Technical Bulletin CS-20-05

Network Ports and Destination Hosts

This document provides guidance on those network ports and destination hosts a customer may need to accommodate in their network security settings, such as Access Control Lists (ACL), or firewall rules for a Versity deployment.

System Affected

Spectralink Versity

Introduction

Each deployment will likely have different applications and configurations that can affect the required network port and destination host rules, but correctly configuring network devices is critical to Versity operation and installed apps.This document walks through these considerations.

Note: Security implications of network changes described within this document need to be fully considered and understood by the customer or administrator before implementation. This document is not a substitute for an enterprise security policy. Spectralink shall not be held liable as a result of implementation of these guidelines. This document does not consider VoIP performance or suggest network architectures.

This document breaks down the network requirements into logical components:

1. Google Services
2. EMM. Most deployments will use an EMM.
3. Third-party apps. Many apps rely on a connection to a remote server.
4. Spectralink OA&M Servers. These include logging servers, SAM, firmware update servers.
5. Unified Communications, e.g. SIP dialer app.
6. General network services, e.g. DNS, NTP etc.

Google Services

As an Android smartphone, Spectralink Versity requires access to the public Internet for underlying Google services, app updates from the Google Play Store, Google Push notifications, and access to other Google cloud-based servers.

Even if an administer intends to disable, or hide, many of the consumer oriented Google apps installed (e.g. Gmail, Maps, Hangouts), Versity will still typically need some external access to the public Internet to allow the underlying Google services to function. Many third-party apps rely on these Google services being operational.

Push Notifications (GCM / FCM), Play Store App Updates, and Network Validation

Google's Push notifications are used by almost all alarm and texting apps to deliver users with message and alert notifications. These notifications are sent from the Google cloud servers to Versity devices, so external corporate firewalls need to allow these packets into their networks to the Versity devices. The following table provides guidance per Google docs, but for more detail, refer to https://firebase.google.com/docs/cloud-messaging/concept-options#ports_and_your_firewall

App updates from the Play Store (i.e. if you are using Android Enterprise via an EMM) also require the same ports listed opened. Lastly, the Android OS tests if Wi-Fi networks have access to external Internet. Without this, Android may present notifications that the Wi-Fi network may not be operational.

Port	UDP/TCP	In/Out	Protocol	Description
443	TCP	IN	HTTPS	
5228-5230	TCP,UDP	IN	Proprietary	Push Notification, Play Store
*	TCP	OUT	-	Either : 1. No IP restrictions 2. All IP addresses contained in the IP blocks listed in Google's ASN of 15169. Don't forget to update this at least once a month.

It is recommended to make the following Public Internet destination hosts accessible for the above Google services's operation.

Destination Host / Domain
play.google.com
googleapis.com
accounts.google.com
ssl.gstatic.com
www.gstatic.com
connectivitycheck.android.com
connectivitycheck.gstatic.com
google.com

Other Google Apps

Many Google apps are not typically suitable for enterprise-owned, shared-use devices, like Versity. But if you are planning to allow users access to Google Maps, Chrome, Gmail etc., it is recommended to review the Google Support site to verify what ports and domains are required.

EMM Considerations

Every Versity deployment should utilize an Enterprise Mobility Manager (EMM) solution (e.g. AirWatch, MobileIron, SOTI). Each EMM vendor may have different device port and destination host connectivity requirements, and will further differ if the EMM is on-premises or cloud-based. It is critical to refer to the vendor's documentation for their precise requirements.

The following provides some conceptual guidance on device-EMM network connectivity requirements, and potentially can assist troubleshooting:

1. Initial Agent installation
2. EMM enrollment
3. EMM communication

Initial EMM Agent Installation

Most Versity deployments will use Android Enterprise, and employ the EMM agent as a Device Owner. During an NFC bump, or QR code based enrollment, parameters are passed to Versity telling the device where to download the EMM agent APK from. Usually the agent APK is not downloaded from the Google Play Store, but likely an EMM vendor's web-server. For example, reviewing the relevant NFC parameters passed by VMWare's AirWatch Relay app:

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https\://awagent.com/monileenrollment/airwatchagent.apk

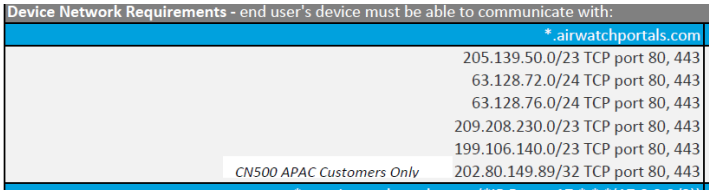
Therefore, the network should allow the Versity device to retrieve the APK using HTTPS (i.e. port 443) from the specified domain (e.g. awagent.com). As this request is initiated by the device, this would not require an explicit inward network port opened, although the target web-server should be accessible to the device.

