IMS Integration Guide

Prepared for:

IMS Customers
30th September 2020

Document Details:
Version 1.11.0.1

FTP SOLUTIONS

Level 10,
182 St Georges Terrace,
Perth, WA, 6000

otsc@ftpsolutions.com.au
(08) 6355 5281
ftpsolutions.com.au

Document name	IMS Integration Guide
Version	1.11.0.1
Version date	31 August 2020
Created by	Steven Brown
Approved by	Acea Quigg

1. Version History

Version should be the current IMS release version with an extra number. I.e. for IMS version 1.8.2, the IMS Integration Guide should have a version 1.8.2.X. Increment X as required.

Date	Version	Author	Description of Change
22/03/2017	1.0	Steven Brown	Created
24/10/2017	1.1	Acea Quigg	Added GIS info
25/10/2017	1.2	Acea Quigg	Added remote access requirement
26/10/2017	1.3	Acea Quigg	Added FTP IPs
12/04/2018	1.4	Acea Quigg	Added distributed IMS info
19/07/2018	1.5	Acea Quigg	Updated for IMS 1.7
10/09/2018	1.6	Acea Quigg	Added WebGL requirement
18/09/2018	1.7	Acea Quigg	Added new IMS components
21/03/2019	1.8	Aaron Low	Updated for IMS 1.8
28/05/2019	1.8.2.1	Aaron Low	Updating SRS, SMTP requirement
20/06/2019	1.8.2.2	Acea Quigg	Bandwidth info, more device support
27/06/2019	1.8.2.3	Acea Quigg	Updating NAM and agent ports
5/07/2019	1.8.3.0	Aaron Low	WMI static port information
5/08/2019	1.8.3.1	Acea Quigg	Updated IMS architecture diagrams
13/11/2019	1.8.3.2	Acea Quigg	Updated IMS architecture diagrams
21/11/2019	1.9.0.0	Acea Quigg	Updated for IMS 1.9
05/12/2019	1.9.0.1	Aaron Low	Updated IMS architecture diagrams
15/04/2020	1.9.0.2	Acea Quigg	Updated access requirements
22/04/2020	1.9.0.3	Aaron Low	Updated integration diagrams and flows
24/04/2020	1.9.0.4	Aaron Low	Updating ports and protocols
24/04/2020	1.9.0.5	Aaron Low	Updating ports and protocols
05/06/2020	1.10.0.0	Aaron Low	Updating IMS VM spec
09/06/2020	1.10.0.1	Edward Beech	Adding IMS Roles and LDAP overview
16/06/2020	1.10.0.2	Edward Beech	Updating user computer specification
25/06/2020	1.10.0.3	Aaron Low	Updating terrain data requirements
08/07/2020	1.10.1.0	Aaron Low	Updating IMS VM spec
31/08/2020	1.11.0.0	Aaron Low	Updating pre-deployment section and minor 1.11.0 changes
30/09/2020	1.11.0.1	Aaron Low	Adding NTP and DNS requirements

Contents

FTP SOLUTIONS

Level 10,
182 St Georges Terrace,
Perth, WA, 6000

otsc@ftpsolutions.com.au
+61 8 6355 5281
ftpsolutions.com.au

Please Note:

The document is meant to be an accurate deployment and requirements guide and should be read and thoroughly understood by anyone looking to deploy IMS, both from a technical and non-technical perspective.

It is important to understand the IMS' requirements and ensure that they are met. The requirements set out in this document are exactly that, requirements. Very few things are nice to haves, rather they are a necessity. In saying that though, FTP is always happy to work with customers and provide alternate solutions where network security or environmental challenges become a concern, especially in the likes of AHS environments.

IMS access for integration and support activities seems to field the most questions and is generally met with the most opposition, and rightly so. We acknowledge that outbound connections from the IMS server back to the FTP office servers may appear to be a nice to have, but, in reality, are a necessity.

These outbound connections allow the deployed IMS server to receive application and security updates, allow IMS server health to be monitored proactively and they also allow FTP support staff to provide customer support when customers pose questions or experience technical difficulties.

If outbound connectivity can't be permitted, then there are many other options, such as a direct VPN connectivity and direct SSH connectivity, as long as this allows for an OSX machine to directly communicate via IP to the target IMS server.

IMS is managed with a set of robust deployment tools that manage IMS versioning, system requirements, software requirements, system optimisation, backup and rollback functionality. Without the ability to use the IMS deployment tools the job of supporting and maintaining IMS becomes a burden of concern for FTP and will fall into a different category of support where the customer will be charged for support by the hour, rather the usual free application support. In the absolute worst case, it is possible to fly a technician to site once a year to update IMS or when as is required, FTP can provide pricing for this option if required.

2. Document Intent

The Intent of this document is to provide clients with a technical overview of the steps and processes associated with the implementation and enablement of the Integrated Management System (IMS) at a customer's site.

FTP SOLUTIONS

Level 10,
182 St Georges Terrace,
Perth, WA, 6000

otsc@ftpsolutions.com.au
+61 8 6355 5281
ftpsolutions.com.au

3. Technical Overview

Refer to Annexure A – IMS Application Overview for architecture diagram

The IMS software operates on a virtual machine; the architecture within the IMS is broken down as:

- IMS frontend (approximate)
  - Nginx web server (SSL)
- IMS API (approximate)
  - Brokers connections between the frontend and the backend
  - Caches data
  - Limits requests
  - Provides a data pipeline to request or save data in the backend
- IMS backend (approximate)
  - Trailer and Vehicle device monitoring
  - Backhaul device monitoring
  - Server monitoring
  - Power system (solar/generator) monitoring
  - Availability monitoring
  - ICMP ping streams
  - SNMP streams (hardware dependant)
  - HTTP/HTTPS streams (hardware dependant)
  - SSH streams (hardware dependant)
  - Location sources
    - FMS API and/or database tie-in
    - Intermittent streams to trailer GPS data source (hardware dependant)
- IMS database
  - PostgreSQL
  - Holds all of the IMS data
- IMS message queue
  - Internal IMS message queue
  - Provides a message bus for inter-module communications
- IMS messenger service
  - Sends physical emails, alerts, reports and other messages outbound
- IMS report generator
  - Responsible for creating reports utilising IMSQL
- IMS imagery
  - Generates flyover and terrain imagery
  - Server flyover and terrain imagery

