Area											
Number Type											
Capability											
Assigned to											
Number Status											
Site											
4080											
United States											
Toll Number											
Incoming & Outgoing											
Local Survivability											
Normal											
Site											

## Call Forwarding Configuration

Prior to any outage, Administrators should set up call forwarding logic to determine how Zoom Native numbers are redirected in the event of an outage.

From the Zoom Administrator Web Portal the admin should navigate to **Phone System Management > Company Info > “Site\_Name” > Zoom Node** and under **Call Forwarding Local Survivability** click **Manage**.

	<b>Call Forwarding Local Survivability</b> Manage
Proxy	Integrate the Local Survivability Node with a gateway or SBC which has PSTN services to enable Call Forwarding. When enabling Call Forward Local Survivability, calls are forwarded to the Destination Number without being processed at the Zoom data centers.
Routing	
Zoom Node	
Hours	

All the numbers that require forwarding during an outage should be selected.

Company Info > Site > Settings > Call Forwarding Local Survivability

### Call Forwarding Local Survivability

**Add**

The number being forwarded is the Source Number and can be extensions assigned to Users, Common Area Phones, Share Line Groups, Call Queues and Auto Receptions. Destination numbers are the BYOC numbers that have been assigned to Users within the site that are enabled for Local Survivability. Multiple source numbers can be forwarded to a single destination number.

Company Info > Site > Settings > Call Forwarding Local Survivability > Add Call Forwarding

### Add Call Forwarding

Source Number(s) Add

Emma Watson 4295 ×

Destination Number 00122

Require a BYOC-P number that is assigned to a user in this site

**Save** Cancel

By default the forwarding status of each source number is disabled.

Source Name	Source Number(s)	Status	Site
2114	30122	Disabled	Site
2591	30122	Disabled	Site
2339	30122	Disabled	Site
4511	30122	Disabled	Site

During an outage admins will need to access the web portal and invoke call forwarding for the selected numbers (**select all** is a shortcut to enable forwarding for all defined source numbers).

### Call Forwarding Local Survivability

**Add**

Q Search

Enable Forwarding   Disable Forwarding

Source Name                      Source Number(s)

## Routing Rules

Routing Rules that are being used under normal conditions can be preserved while survivability is active. From the Zoom Administrator Web Portal the admin should navigate to **Phone System Management > Company Info > “Site\_Name” > Zoom Node** and mark the checkbox for Routing Rules. The ZPLS module will need to be restarted for this change to take effect immediately.

	<b>Zoom Node</b>
Proxy	
Routing	<b>Local Survivability</b> <input type="checkbox"/> <b>Manage</b>
Zoom Node	Local Survivability allows customers to have basic Zoom Phone service in the event that the site loses connectivity to Zoom data centers. Zoom Phone functionality will be limited to basic extension to extension calling. PSTN calling can be added by integrating the Survivability Node with a gateway or SBC which has PSTN services.
Hours	
Call Park	
Security	<input type="checkbox"/> <b>Enable Routing Rules</b>
Outbound Caller ID	During Local Survivability mode, outgoing calls will be routed based on the rules defined in Routing Rules at Site and Account level. The Routing Path assigned to the Routing Rules will be ignored and calls will be sent to the Route Group assigned to the Local Survivability module.
Audio Prompt	

Routing Rules are defined under **Phone System Management > Company Info > “Site\_Name” > Routing > Routing Rules**

**Note:** Routing Rules defined at the Site level can be preserved by ZPLS- rules at the account level will not be preserved.

Typically Routing Rules are used for customized call routing for BYOC-P in addition to preserving users’ legacy dialing habits. When routing rules are used by ZPLS, the Routing Path (SIP Group) is ignored, however number translations are preserved.

## Troubleshooting

### Testing and Validation

The steps below can be used to ensure Zoom Node connectivity to the cloud is operational and all the necessary agents and services required to run the ZPLS module are working correctly.

1. Verify the required services are running:
  - a. Navigate to **Advanced > Zoom Node > Zoom Node - Phone > Nodes** and locate the appropriate server. Click on the server name and validate that the Status of Node Agent and Monitor Agent are started.

Nodes >				
Edit				
IP: <b>192.168.2.66</b>	Location: -	OS: <b>Linux</b>		
Status: <input checked="" type="checkbox"/> Online	PID: <b>1594</b>	Disk Storage: <b>24.40G</b>		
CPU: <b>0.6%</b>	Memory: <b>784M</b>			
<b>Service</b>				
Service	Status	CPU	Memory	Version
<b>Zoom Node OS</b>	Runn ng	-	-	1.6.2.20221209-328.el8
<b>Local Survivability</b>	Runn ng	1.2%	133M	1.12.0.14
<b>Monitor Agent</b>	Runn ng	1.9%	78M	1.2.1.20220808-861.el8
<b>Node Agent</b>	Runn ng	0.3%	51M	1.2.0.20221209-391.el8

