Ports used on your PBX

The table below outlines all the ports used on your PBX that you need to open on your hardware firewall if you want outside users to have access to things. These are default port assignments for new installs, but most can be changed by the user post install. Legacy versions may have used different default port numbers (notably http provisioning) and the original port numbers remain unaffected when the system is upgraded.

For a list of IPs your PBX will need to communicate with, please see Allowed IPs for PBXact Upgrade.

PBX Admin Access

PORT	TCP/UDP	PURPOSE	CHANGING PORT	SECURITY	NOTES
22	TCP	SSH Console	This can only be changed inside from inside Linux CLI and not recommended to be changed.	Not recommended to open this up to untrusted networks.	Port used to allow SSH to the PBX from the outside world.
80 FreePBX 2001 PBXact	TCP	PBX GUI HTTP (Non HTTPS)	Can change this port inside the PBX Admin GUI > System Admin Module > Port Management section.	Not recommended to open this up to untrusted networks.	Used to access the PBX Admin GUI
443	TCP	PBX GUI HTTPS	Can change this port inside the PBX Admin GUI > System Admin Module > Port Management section.	Not recommended to open this up to untrusted networks.	Used to access the PBX Admin GUI with SSL encryption
1194	TCP/UDP	OpenVPN server	Change not supported	Can open to untrusted hosts	Used to connect OpenVPN clients to PBX VPN Server.

PBX SIP and IAX Communication

PORT	TCP/UDP	PURPOSE	CHANGING PORT	SECURITY	NOTES
5060	UDP	chan_PJSIP Signaling	Can change this port inside the PBX Admin GUI SIP Settings module.	Not recommended to open this up to untrusted networks.	Standard Port used for chan_PJSIP Signalling.
5061		chan_PJSIP Secure Signaling	Can change this port inside the PBX Admin GUI SIP Settings module.	Not recommended to open this up to untrusted networks.	Secure Port used for chan_PJSIP Signalling.
5160	UDP	chan_SIP Signaling	Can change this port inside the PBX Admin GUI SIP Settings module.	Not recommended to open this up to untrusted networks.	Standard Port used for chan_SIP Signalling.
5161		chan_SIP Secure Signaling	Can change this port inside the PBX Admin GUI SIP Settings module.	Not recommended to open this up to untrusted networks.	Secure Port used for chan_SIP Signalling.
10000-20000	UDP	RTP for SIP	Can change this port inside the PBX Admin GUI SIP Settings module.	Safe to open to the outside world and is required by most SIP Carriers as your RTP traffic can come from anywhere.	Used for the actual voice portion of a SIP Call.

4569	UDP	IAX	Can change this port inside the PBX Admin GUI IAX Settings module.	Not recommended to open this up to untrusted networks.	Used for IAX protocol and trunking
4000-4999	UDP	FAX UDPTL	Not configurable in the GUI, on by editing custom conf file.		Used for T38 fax media

PBX User Control Panel (UCP)

PORT	TCP/UDP	PURPOSE	CHANGING PORT	SECURITY	NOTES
81	TCP	PBX User Control Panel (UCP) HTTP (Non HTTPS)	Can change this port inside the PBX Admin GUI > System Admin Module > Port Management section.	Not recommended to open this up to untrusted networks as the traffic is not encrypted. Recommend using HTTPS version of PBX User Control Panel instead for remote users.	Port used to access the GUI portion of UCP
4443	TCP	PBX User Control Panel (UCP) HTTPS	Can change this port inside the PBX Admin GUI > System Admin Module > Port Management section.	Safe to open this up to untrusted networks as the traffic is encrypted and requires username and password authentication.	Port used to access the GUI portion of UCP with SSL encryption
8088	TCP	WebRTC Unencrypted Softphone Client	Can change this port inside the PBX Admin GUI > Advanced Settings > Asterisk Builtin mini-HTTP section > HTTP Bind Port	Not recommended to open this up to untrusted networks as the traffic is not encrypted. Recommend using HTTPS version	Used for the WebRTC portion of UCP
8089	TCP	WebRTC Encrypted Softphone Client	Can change this port inside the PBX Admin GUI > Advanced Settings > Asterisk Builtin mini-HTTP section > HTTPS Bind Port	Safe to open this up to untrusted networks as the traffic is encrypted with SSL and requires username and password authentication.	Used for the WebRTC portion of UCP
8001	TCP	Node Server	Can change this port inside the PBX Admin GUI > Advanced Settings > UCP NodeJS Server > NodeJS Bind Port	Not recommended to open this up to untrusted networks as the traffic is not encrypted.	Used by UCP with HTTP for Conf Rooms and Chatting and other products in UCP
8003	TCP	Node Server (secure)	Can change this port inside the PBX Admin GUI > Advanced Settings > UCP NodeJS Server > NodeJS HTTPS Bind Port	Safe to open this up to untrusted networks as the traffic is encrypted with SSL and requires username and password authentication.	Used by UCP with HTTPS for Conf Rooms and Chatting and other products in UCP