4. Technical Requirements

4.1. User Environment

The user environment will be the standard client desktop or laptop SOE; with the exceptions:

- The latest Google Chrome should be installed to utilise the IMS web GUI
    - Chrome v62 or less must be used if computers have Intel iris 6100s
- For users, whose job it will be to focus on the IMS application, it is recommended that a dedicated graphics processor is installed, a Nvidia GTX 950 or better or AMD equivalent
- For users who will be checking on the IMS for statistics and reporting, a standard laptop with integrated graphics will be sufficient, however, a dedicated GPU is recommended.

4.1.1. IMS User Hardware Configurations

4.1.1.1. User Desktop

- Ubuntu 16.04 desktop/OSX 10.10/Windows 7 or newer
- CPU – 4 x 2GHz+ cores
- RAM – 8GB
- Storage – 80GB HDD
- Google Chrome 64-bit (v58 or above)
- Dedicated 3D graphics accelerator (where applicable)
    - Nvidia GTX 950 or better or AMD equivalent
- Correct graphics drivers to ensure best performance
- WebGL enabled in Chrome and the user's SOE
- Client corporate network connectivity to IMS server; or
- Client corporate VPN access with access to IMS server

4.1.1.2. User Laptop

- As above, with equivalent mobile GPU
    - SSDs are recommended

4.2. Production Environment

4.2.1. Network Access

It is a requirement for the IMS to have routed access to all services, devices and hardware that should be polled/interrogated/accessed/utilised in the gathering and display of fleet and network data. Those requirements include SSH, Telnet, HTTP, HTTPS, MODBUS, SNMP, database access via ODBC and a source of flyover imagery from a system like ArcGIS' RESTful web interface. Access and system requirements are likely to grow over time. A list of ports and protocols is in Annexure E - IMS Ports and Protocols.

4.2.1. IMS bandwidth requirement

The IMS' bandwidth requirement to the field is heavily dependent on the hardware that is being monitored. It ranges from about 250bps to about 3kbps averaged out over an 8 second polling cycle. As you can imagine, SNMP polling a switch pulls back a fair amount more data than an IMS agent running onboard a Linux radio pushing back data.

IMS bandwidth requirement to the user is somewhat bursty, as it is a dynamic web application. When the user loads the IMS application for the first time the user's chrome browser will load an additional ~2MB of data, which is the IMS application's static data. Every subsequent IMS page load will result in ~6MB of data being first loaded, this includes 30 minutes of live data for the site.

Once the initial data is loaded IMS will stream in new data as it becomes available at a rate of around ~23KB per 8 seconds or roughly 3KB a second per open IMS instance.

4.2.2. IMS VM configuration

The IMS application is usually installed on a single VM. It can be configured and installed in such a way that the IMS components, specifically, the Frontend, API and Backend are installed on separate VMs. You would choose a distributed installation if you have a specific security requirement that requires the IMS users to access a frontend in the corporate network that was then pulling data from an API/Backend that was protected by a site-based firewall. The other reason to choose a distributed installation is if there are a very large number of devices being polled by IMS, ~2500+. It is possible to poll 2500+ devices on a single VM, however the VM specs would become a considerable portion of the physical host's resources and in most cases a physical server would make more sense.

4.2.2.1. Single VM IMS

- OS:
  - Ubuntu LTS Server 18.04 or newer
    - https://www.ubuntu.com/download/server/thank-you?version=18.04&architecture=amd64
    - Ensure to select LVM when partitioning
    - Ensure SSH server module and access is enabled
- CPU:
  - 8 x 2.2GHz if < 50 trucks
  - 12 x 2.6GHz+ if >= 50 trucks
- RAM:
  - 16GB if < 50 trucks
  - 32GB if >= 50 trucks
- Storage:
  - Mounted at /srv
    - 700GB if < 50 trucks
    - 1TB if >= 50 trucks

        - Mounted at /
            - 50 GB

**Numbers are not exact, testing and adjusting is required. 'Trucks' refers to dump trucks, not devices with an IP.*

4.2.2.2. Distributed IMS

- OS requirements
    - As for Single VM IMS installation
- Front-end VM
    - CPU
        - 4 x 2.2GHz+
    - 8 GB RAM
    - 50GB storage mounted at /
- API + Database + Master backend VM
    - CPU
        - 8 x 2.2GHz if < 50 trucks
        - 12 x 2.6GHz+ if >= 50 trucks
    - RAM
        - 16GB if < 50 trucks
        - 32GB if >= 50 trucks
    - Storage
        - Mounted at /srv
            - 700GB if < 50 trucks
            - 1TB if >= 50 trucks
        - Mounted at /
            - 50GB
- Backend collector VM
    - CPU
        - 8 x 2.2GHz if < 50 trucks being polled from this VM
        - 12 x 2.6GHz+ if >= 50 trucks being polled from this VM
    - RAM
        - 16GB if < 50 trucks being polled from this VM
        - 32GB if >= 50 trucks being polled from this VM
    - 50GB storage mounted at /

**Numbers are not exact, testing and adjusting is required. 'Trucks' refers to dump trucks, not devices with an IP.*

4.2.2.3. IMS required packages

For ease of installation and troubleshooting IMS requires some minimal packages installed on the host. If these packages do not exist in your standard operating environment, FTP requests that these packages be installed on the VM.

- docker 18.06.1-ce or newer
- bash
- htop
- telnet
- tcpdump
- snmpwalk
- nano
- vim
- curl
- wget
- nmap
- ssh and sshd
- python 3
- tar and gzip
- screen

5. IMS Deployment

Integration of assets and devices into the IMS is undertaken by FTP or its agent. The integration team will use the client supplied asset register containing IP address, equipment numbers/types and fixed infrastructure locations. The integration team will provide an Asset Register template. The more time spent getting the asset register correct and updated, the quicker IMS will be available and in production.