EMM enrollment

Once the agent APK is installed and suitable parameters are received, the agent will attempt to contact the EMM server. Parameter(s) passed during initial bump or QR scan provide the server identity. This may vary across EMM vendors, but taking AirWatch as an example, the server URI is provided as an parameter in the Extras bundle:

android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE=\#admin_extrasbundle\nserverurl\=techp.awmdm.com\n<snip>

Reviewing the AirWatch Installation documents, the AirWatch server domain or host will be *.airwatchportals.com domain, and most EMMs will use a encrypted tunnel (e.g. HTTPS via port 443) to ensure secure communication.



EMM-Device Communication

Once Versity is enrolled into the EMM, the EMM and device communicate as needed. The mechanism may vary between vendors, but typically one or both mechanisms listed will be used.

- A device may periodically poll the EMM server to ‘check-in’ and determine if there are any actions queued. Polling allows a device to conserve battery and eliminates the need to explicitly open inward network ports. This mechanism typically uses HTTPS on port 443.
- EMMs can also use Push notification schemes, such as Google’s C2DM, GCM or FCM, to trigger device actions. These would require the same ports/domains as documented in the Google section.

  Some EMM vendors may also support a proprietary notification mechanism (to accommodate devices that are not Google certified, and thus lack the C2DM/GCM/FCM capabilities). These may require additional ports.

EMMs tend to include other applications beyond the Agent, such as email, browser, vpn. Each of these apps may require additional ports and domain network settings.

As a general guideline these are the minimum typical ports for communicating with a cloud-based EMM. Refer to vendor documentation for precise instructions.

Port	UDP/TCP	In/Out	Protocol	Description
443	TCP	OUT	HTTPS	Secure tunnel to EMM
5228-5230	TCP,UDP	IN, OUT	Proprietary	Push Notification

Third-Party Apps

Certain types of apps are designed self-contained and do not require network connectivity to a remote server, whether on-premises or cloud-based. However more and more apps do require some kind of connectivity. As described in the Google Services sections, many apps also rely on Android OS (or Google) services that require public Internet access.

It is recommended to review third-party app installation documentation to ascertain their network requirements. Even then some app-developer may assume network connectivity, or not describe all assumptions, and therefore not document all requirements, so it is important to test apps properly prior to deployment to ensure they are performing as expected.

In absence of complete documentation of network requirements, network and packet analysis tools, e.g. wireshark, may provide insight on the network destinations apps are trying to communicate with.

Spectralink OA&M Servers

The Versity devices utilize several servers for application configuration, logging, and software updates.

Spectralink Application Management (SAM) Server

The SAM server is used by Versity system adminstrators to optimally configure and manage the Spectralink applications installed on Versity. It is not recommended to have the SAM server accessible to the public Internet. Instead it should reside within the corporate private network.

Versity communicates with SAM predominantly in a polling fashion. In the SAM documents, this is referred to as a heartbeat. It uses a secure HTTPS connection via port 443. When an admin need to trigger an immediate heartbeart from the device, the SAM server initiates communication to the device using port 9090.

Port	UDP/TCP	Protocol	Description
443	TCP	HTTPS	Used for Heatbeat communications
9090	TCP	Proprietary	Used to Trigger hearbeat by SAM server.

The SAM server needs to be accessible by the Versity devices.

Note: This document only considers device network considerations. Additional network settings changes may be needed for an administrator to browse or administer updates to the SAM server.

Logging Server

Versity supports several logging or debugging mechanisms. The preferred “Advanced Debudding” mechanism uses HTTP or HTTPS to any configured web-server port. The default ports being 80 and 443 respectively. Alternatively, Versity can send debug using syslog to a syslog server on port 514 (or another port if configured).

It is recommended to have the logging server on your private network and not on the public Internet.