PBX Phone Provisioning and Phone Apps

PORT	TCP/UDP	PURPOSE	CHANGING PORT	SECURITY	NOTES

84	TCP	HTTP Provisioning for Phones (Non HTTPS)	Can change this port inside the PBX Admin GUI > System Admin Module > Port Management section.	Not recommended to open this up to untrusted networks as the traffic is not encrypted. Recommend using HTTPS Phone Provisioning option of instead for remote users.	Make sure if opening up outside access to enable username and password authentication for HTTP provisioning from the PBX Admin GUI System Admin > Provisioning Protocol. I nside EPM you define per template if the phones use TFTP, FTP, HTTP or HTTPS provisioning. In the past, http provisioning defaulted to port 83. When upgrading older systems, the port assignments to not change from their original settings.
1443	TCP	HTTPS Provisioning for Phones	Can change this port inside the PBX Admin GUI > System Admin Module > Port Management section.	Safe to open this up to untrusted networks as the traffic is encrypted as long as your enable username and password authentication as outlined in the Notes section.	Make sure if opening up outside access to enable username and password authentication for HTTP provisioning from the PBX Admin GUI System Admin > Provisioning Protocol. I nside EPM you define per template if the phones use TFTP, FTP, HTTP or HTTPS provisioning.
21	TCP	FTP Provisioning for Phones	This can only be changed inside from inside Linux CLI and not recommended to be changed.	Not recommended to open this up to untrusted networks as it has no ability encrypt traffic and is not NAT Friendly. Recommend using HTTPS provisioning for remote phones instead.	Used if your are having phones inside EPM use TFTP for provisioning. Inside EPM you define per template if the phones use TFTP, FTP, HTTP or HTTPS provisioning.
69	UDP	TFTP Provisioning for Phones	This can only be changed inside from inside Linux CLI and not recommended to be changed.	Not recommended to open this up to untrusted networks as it has no ability encrypt traffic and is not NAT Friendly.	Used if your are having phones inside EPM use TFTP for provisioning. Inside EPM you define per template if the phones use TFTP, FTP, HTTP or HTTPS provisioning.
82	TCP	Phone Apps HTTP (Non HTTPS)	Can change this port inside the PBX Admin GUI > System Admin Module > Port Management section.	Not recommended to open this up to untrusted networks as the traffic is not encrypted. Recommend using Phone Apps HTTPS option of instead for remote users.	Port used for phone apps to communicate with the PBX as HTTP not HTTPS traffic. Inside EPM you pick if the phone apps use HTTP or HTTPS.
3443	TCP	Phone Apps HTTPS	Can change this port inside the PBX Admin GUI > System Admin Module > Port Management section.	Safe to open this up to untrusted networks as the traffic is encrypted.	Port used for phone apps to communicate with the PBX using SSL encryption. Inside EPM you pick if the phone apps use HTTP or HTTPS.

