IMS Integration Guide

Prepared for:

IMS Customers
15th March 2024

Document Details:
Version 1.15.x.2

The Ultimate Vantage Point

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	1.15.x.2
Version date	15/03/2024
Created by	Steven Brown
Approved by	Neale Williams

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

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

1. Version History

Version should be the current IMS release version without the increment (third digit) I.e. for IMS version 1.8.2, the IMS Integration Guide should have a version 1.8.X.

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
15/04/2021	1.12.0.1	Aaron Low	Updating for IMS 1.12.0
19/07/2022	1.12.0.2	Gary Boud	Reformatted document
17/04/2023	1.14	Michael Roberts	Updating for IMS 1.14
18/9/2023	1.15	Michael Roberts	Updating for IMS 1.15
15/3/2024	1.15	Aaron Low	Updating architecture diagrams

Contents

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

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

Please Note:

This document describes the requirements and guidelines to facilitate a successful deployment of IMS. This guide 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. IMS operates with a set of robust deployment tools that manage IMS versioning, system requirements, software requirements, system optimisation, backup, and rollback functionality. As part of IMS management remote access is required to the IMS server. These requirements are specified within this document. If the methodology of the described IMS remote access is a concern, due to network security or environmental challenges (especially in the likes of AHS environments), FTP will work with customers to provide an agreed alternate solution.

2. Document Intent

The Intent of this document is to provide clients with the information to achieve a successful deployment of FTPs Integrated Management System (IMS) at a customer's site.

The information presented provides a technical overview and architecture view of IMS and the steps and processes associated with the implementation of IMS.

3. Technical Overview

An overview of the IMS application architecture is depicted in the following diagram.