5.1. Project Kick-off

Once FTP Solutions has received a PO, implementation will begin, and the pre-deployment stage commences.

5.2. Pre-deployment - Data Collection

During the Pre-deployment phase, the steps involved in the Active IMS Deployment stage are outlined, and the information required from the client is sourced and discussed. This is to ensure that all parties are clear on what is involved in deploying IMS. The Pre-deployment phase will focus on:

- Identify the Deployment/Integration Team
    - Project manager
    - Project contacts
        - Infrastructure
        - GIS personnel
        - Fleet management personnel
        - Network team
- Complete and return the Asset Register information, See Annexure F – Example Asset Register.

    - Fleet management system
        - API/DB access details
        - Transform must be supplied if locations are in local grid. If in a standard SRS, provide the EPSG code.
    - Terrain / high precision management system
        - API/DB access details
        - Transform must be supplied if locations are in local grid. If in a standard SRS, provide the EPSG code.
    - On truck / excavator / drill / trailer / tower wireless radio/s
        - Access details
        - IP addresses
    - Point to point microwave radio/s
        - Access details
        - IP addresses
    - Point to multi-point microwave radio/s
        - Access details
        - IP addresses
    - Power infrastructure on fixed and semi fixed Assets, e.g. solar controllers
        - Access details
        - IP addresses
    - Location source for fixed and semi fixed Assets
        - Database
        - GPS device on Asset. Require access details and IP addresses
        - Fixed locations given in Asset Register (one time update only)
- Provide network diagrams. If there are any specific networking requirements, please make them known to the FTP Solutions team.
- Provide access to NMS software to speed up IMS deployment
- Build the IMS VM in line with the IMS VM configuration section
    - Create 'ftpsolutions' user account
        - Must have sudo rights
- Create service accounts for device polling
    - IAW Annexure E – IMS Ports and Protocols
- Create LDAP IMS RO, RW and Manager groups
    - Provide LDAP server details
- Configure SMTP relay for sending IMS notifications and reports
    - Provide SMTP relay details
- Put in change management for any required firewall rules
    - IAW Annexure E – IMS Ports and Protocols
- Provide high resolutions site flyover imagery
    - ArcGIS or ERDAS or compatible WMS/WMTS/TMS URL
    - Static file can be supplied
        - Must be geo-referenced

        - Transform must be supplied if in local grid. If in a standard SRS, provide the EPSG code.
- Provide 3D xyz terrain file for site. Note that for formats that do not contain spatial reference system (SRS) information, the user will require an EPSG code. https://spatialreference.org/ref/epsg/
    - Vulcan DXF file (Feature type Point or LineString or Polygon), or
    - GeoTIFF containing SRS information, or
    - Esri Shape file, or
    - ASCII x,y,z file
- Ensure all IMS servers can connect to a NTP server.
- If DNS is used in the environment, ensure all IMS servers can connecto to a DNS server.

5.3. Pre-deployment – IMS VM Access Requirements

FTP requires access to the IMS VM in order to deploy the IMS software. The easiest way to do that is to provide FTP with a VPN connection to the client's site. Direct SSH or HTTP access is acceptable from the Internet to the IMS VM or in reverse, from the IMS VM to the IP addresses and ports listed below.

RDP and Citrix are not acceptable forms of network access! The FTP deployment server needs to be able to communicate using TCP/IP directly with the IMS VM that is being integrated.

In the majority of cases, IMS will require outbound access to FTP's servers for support, licensing and updates:

- 49.255.243.204 port 443 (TCP) for IMS app support/IMS app updates/Integration
- 49.255.243.205 port 80 & 443 (TCP) for server health/IMS app health monitoring

5.4. Deployment

Active IMS deployment usually takes around two weeks. During this time FTP will use the information gathered during the pre-deployment phase to populate the IMS with the site's network information. FTP will work with the site to ensure that all devices are being polled and IMS is operating as anticipated. If the site has any technology that IMS does not support new polling engines will be written, providing the technology is in scope.