Sangoma Connect (Mobile)

PORT	TCP/UDP	PURPOSE	CHANGING PORT	SECURITY	NOTES
see PBX SIP section above	TCP	Sangoma Connect Signaling Sangoma Connect uses chan_PJSIP TCP signaling by default	Change this port in the PBX Admin GUI Settings Asterisk SIP Settings PJSIP TCP Bind Port	Opening this port to untrusted source IPs is necessary for mobile clients, but it's important that it be protected with PBX Responsive Firewall and/or Intrustion Detection (fail2ban)	Used for signaling
See PBX SIP section above	UDP	Media Sangoma Connect media uses the default Asterisk SIP RTP range	The port can be changed by going to Settings Asterisk SIP Settings General SIP Settings Tab. Note: same RTP port configuration as SIP.	Safe to open this up to untrusted networks	Used for media
8443	TCP	Node Server. The SangomaConnect node servers binds on this port only on localhost interface (127.0.0.1). If ConnectMobile SSL certificates are being used, the binding to this port will be secured (https).	The port can be changed by going to Settings Advanced Settings SangomaConnect section Sangomaconnect server Bind Port.	This port is ONLY opened and used on localhost (127.0.0.1). No need to enable /expose it on the firewall.	Used for internal Sangoma Connect API

Zulu 3

PORT	TCP/UDP	PURPOSE	CHANGING PORT	SECURITY	NOTES
8002	TCP	Zulu 3 Client Communication with PBX	Can change this port inside the PBX Admin GUI > Advanced Settings > Zulu Section > Zulu Bind Address	Safe to open this up to untrusted networks as the traffic is encrypted with SSL and requires username and password authentication.	Used for signalling
10000-20000	UDP	Media - RTP	The port can be changed by going to Settings Asterisk SIP Settings General SIP Settings Tab. Note: Zulu uses the same rtp port configuration as SIP.	Safe to open this up to untrusted networks, as your RTP traffic can come from anywhere your Zulu users are connecting from.	Used for handling media during a call

Zulu 2

PORT	TCP/UDP	PURPOSE	CHANGING PORT	SECURITY	NOTES
8002	TCP	Zulu 2 Client Communication with PBX	Can change this port inside the PBX Admin GUI > Advanced Settings > Zulu Section > Zulu Bind Address	Safe to open this up to untrusted networks as the traffic is encrypted with SSL and requires username and password authentication.	Zulu 2.0 requires this and the ports below to be opened. NOTE: You may require the "RTP for SIP" port range to be open as well, for call audio.

8088	TCP	Zulu 2.0 Unencrypted Softphone Client	Can change this port inside the PBX Admin GUI > Advanced Settings > Asterisk Builtin mini-HTTP section > HTTP Bind Port	If using Zulu 3.0 this port should not be open. Not recommended to open this up to untrusted networks as the traffic is not encrypted. Recommend using HTTPS version	Used for the softphone portion of Zulu
8089	TCP	Zulu 2.0 Encrypted Soft phone Client	Can change this port inside the PBX Admin GUI > Advanced Settings > Asterisk Builtin mini-HTTP section > HTTPS Bind Port	If using Zulu 3.0 this port should not be open. Safe to open this up to untrusted networks as the traffic is encrypted with SSL and requires username and password authentication.	Used for the softphone portion of Zulu
5000	TCP	Zulu 2.0 Chat	At this time can not change the port	If using Zulu 3.0 this port should not be open. Safe to open this up to untrusted networks as the traffic is encrypted with SSL and requires username and password authentication.	Used for chat portion of Zulu

RMS Monitoring

PORTS	TCP/UDP	PURPOSE	CHANGING PORT	SECURITY	NOTES
443 5071 4505 4506	TCP Outbound	Checks Metrics RPC	N/A	RMS only uses these ports for outbound connections. Thus, no INBOUND firewall rule changes are necessary.	If the firewall is configured to block outbound ports /connections, then these ports need to be added to the allowed outbound port list.

Reserved Port Range (6000-6199)

This range of ports will be reserved for internal usage. A future release of the sysadmin module will prevent using these for other settings by having System AdminPort Management show an alert when trying to set these as a custom port. These ports will only be used for a variety of internal services. In other words, they are intended for services that will only be accessed by localhost, and should not need any additional firewall configuration since they will not be accessed from external networks. If you have any of these ports configured for use by any known service such as the ones listed above, please change it to something outside of this range to avoid conflicts.