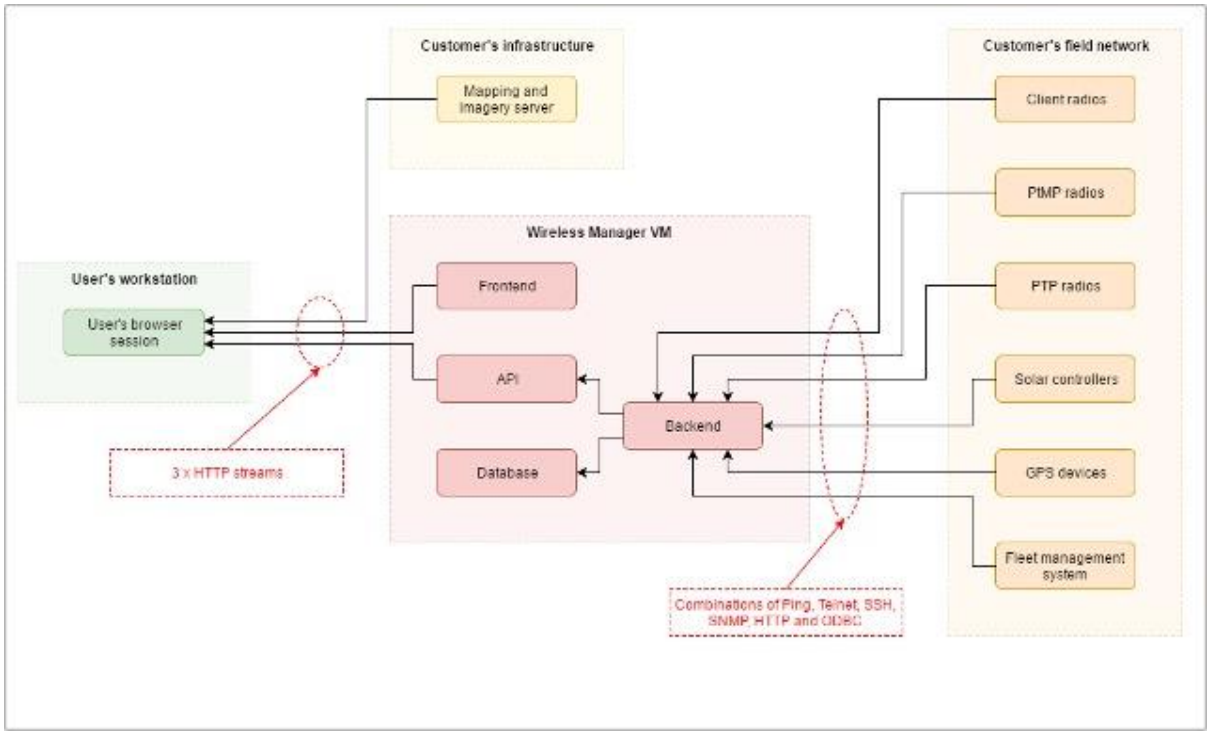


Figure 1 - IMS Application Overview

The IMS software operates on a virtual machine, either in a single or distributed instance (see section 4.2.1). The architecture components within the IMS comprise of:

- IMS Frontend
  - Nginx web server (SSL)
- IMS API
  - 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 – Collectors and Pollers
  - 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
    - Repository for the IMS data

In addition to the above IMS components the following are integrated within IMS:

- IMS message queue – integrates with the IMS Backend
    - Internal IMS message queue
    - Provides a message bus for inter-module communications
- IMS messenger service – integrates with the IMS Backend
    - Sends physical emails, alerts, reports, and other messages outbound
- IMS report generator
    - Responsible for creating reports utilising IMSQL
- IMS imagery – integrates with the IMS Frontend
    - 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
- 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 20.04 desktop/OSX 12/Windows 7 or newer
- CPU – 4 x 2GHz+ cores
- RAM – 8GB
- Storage – 80GB HDD
- Google Chrome 64-bit (latest version recommended)
- 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. IMS Server Environment

4.2.1. IMS Server Hardware Configurations

IMS configuration supports a single (centralised) and distributed VM deployment.

The IMS application is commonly installed on a single VM (See Appendix A – IMS Single VM Architecture for architecture overview). However, if there are client requirements to securely separate the Frontend from the Backend (with a firewall) or a large number of devices (~2500+) are to be polled by IMS, a distributed configuration would be recommended. IMS can be configured and installed in such a way that the IMS components,

specifically, the Frontend, API and Backend are installed on separate VMs (See Appendix B – IMS Distributed Architecture for architecture overview). Other Distributed architectures can be configured – contact FTP for details.

4.2.1.1. Single VM IMS Hardware Configuration

- OS:
  - Ubuntu LTS Server 20.04 or newer
    - https://www.ubuntu.com/download/server/thank-you?version=20.04&architecture=amd64
    - Ensure to select LVM when partitioning
    - Ensure SSH server module and access is enabled
- CPU:
  - 8 x 2.2GHz if < 150 Assets
  - 12 x 2.6GHz if between 150 & 300 Assets
  - 18 x 2.6GHz+ if >300 Assets
- RAM:
  - 16GB if < 150 Assets
  - 32GB if between 150 & 300 Assets
  - 64GB+ if > 300 Assets
- Storage:
  - A single drive can be provided. Linux LVM will be used to do further partitioning
  - Mounted at /srv
    - 500GB if < 150 Assets
    - 1TB if between 150 & 300 Assets
    - 2TB+ if >= 300 Assets
  - Mounted at /
    - 200 GB

**Numbers are not exact, testing and adjusting is required.*

4.2.1.2. Distributed IMS Hardware Configuration

- OS requirements
  - As for Single VM IMS installation
- Front-end VM
  - CPU:
    - 4 x 2.2GHz
  - RAM:
    - 8 GB
  - Storage:
    - Mounted at /
      - 100GB
- API + Database + Master backend VM