5.5. Post-deployment

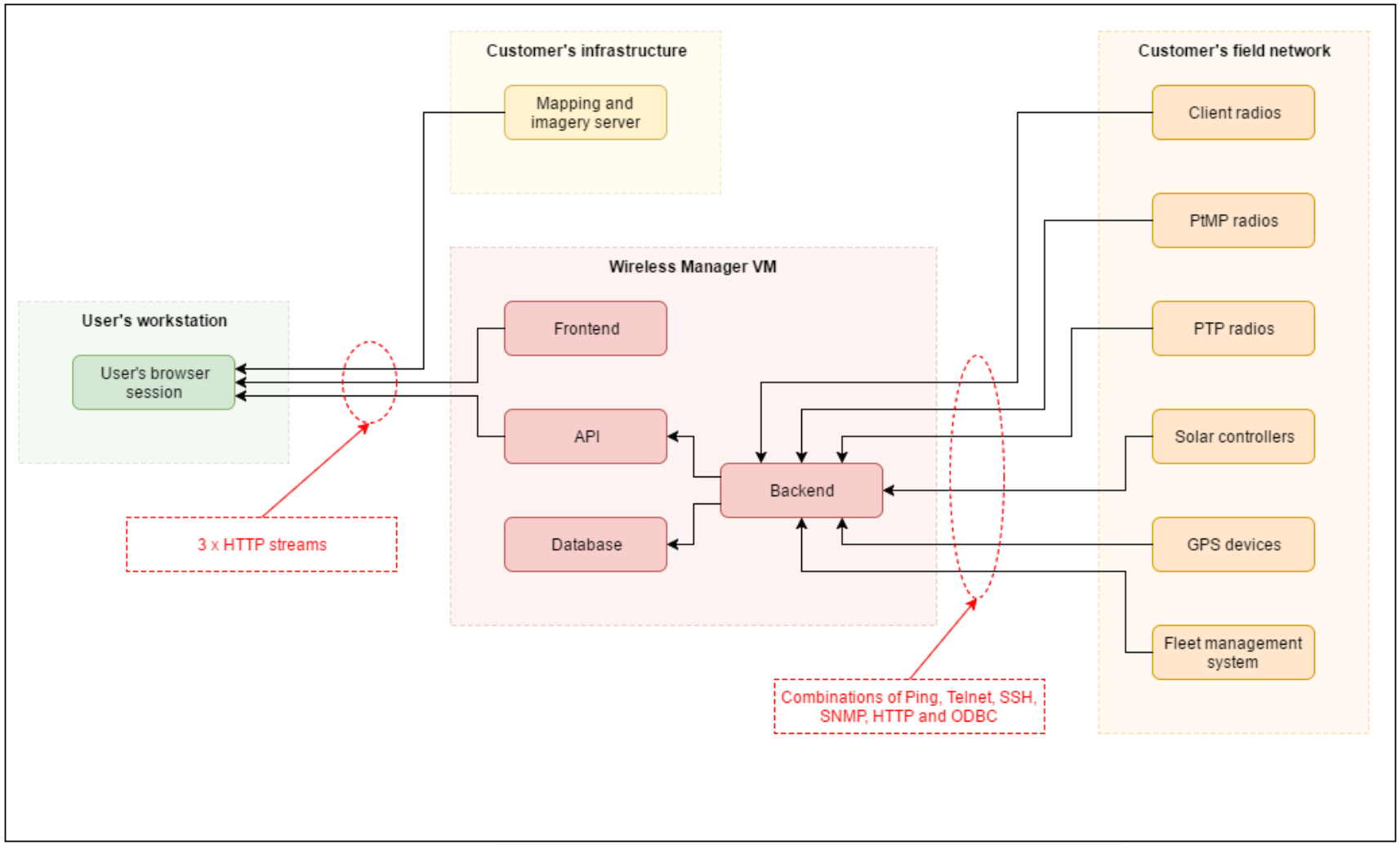
5.5.1. Training

FTP will provide training to the client's relevant personnel on the use of the IMS platform. This training has been developed in a "*train-the-trainer*" format, so as to enable the internal personnel to pass on the relevant training to other potential users. Training time required is typically 6-8 hours and is conducted at either the client's site or FTP's office.

5.5.2. Project Completion / Integration Sign-Off

Once the software has been integrated and accepted by the client, invoicing will follow. Training will be conducted outside of integration on a separate PO.

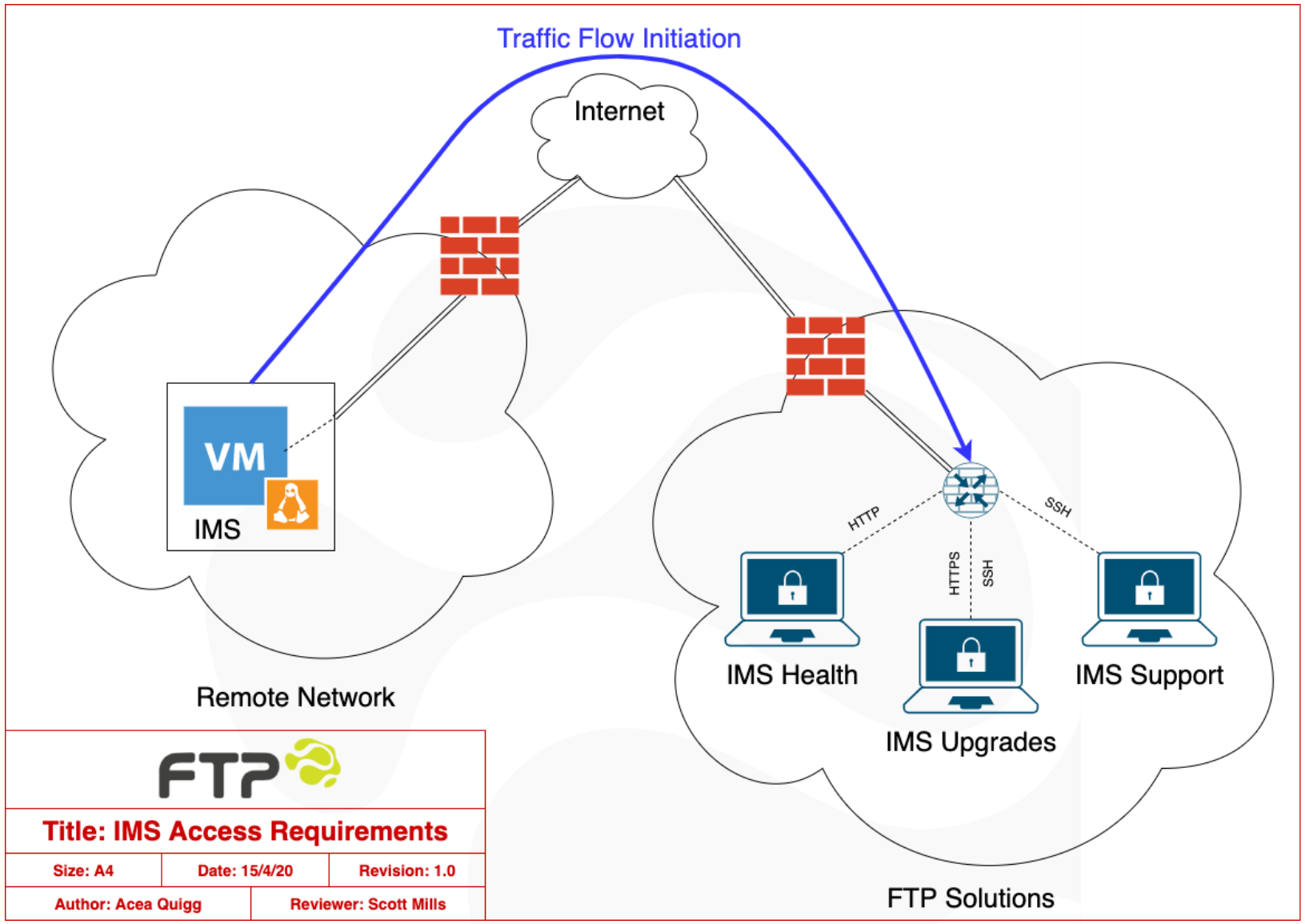
6. Annexure A – IMS Application Overview