2. Verify network connectivity from the virtual machine:
  - a. Open a console window into the virtual machine and enter the credentials for user *zoom-setup*.
  - b. Select Option 2 - **“Test Connectivity to Zoom Cloud”**
  - c. Select Option 1 - **“Test Common Connectivity”**

```
LocalSurvivability

Please wait while your server connects to the Zoom Cloud.

Zoom web front end           success
Zoom node agent distribution  success
Zoom node message broker     success
Zoom node package server     success

Connection test was successful.

Press any key to continue.
```

Select Option 2: **“Test Phone Connectivity”** to validate connectivity to the Zoom Phone data centers

```
LocalSurvivability

Please wait while your server connects to the Zoom Cloud.

US West           success
US East           success
Amsterdam         success
Germany           success
Australia         success
Melbourne         success
Hong Kong         success
Japan             success

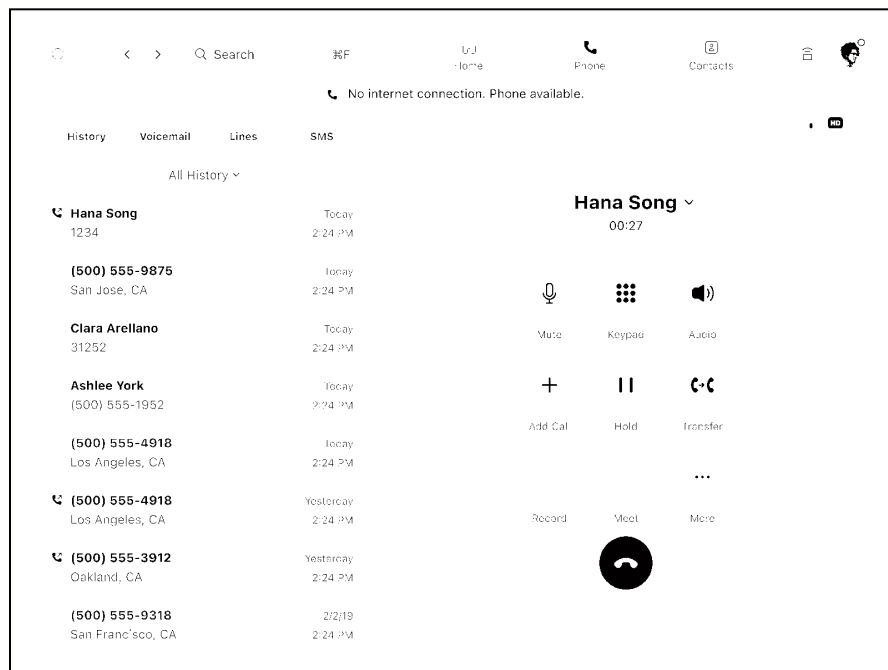
Connection test was successful.

Press any key to continue.
```

## Simulating a failover

To test the Local Survivability module, an internet outage will need to be simulated by disconnecting your internet connection or by creating firewall rules to block access to Zoom Phone networks. To determine which TCP ports to block refer to the [Signaling and Media](#) section of this document.

The Zoom desktop client and physical phones should detect the network loss and connect to the local survivability node. The Zoom desktop clients will show a loss of connection as shown here:



To validate that the Zoom soft clients are registered to the Local Survivability module, do the following on the Zoom client:

1. Click on the Profile picture or icon in the upper right.
2. Click on **Settings**.
3. Click on **Statistics**.
4. Click on **Phone**.
5. Verify the **Register Server IP/Port** is that of your Zoom Node

**Note:** The ZPLS will not be able to accept SIP Registrations unless the Options keepalive mechanism to the cloud has failed. In addition to blocking Zoom Phone traffic to/from the cloud, Admins will also be required to traffic between the ZPLS module and Zoom.

## Testing Mode

Admins are able to bypass creating firewall rules to simulate failover by enabling testing mode. Testing mode removes the need to block cloud connectivity from the desktop client and ZPLS module.

From the Zoom Administrator Web Portal the admin should navigate to **Phone System Management > Company Info > “Site\_Name” > Zoom Node > Local Survivability** and click **Manage**.

Proxy	Zoom Node
Routing	<b>Local Survivability</b> Manage
Zoom Node	Local Survivability allows customers to have basic Zoom Phone service in the event that the site loses connectivity to Zoom data centers. Zoom Phone functionality will be limited to basic extension to extension calling. PSTN calling can be added by integrating the Survivability Node with a gateway or SBC which has PSTN services.
Hours	
Call Park	

By enabling the **Testing Mode** Toggle, new registrations from clients within the associated Site will register to the learnt ZPLS module as opposed to the cloud.

Company Info > Site > Settings > Local Survivability	
<b>Local Survivability</b>	
Display Name	Local Survivability
Server	
Site	Site Unbind
Route Group	ZPLS-RG Unbind
Status	Running Last sync time: Jan 11, 2023, 5:06 AM ⓘ
Version	1.12.0.114
IP Address	192.168.2.66
Testing Mode	<input checked="" type="checkbox"/>



## ZOOM Phone

Testing Mode is only active once the ZPLS module has been restarted. Users should logout and log back into the client in order to verify Local Survivability. Testing Mode is restricted to the Desktop client and does not affect physical devices.