    - CPU
        - 8 x 2.2GHz if < 150 Assets
        - 12 x 2.6GHz if between 150 & 300 Assets
        - 18 x 2.6GHz+ if > 300 Assets
    - RAM
        - 16GB if < 150 Assets
        - 32GB if between 150 & 300 Assets
        - 64GB+ if > 300 Assets
    - Storage
        - A single drive can be provided. Linux LVM will be used to do further partitioning
        - Mounted at /srv
            - 500GB if < 150 Assets
            - 1TB if between 150 & 300 Assets
            - 2TB+ if > 300 Assets
        - Mounted at /
            - 200GB
- Backend collector VM
    - CPU
        - 8 x 2.2GHz if < 150 Assets being polled from this VM
        - 12 x 2.6GHz if between 150 & 300 Assets being polled from this VM
        - 18 x 2.6GHz+ if > 300 Assets being polled from this VM
    - RAM
        - 16GB if < 150 Assets being polled from this VM
        - 32GB if between 150 & 300 Assets being polled from this VM
        - 64GB+ if > 300 Assets being polled from this VM
    - Storage
        - A single drive can be provided. Linux LVM will be used to do further partitioning
        - Mounted at /
            - 150GB

**Numbers are not exact, testing and adjusting is required.*

4.2.1.3. 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 23.0.3 or newer

- bash
- htop
- telnet
- tcpdump
- snmpwalk
- nano
- vim
- curl
- wget
- nmap
- ssh and sshd
- python 3
- tar and gzip
- screen

4.2.2. 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. A list of ports and protocols is detailed in Appendix C – IMS Ports and Protocols.

4.2.1. IMS bandwidth

The IMS bandwidth requirement to the field is heavily dependent on the end points that are being monitored. It ranges from approximately 250bps to 3kbps averaged out over an 8 second polling cycle.

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 additional data 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.

5. IMS Deployment

The implementation of IMS at a client's site will include several phases. These phases include:

- Deployment Initiation.
- Pre-Deployment Activities.
- Deployment Activities; and
- Post-Deployment Activities.

5.1. Deployment Initiation

Once FTP Solutions has received a PO, implementation activities will begin, and the pre-deployment stage commences. A kick-off meeting will be scheduled to introduce the FTP deployment team, clarify any technical questions, and agree on schedule for the deployment plan.

5.2. Pre-deployment

The first stage of the IMS implementation is a Pre-deployment phase. This stage details the requirement inputs to enable a successful deployment of IMS. The following section describes the Pre-deployment phases.

5.2.1. IMS Deployment/Integration Team

Establish a team to support the implementation phase of IMS.

- Project manager
- Project contacts
    - Infrastructure
    - GIS personnel
    - Fleet management personnel
    - Network team

5.2.2. IMS Data Collection

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.

- Complete and return the Asset Register information, See Appendix D – Example Asset Register. The Asset Register will capture the following:
    - 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 assist with the IMS deployment.

5.2.3. IMS VM Build

- Build the IMS VM in line with the IMS VM configuration section.
    - Create 'ftpsolutions' user account.
        - Mandatory sudo rights
- Create service accounts for device polling.
    - IAW Appendix C – 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 Appendix C – 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 an NTP server.
- If DNS is used in the environment, ensure all IMS servers can connect to a DNS server.

5.2.4. IMS VM Access

To enable deployment of the IMS software, FTP requires access to the IMS VM. The FTP deployment server needs to be able to communicate using TCP/IP directly with the IMS VM that is being integrated. The recommended method to enable remote access 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.

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

- https://licensing-heartbeat.ftpsolutions.com.au 443 (103.186.242.4)(TCP) for IMS app support/IMS app updates/Integration.

The following diagram illustrates the IMS remote access architecture overview.