Level 10,
182 St Georges Terrace,
Perth, WA, 6000

otsc@ftpsolutions.com.au
+61 8 6355 5281
ftpsolutions.com.au

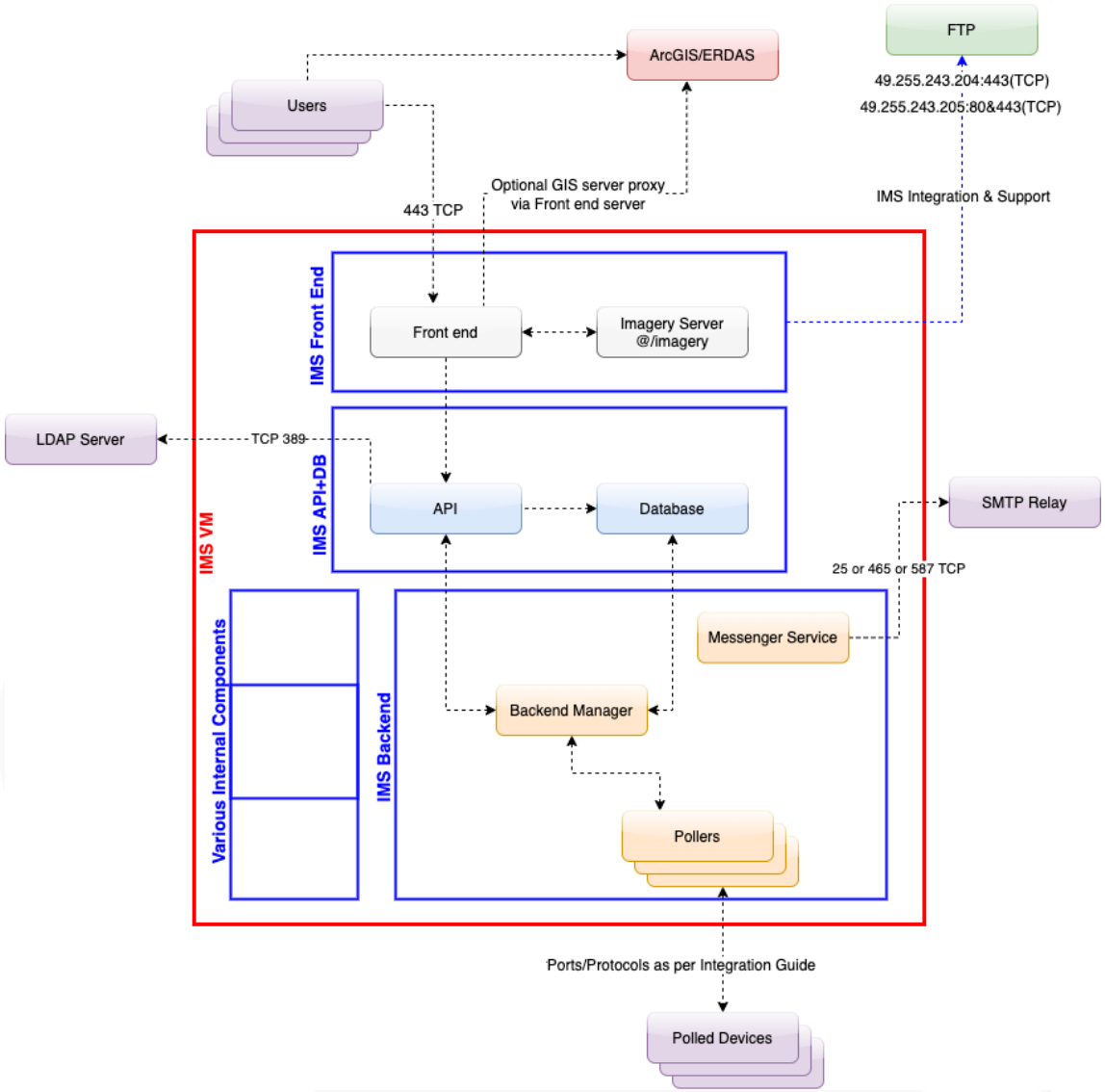
7. Annexure B – IMS Remote Access Architecture Overview