Port	UDP/TCP	Protocol	Description
514*	UDP	Syslog	Default port for Syslog server – if used (optional)
80*	TCP	HTTP	HTTP or HTTPS can be used to upload logs to logging server.
443*	TCP	HTTPS	

* default – configurable.

Software Update Server

It is highly recommended to have a web-server host Versity software images for software updates. This server may reside somewhere on the corporate (private network), or can even be hosted on a publicly accessible server, e.g. AWS S3. One consideration of external hosted web-servers is the WAN bandwidth consumed during software updates by all devices.

Versity’s SysUpdater app will poll the webserver either using HTTP or HTTPS, and download new firmware images using those protocols when available. The SysUpdater app receives web-server URI, port number, and desired protocol (HTTP/HTTPS) as configuration parameters from SAM or an EMM.

Port	UDP/TCP	Protocol	Description
80*	TCP	HTTP	HTTP or HTTPS can be used by Versity to update device software
443*	TCP	HTTPS	

* default – configurable.

AMIE Gateway

If purchased or utilized, the AMIE Advanced analytics system requires Versity devices to communicate to an AMIE Gateway before the data is sent to the cloud-based analytics servers. The AMIE Gateway is a virtualized server that should reside within the corporate network or DMZ. Versity sends analytics data to the AMIE Gateway using the MQTTS protocol (i.e. MQTT over SSL) on port 8883.

Port	UDP/TCP	Protocol	Description
8883*	TCP	MQTTS	Used for Analytics data capture.

Unified Communications

Versity has an integrated SIP telephony dialer app, Biz Phone. The following section describes the port requirements for this app. Customers using third-party UC apps, e.g. Jabber, Bria, Skype will need to refer to the vendor's documentation for network requirements.

Biz Phone does not support NAT traversal (e.g. STUN, ICE), thus the call-server must reside within the internal network.

Port	UDP/TCP	Protocol	Description
389	TCP	LDAP	Optional for contact directory lookup
636	TCP	LDAP	
2222	UDP	RTP	Audio Packets
2223	UDP	RTCP	Audio Control
5060	UDP,TCP	SIP	SIP Signaling
5061	UDP,TCP	SIP	SIP Signaling (Secure SIP)
5070	UDP,TCP	SIP	SIP Signaling
5071	UDP,TCP	SIP	SIP Signaling
4000-	UDP	RTP	The target port is dynamic

General Networking Services

Versity utilizes many common networking services. The servers are associated ports need to be accessible by the devices. These include:

Port	UDP/TCP	Protocol
53	UDP	DNS
67	UDP	DHCP
68	UDP	DHCP
123	UDP	NTP

Unless configured to use a local NTP server, by default, Versity will attempt to use public Internet based NTP servers. If a NTP server is not accessible, then the time and date of the device may be wrong, causing problems with applications and/or authentication. This can include failing to provision when performing setup to an EMM/MDM and validating certificates. The default time server the phone searches for is 0.android.pool.ntp.org. This will include the phone trying to use variations of this address with the 0 being replaced with 1, 2, 3 and so on.

Firewall rules should focus on allowing requests to ntp.org to, or even android.pool.ntp.org, to limit the number of rules required. Please note that Android 10 does not support the use of DHCP option 42. However, Spectralink added support for DHCP option 42 in release 2.5 and 1.5.

Document Status Sheet

Document Control Number: CS-20-05

Document Title: Network Ports and Destination Hosts

Revision History: I01 – Released
I02 – Released
I03 – Released

Date: *March 14, 2019*

Status: ☐Draft ☒Issued ☐Closed

Distribution Status: ☐Author Only ☐Internal ☐Partner ☒Public

Copyright Notice

Notice

Warranty

The *Product Warranty and Software License and Warranty* and other support documents are available at http://support.spectralink.com.

Contact Information

US Location
+1 800-775-5330

Spectralink Corporation
2560 55th Street
Boulder, CO 80301
USA

info@spectralink.com

Denmark Location
+45 7560 2850

Spectralink Europe ApS
Bygholm Soepark 21 E Stuen
8700 Horsens
Denmark

infoemea@spectralink.com

UK Location
+44 (0) 20 3284 1536

Spectralink Europe UK
329 Bracknell, Doncastle Road
Bracknell, Berkshire, RG12 8PE
United Kingdom

infoemea@spectralink.com