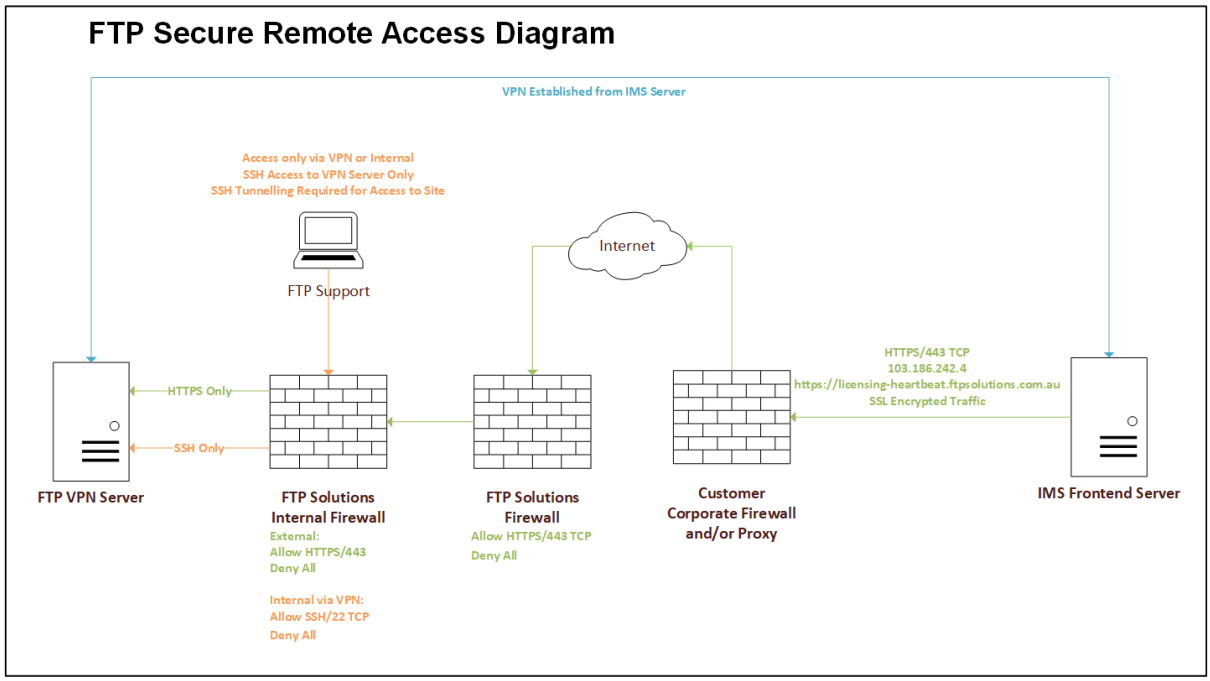


Figure 2 - IMS Remote Access Architecture Overview

5.3. Deployment

Once the Pre-Deployment phase has been completed the implementation of IMS can commence. 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 required. If the site has any technology that IMS does not currently support, and the technology is in scope, new polling engines will be written.