Level 10,
182 St Georges Terrace,
Perth, WA, 6000

otsc@ftpsolutions.com.au
+61 8 6355 5281
ftpsolutions.com.au

8. Annexure C – IMS– Single VM Traffic Flows

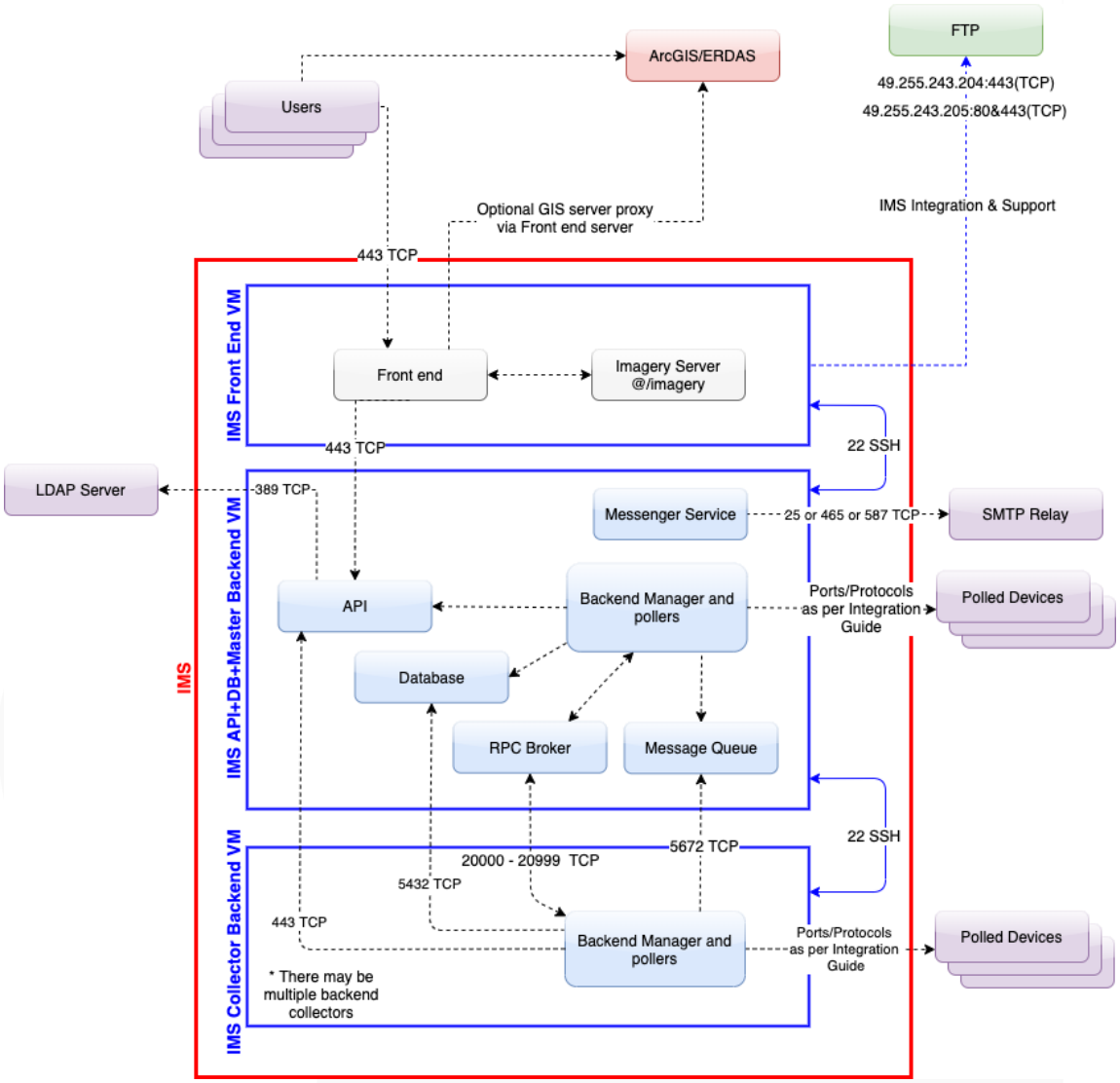


Note: *Any part within the red square is internal to the IMS application. MS SQL for example, is not compatible or needed.*

Level 10,
182 St Georges Terrace,
Perth, WA, 6000

otsc@ftpsolutions.com.au
+61 8 6355 5281
ftpsolutions.com.au

9. Annexure D – IMS Distributed Installation – Traffic Initiation – Ports



Note: *Any part within the red square is internal to the IMS application. MS SQL for example, is not compatible or needed.*

Note: *FTP reserves the right to adjust the quoted IMS price if a distributed IMS installation is chosen.*

Level 10,

182 St Georges Terrace,

Perth, WA, 6000

otsc@ftpsolutions.com.au

+61 8 6355 5281

ftpsolutions.com.au

10. Annexure E – IMS Ports and Protocols

Back end:

Polling Engine	Port (Destination port of polled device unless otherwise specified)	Protocol
3DP e200 Hornet (server-side)	TCP 22	SSH
3DP e200 Hornet (client-side)	UDP 13339 in, UDP 13338 out	Custom UDP
AVI 9/8/3 series modems/routers	TCP 22	SSH
AVI CCMS	UDP 3337 in	Custom UDP
Aviat radio	UDP 161 and TCP 80	SNMP and HTTP
Axis Q-series camera	TCP 80/443	HTTP/S
Cambium PMP4xx microwave radio	UDP 161	SNMP
Cambium PTP6xx microwave radio	TCP 80/443	HTTP/S
Cambium PTP8xx microwave radio	UDP 161	SNMP
Cambium ePMP microwave radi	TCP 22	SSH
Cisco Wireless LAN Controller	TCP 22	SSH
Cisco 350 AP	UDP 161	SNMP
Cisco IR829 LTE UE	UDP 161	SNMP
Cisco switch	UDP 161	SNMP
Cisco wireless access point (nothing, data comes from WLC)	N/A	N/A
Cisco workgroup bridge (WGB)	UDP 161	SNMP
ESXi host	UDP 161	SNMP
Exalt microwave radio	UDP 161	SNMP
Extreme AP71xx access point	TCP 22	SSH
Extreme AP75xx access point	TCP 22	SSH
Extreme RFS Controller	TCP 22	SSH
Fluidmesh 4200 microwave radio	TCP 22 and UDP 161	SSH and SNMP
FTP TracBox (server-side)	TCP 80	HTTP/S
Generic SNMP / TFTP polling engine	UDP 161, TCP 69	SNMP, TFTP
Huawei AR-series router	UDP 161	SNMP
Hyper-V Host	UDP 161	SNMP
Komatsu FrontRunner via CCMS	UDP 3338 in	Custom UDP
Linux System	TCP 22	SSH
MTGA Thumb GPS (server-side)	TCP 80	HTTP
Mikrotik RB-series microwave radio	UDP 161	SNMP
MineStar Fleet or Command FMS server	TCP 8080	HTTP

