airespring®

Cloud, Fully Managed and Connected

AireSpring User Guide

Accession and VOP Customer Network Configuration Guide v. 1.0

Configure Your Network to Support Accession Communicator for Desktop and VoIP

You must ensure that your network is configured correctly to support **Accession Communicator for Desktop** and the **Voice Operator Panel.**

The following instructions are necessarily at a high level, because the network configuration may be very different at each enterprise customer.

Therefore the customer needs to adapt the information in this section to make it suitable for your particular enterprise's network.

> **For example:** in the section on Firewall Configuration, you should specify the address and port ranges on your Session Border Controller that Accession Communicator Desktop must be able to reach.
>
> If the enterprise is only deploying Accession Communicator for Desktop without softphone function, most of the network configuration is not required and can be removed.
>
> The enterprise will only need to configure their firewall to ensure that Accession Communicator for Desktop can communicate to Airespring's servers.

We assume that DSCP markings on media will be preserved between your core network and the Enterprise's network. If this is not the case, for example, because you do not own the network between the two, you may want to advise your enterprise customers to identify VoIP packets from your SBC and reinstate the appropriate DSCP markings (where they have a border router that supports it). This will typically be DSCP 46 if they are from ports 5060-5070 (signaling) or 46 if they are UDP from any port above 8000 (media).

About this Task

In this task you will:

- Ensure you have adequate bandwidth from your users' computers to the network device (LAN or WAN) and then adequate bandwidth on the WAN side.
- Check that your firewalls or Session Border Controllers permit the codecs used by Accession Communicator for Desktop.
- Configure your firewall(s) to ensure that Accession Communicator for Desktop can communicate with your Service Provider's servers.
- Configure your network to correctly prioritize VoIP signaling, voice and video traffic.

Configure your Bandwidth Requirements

- You must ensure that you have adequate bandwidth for the number and types of calls that you are expecting.

Detailed Procedure

1. For audio calls, the amount of bandwidth you need depends on the codec you are using. You should allow 100Kbps (in each direction) for every call.

- Therefore, if you expect a maximum of 10 concurrent calls, you should assign 1Mbps of bandwidth for voice calls alone, and then ensure you have adequate bandwidth on top of that for other traffic (VPN, web, file transfer) which shares the same connection.

2. For video calls, the bandwidth requirement varies hugely depending on resolution, ranging from 500Kbps (low definition) up to 8000Kbps (HD), again in each direction per concurrent video call. Accession Mobile and Desktop have video enabled in the product by default.

Check you have support for Accession Communicator codecs

- Accession Communicator uses the SILK codec for all calls, including video calls and those to the PSTN - 16kHz for direct media calls to clients that support it or 8kHz for all other calls. Perimeta, the Session Border Controller, transcodes from SILK to G.711 as required when Accession Communicator is talking to other.
- Voice Operator Panel uses G.711 and G.722.
- Accession Communicator also uses G.722 to communicate with compatible remote devices (for example, many SIP desk phones).
- H.264 is used for video on Accession Desktop and Accession Mobile.

Detailed Procedure

You must ensure that your firewalls or Session Border Controllers permit the use of the Accession Communicator for Desktop codecs that you are using.

Configure your firewalls

You must ensure that you have the correct ports open on your firewall to ensure that Accession Communicator for Desktop can communicate with your Service Provider's servers.

By default many firewalls will allow communication from the internal LAN side meaning that no configuration is required here. However, if your firewall requires specific configuration, you must ensure that it is not blocking traffic.

The following table lists all the ports that must be open on your firewall. This table defines the external IP addresses and ports that the Accession Communicator Desktop client needs to be able to reach through your firewall. It is assumed that other standard ports, notably 443 for HTTPS are also open.

Figure 1. All the ports that must be open on your firewall.

Protocol/ Service	Transport	External IP addresses and ports	Notes
SIP/TLS	UDP	199.195.183.249 199.195.183.250 173.245.47.122 173.245.47.121 Ports 5060-5070	The signaling IP address and port of your Service Provider's SBC
RTP	UDP	199.195.183.249 173.245.47.121 Ports 8000 to 65534	The media IP address and port range of your Service Provider's SBC
XMPP (for example, ejabberd)	TCP	8.44.216.41 8.44.216.42 Port 5222	The IP address or domain name of the XMPP server being used. Port will typically be 5222 but may also vary between services.
SOCKS5 (for example ejabberd)	TCP	8.44.216.43 8.44.216.44 Ports 7081 and 7082	The IP address or domain name of the SOCKS5 proxy being used. Port will typically be 7777 but may also vary between services. This is used for fast file transfer on the Accession client.

Configure your Quality of Service (QoS) settings (simple network)

For optimal audio quality, you must ensure that your network is set up to correctly prioritize VoIP signaling, voice and video traffic.

The steps you need to take depend on the configuration of your network. If you have a very complex set-up, then you may need to contact your equipment vendor for advice.

If you have a simple network, you will typically only need to do the following:

- If any Accession Communicator for Desktop user will access your network via a wireless Access Point (AP), ensure that WMM (Wireless Multimedia extensions) support is available and enabled on any such access points.
- Use Quality of Service (QoS) on the WAN/Internet router to prioritize all traffic to and from the SBC IP addresses.

Configure your Quality of Service (QoS) settings (complex network)

If you have a more complex network then you may need to carry out further configuration to ensure optimal audio quality.

You should consult your IT Provider if you need any additional information.

Detailed Procedure

1. Ensure the correct QoS information is signaled on traffic originated by users' computers.

   - You can configure the QoS values that Accession Communicator for Desktop will signal in the Accession Communicator for Windows Phone Profile.
   - However, if you are in an Active Directory domain, Windows will override these values. Instead you will need to configure a QoS group policy that looks for any packets coming out of communicator.exe and marks them appropriately (typically with DSCP 46 if they are going to ports 5060-5070 (signaling) or 46 if they are UDP on any port above 8000 (media). Reference https://docs.microsoft.com/en-us/windows-server/networking/technologies/qos/qos-policy-top for a more detailed description.

2. Configure all your network equipment to correctly prioritize traffic based on the IP header DSCP markings.

   - Signaling and Media traffic should be expedited delivery at the highest priority.

3. You may also need to configure your equipment to rewrite the Ethernet header COS values based on the IP header DSCP values. If you don't take this step, then most managed switches will rewrite DSCP marking based on COS (and COS will typically be zero or incorrect on packets originated from a computer).

Set DSCP marking for domain-joined Windows computers

You must set group policies if you want to do DSCP marking on domain-joined Windows machines.

You can either allow all apps to mark traffic as they wish, or you can create policy conditions. You can set policy conditions to match your individual network set up for Accession Communicator and VoiceOperatorPanel. The simplest way to do this is to match on the application AccessionCommunicator.exe and VOP.exe.

Results

You have now taken the necessary steps to configure your network to support Accession Communicator for Desktop.