5.4. Post-deployment

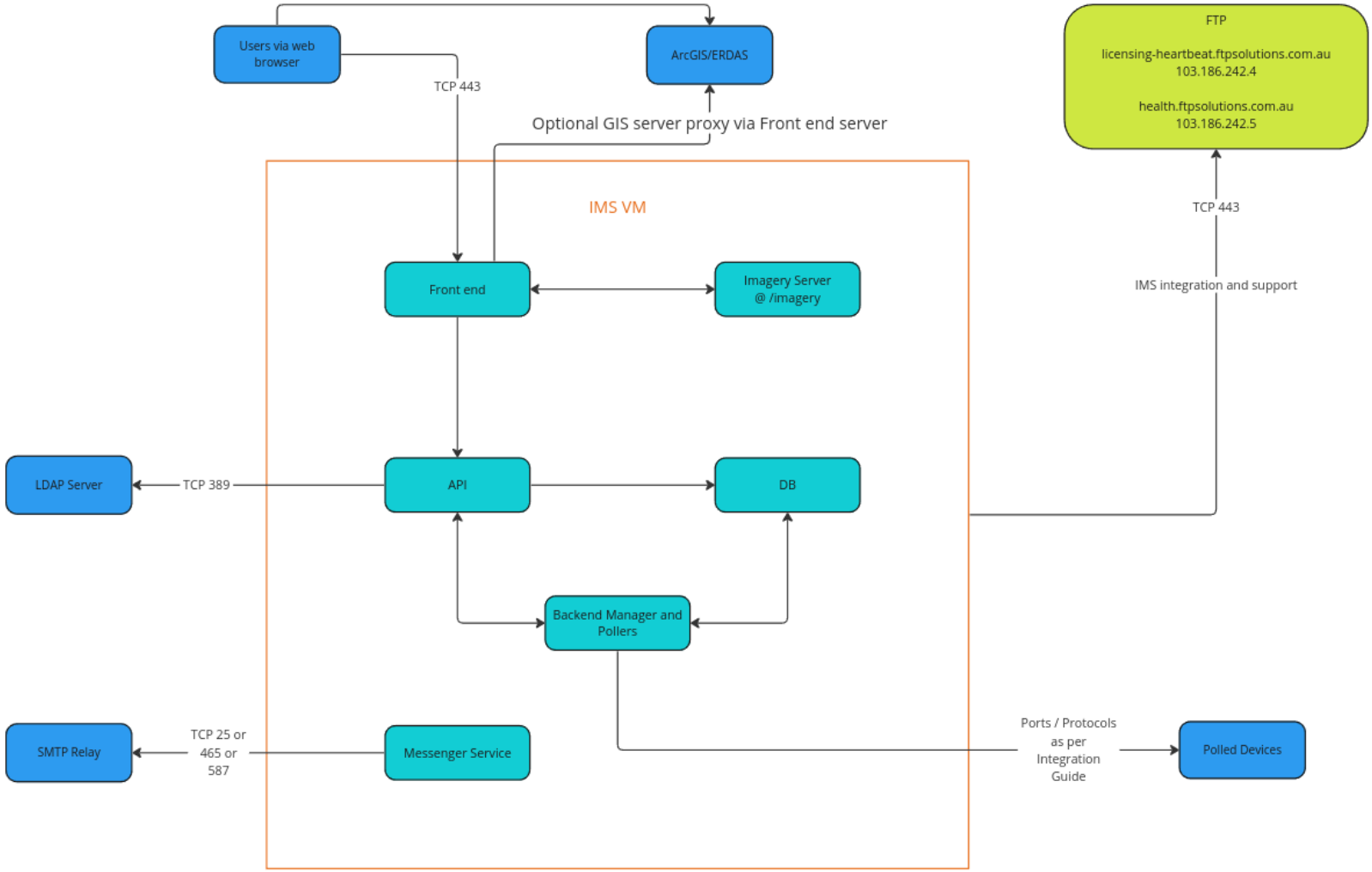
5.4.1. Training

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, 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.