MineStar Terrain FMS server	TCP 1433	ODBC
MineStar TOPE NAM receiver	UDP 13337	Custom UDP
Motorola IAP access point	UDP 161	SNMP
Modular Dispatch 5/6	TCP 1433	ODBC
Modular ProVision 3.x	TCP 1433	ODBC
Moxa/Trimble GPS	TCP 4001	MODBUS over TCP/IP
Moxa N-port version information	TCP 23	Telnet
Nokia 7705 LTE UE	UDP 161	SNMP
OpenWrt wireless router (server-side)	TCP 22	SSH
OpenWrt wireless router (client-side)	UDP 13339 in, UDP 13338 out	Custom UDP
Other (nothing, ping-only polling)	ICMP	ICMP
RAD Airmux microwave radio	TCP 22, TCP 80/443	SSH, HTTP/S
Radwin 2xxx microwave radio	UDP 161	SNMP
Redline 3xxx microwave radio	UDP 161	SNMP
Redline 5xxx microwave radio	UDP 161	SNMP
SAF microwave radio	UDP 161	SNMP
Siklu Etherhaul microwave radio	TCP 80/443	HTTP/S
Sony IPELA camera	TCP 80	HTTP
Strix microwave radio	UDP 161	SNMP
TriStar MPPT	TCP 80 or TCP 502	HTTP or Modbus TCP
Ubiquiti AirOS microwave radio	TCP 22	SSH
Ubiquiti microwave radio with FTP Firmware	TCP 80/443	HTTP/S
Ubiquiti LiteStation 2	UDP 161	SNMP
Wenco FMS server	TCP 1433	ODBC
Windows servers	TCP 135 + random	WMI
Windows systems	TCP 135 + random	WMI

Note: *Not all polling engines are needed for each site, these ports are provided for guidance only*

***Note*:** For static WMI port config see here

11. Annexure F – Example Asset Register

	Asset Name (Must match FMS)	Asset Type	Child IP Device Name	Child IP Device Type	Child IP Device IP
2	DumpTruck1000	Dump Truck	DumpTruck1000 Radio	Cisco wireless client	10.200.10.10
3	DumpTruck1000	Dump Truck	DumpTruck1000 Onboard Device	Other device	10.200.10.11
4	Trailer1	Trailer	CiscoAP1	Cisco wireless access point	10.200.11.20
5			PMP1	Cambium PMP4xx device	10.200.11.21
6	Admin building	Building	WLC1	Cisco Wireless LAN controller	10.200.11.1
7			FMS Database	Linux server	10.10.10.10

This is an example image. FTP Solutions will provide a template Asset Register as a separate file.

Note: The idea is to list out all the devices that need to be monitored by IMS. FTP needs to be able to associate IP devices (e.g. radios) with assets (e.g. trucks) and know how to poll them (e.g. usernames/passwords/strings etc.). This also includes things like wireless controllers, databases, servers (WMI) etc. Please look at the Back-End polling engine tab le above for the correct username/polling credentials to provide.

12. Annexure G – IMS Roles and LDAP Overview

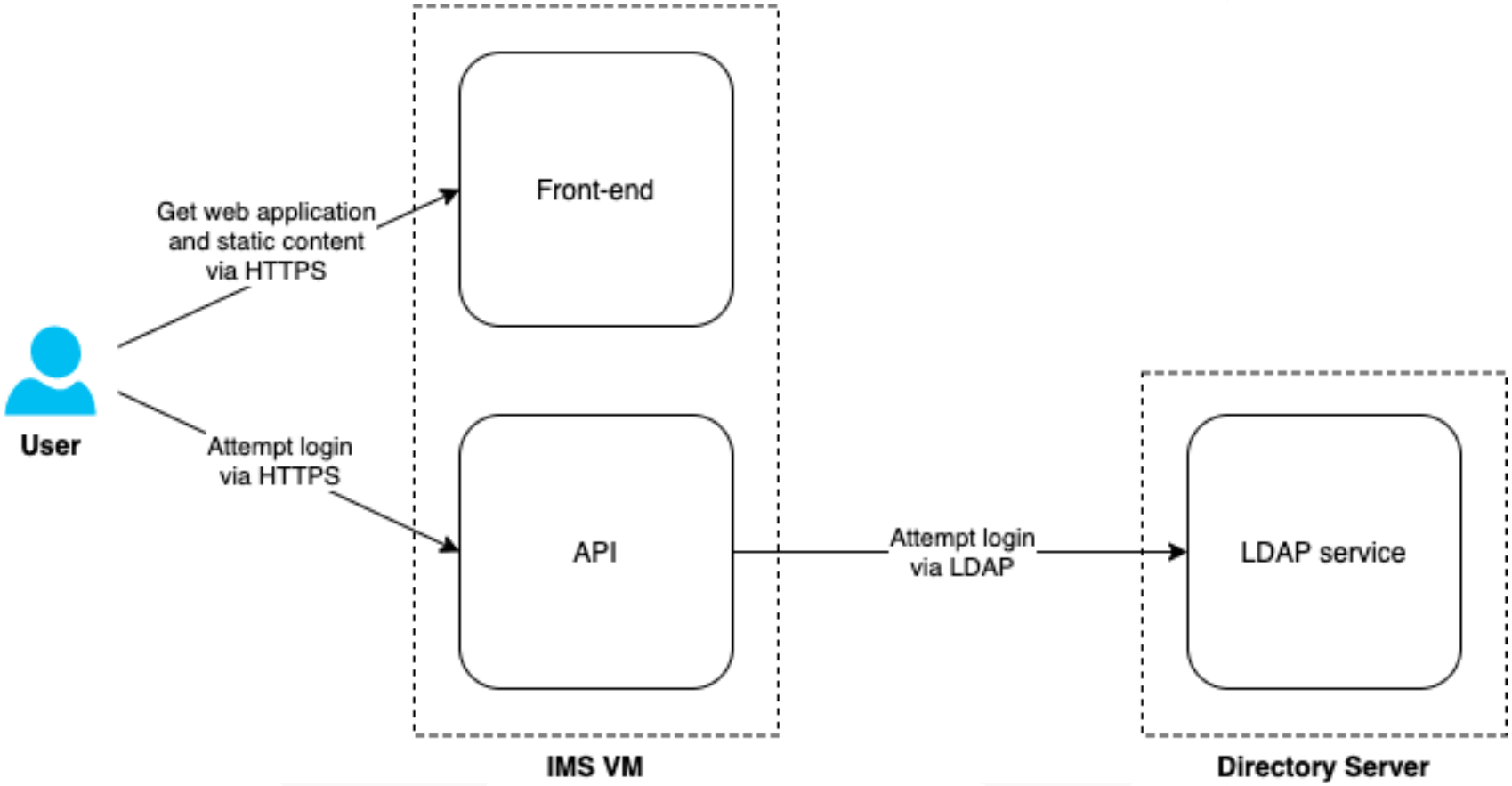
The IMS describes 3 roles; these roles may be used locally (with local users, defined in the IMS) or mapped to LDAP groups (recommended, not required):