5.4.2. Project Completion / Integration Sign-Off

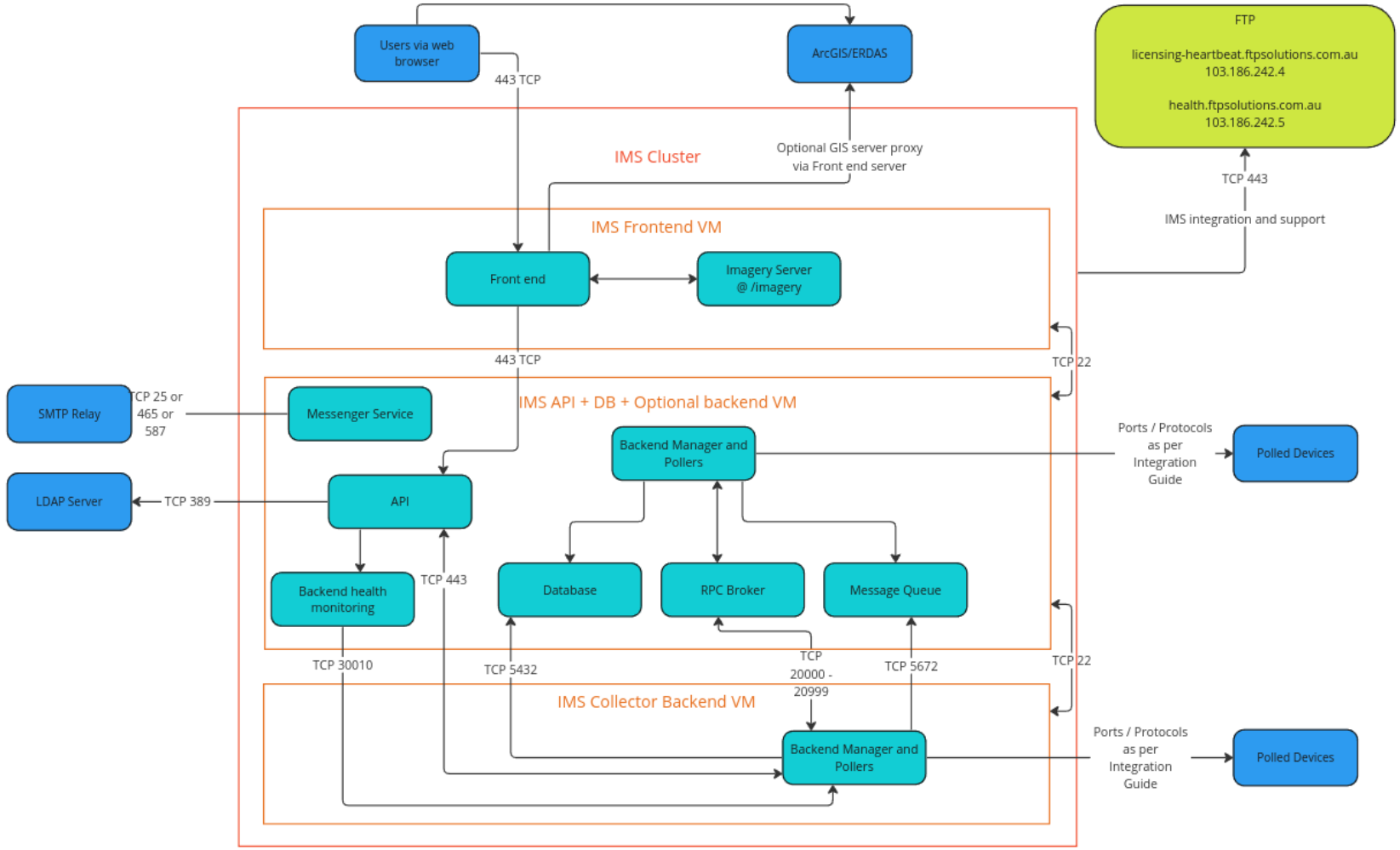
Once the software has been integrated and accepted by the client, invoicing will follow. Training will be conducted outside of integration on a separate PO.

Appendix A – IMS Single VM Architecture



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

Appendix B – IMS Distributed Architecture



*Other Distributed architectures can be configured – contact FTP for details.

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

6. Appendix C – IMS Ports and Protocols

Back end:

Current details of IP Device Types, System Types and Dynamic Schemas are regularly published to:
https://ftpsolutions.helpjuice.com/questions/1862724-raw-ip-device-types-system-types-dynamic-stat-schemas-csvs-and-jsons