- Read-only
- Read-write
- Manager

The table below describes the mapping of permissions to roles:

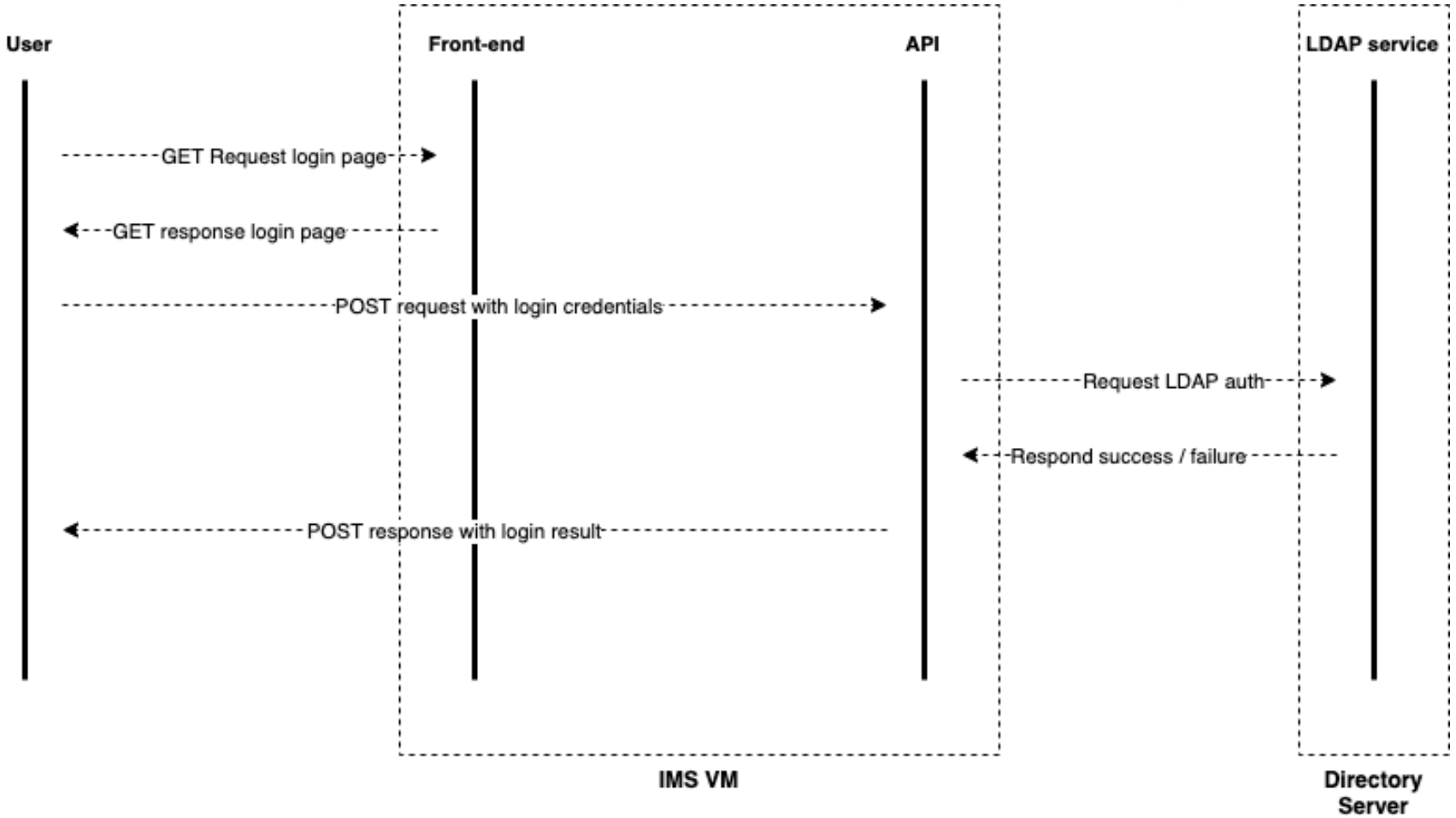
Permissions	**IMS Roles**		
	Read-only	Read-write	Manager
View everything			
Create / edit / delete dashboard tabs			
Create / edit / delete own reports			
Create / edit / delete tickets			
Create / edit / delete triggers			
Snooze / acknowledge alerts			
Create / edit / delete Assets, IP devices, Interfaces or Integrations (Manage tab)			
Create / edit / delete own comments			
Create / edit / delete Global RF plan			
Create / edit / delete own RF plans			
Create / edit / delete zones			
Create / edit / delete front-end configuration items (Admin tab, Configuration sub-tab)			
Create / edit / delete back-end configuration items (Admin tab, Systems Configuration sub-tab)			

The diagram below describes the interactions between the user, the deployed IMS services and the customer's LDAP service:



NOTE: In a distributed IMS configuration, the Front-end and API services may not be co-located on the same VM

The diagram below describes the login / authentication sequence:



NOTE: In a distributed IMS configuration, the front-end and API services may not be co-located on the same VM