Polling Engine	Port (Destination port of polled device unless otherwise specified)	Protocol
3DP Hornet polling instance	22	TCP - SSH
3DP Osprey polling instance	80	TCP - HTTP
Acksys polling instance	22	TCP - SSH
Allen-Bradley PLC version polling instance	80	TCP - HTTP
AVI UE event receiver instance		UDP - Custom
AVI UE SSH polling instance	22	TCP - SSH
AVI UE statistic receiver instance		UDP - Custom
Aviat polling instance	161	UDP - SNMP
Axis camera version and configuration polling instance	80	TCP - HTTP
Azure IoTHub server polling instance	1433	TCP - MSSQL
B+B SmartWorx VLinx ethernet-serial server version polling instance	80	TCP - HTTP
BCAPI polling instance	2300	TCP - BCAPI
Bosch camera version and configuration polling instance	80	TCP - HTTP
Cambium ePMP polling instance	22	TCP - SSH
Cambium PMP4xx SNMP polling instance	161	UDP - SNMP
Cambium PTP600 polling instance	80	TCP - HTTP

Cambium PTP800 polling instance	161	UDP - SNMP
Cambium PTP820 polling instance	161	UDP - SNMP
CAT JHM Data Gatherer	20041	TCP - HTTP
CAT MineStar Datashare FMS API polling instance	80	TCP - HTTP
CAT MineStar DB polling instance	1433	TCP - MSSQL
CAT MineStar Terrain FMS DB polling instance	1433	TCP - MSSQL
CAT MineStar Underground Cycle polling instance	80	TCP - HTTP
CAT Network Access Monitor receiver instance		UDP - Custom
Caterpillar HIM Polling Instance	80	TCP - HTTP
Cisco BR350 HTTP polling instance	80	TCP - HTTP
Cisco BR350 SNMP polling instance	161	UDP - SNMP
Cisco Catalyst 9800 SNMP polling instance	161	UDP - SNMP
Cisco Catalyst 9800 SSH polling instance	22	TCP - SSH
Cisco IR-series polling instance	161	UDP - SNMP
Cisco switch polling instance	161	UDP - SNMP
Cisco WGB polling instance	161	UDP - SNMP
Cisco WLC SNMP polling instance	161	UDP - SNMP
Cisco WLC SSH polling instance	22	TCP - SSH
Decawave RTLS polling instance	1883	TCP - MQTT
Deepsea DSE892 Polling Instance	161	UDP - SNMP
Eaton EFX48 UPS	161	UDP - SNMP
Eaton Matrix Inverter Controller	161	UDP - SNMP
Eaton SC 200 and 300 Polling Instance	161	UDP - SNMP
EFOY EMI Fuel Cell polling instance	80	TCP - HTTP

EFOY Hornet Fuel Cell polling instance	80	TCP - HTTP
EFOY TBox Fuel Cell polling instance	80	TCP - HTTP
Eltek Compack	161	UDP - SNMP
Eltek Smartpack	161	UDP - SNMP
Ensol EMI v2 polling instance	80	TCP - HTTP
Epiroc Surface Manager FMS DB polling instance	1433	TCP - MSSQL
Exalt polling instance	161	UDP - SNMP
Fluidmesh 4200 polling Instance	161, 22	UDP - SNMP, TCP - SSH
Fluidmesh 4500 polling Instance	161, 22	UDP - SNMP, TCP - SSH
Fortinet Fortigate 60F-3G4G polling instance	161	UDP - SNMP
FrontRunner SQL Event Manager	1433	TCP - MSSQL
FTP IoTBox polling instance	1883	TCP - MQTT
FTP TracBox polling instance	80	TCP - HTTP
Generic MQTT Stat Mapper integration	1883	TCP - MQTT
Huawei Agile Gateway polling instance	161	UDP - SNMP
Huawei CE-series switch polling instance	161	UDP - SNMP
Huawei eSight alarm receiver instance	80	TCP - HTTP
Huawei ETP48200 polling instance	161	UDP - SNMP
Huawei HiLink E3372 polling instance	80	TCP - HTTP
ICT240DB-8IRC polling instance	161	UDP - SNMP
IMS Agent receiver instance	80	TCP - HTTP
IMS Farm Simulator integration	80	TCP - HTTP
IoTBox Stat Mapper instance	4222	TCP - NATS
ISS polling instance	80	TCP - HTTP

JSON HTTP API location source polling instance	80	TCP - HTTP
Komatsu FrontRunner API location polling instance	80	TCP - HTTP
Leica FMS DB polling instance	5432	TCP - PostgreSQL
Linux server health polling instance	22	TCP - SSH
Linux server network polling instance	22	TCP - SSH
Linux server version polling instance	22	TCP - SSH
MAS GPS polling instance	80	TCP - HTTP
Microsoft WMI polling instance	135	TCP - WMI
Mikrotik RouterBoard polling instance	161	UDP - SNMP
Minetec MineOffice API location polling instance	80	TCP - HTTP
Minetec VPC	22	TCP - SSH
Modular Dispatch 5 Load Stat polling instance	1433	TCP - MSSQL
Modular FMS DB polling instance	1433	TCP - MSSQL
Motorola MeshConnex polling instance	22	TCP - SSH
Motorola MotoMesh polling instance	161	UDP - SNMP
Moxa AWK polling instance	161	UDP - SNMP
Moxa N-port version polling instance	23	TCP - Telnet
MSSQL database location source polling instance	1433	TCP - MSSQL
MST Impact WAP	80	TCP - HTTP
MTGA Thumb GPS polling instance	80	TCP - HTTP
NEC iPASOLINK polling instance	161	UDP - SNMP
NetModule NB1601 polling instance	161, 22	UDP - SNMP, TCP - SSH
Nokia 7705 polling instance	161	UDP - SNMP
Nokia FW2Series polling instance	80	TCP - HTTP

Norsonic Nor145 measurement API polling instance		TCP - Custom
Norsonic Nor145 recording FTP downloader instance	21	TCP - FTP
OpenSky API polling instance	80	TCP - HTTP
OpenWeather API polling instance	80	TCP - HTTP
OpenWrt polling instance	22	TCP - SSH
Oracle database location source polling instance	1521	TCP - Oracle
Ports Authority NSW API polling instance - Berth Metadata	80	TCP - HTTP
Ports Authority NSW API polling instance - Vessel Metadata	80	TCP - HTTP
Ports Authority NSW API polling instance - Vessel Movement	80	TCP - HTTP
Ports Authority NSW API polling instance - Vessel Position	80	TCP - HTTP
Ports Authority NSW API polling instance - Weather	80	TCP - HTTP
PostgreSQL database location source polling instance	5432	TCP - PostgreSQL
Radwin PTP/PtMP polling instance	161	UDP - SNMP
Redline RDL3000 Stat polling instance	161	UDP - SNMP
SAF Tehnika polling instance	161	UDP - SNMP
ScadaPack EFOY2400Midnite polling instance	502	TCP - Modbus
ScadaPack EFOY2400MPPT polling instance	502	TCP - Modbus
ScadaPack EFOY2800MPPT polling instance	502	TCP - Modbus
Siklu EtherHaul EH-710	161	UDP - SNMP
SNMP network polling instance	161	UDP - SNMP
SNMP trap receiver instance	162	UDP - SNMP
SNMP version polling instance	161	UDP - SNMP

Sprint Web Relay x410e	161	UDP - SNMP
Stratos Media location receiver instance	80	TCP - HTTP
Strix polling instance	161	UDP - SNMP
Syslog receiver instance		UDP - Custom
Telrad BreezeVIEW API receiver instance	80	TCP - HTTP
Telrad CPE12000 polling instance	161	UDP - SNMP
Trimble BX992 polling instance	80	TCP - HTTP
TriStar MPPT solar polling instance	502	TCP - Modbus
TriStar MPPT version polling instance	502	TCP - Modbus
Ubiquiti AirOS HTTP polling instance	80	TCP - HTTP
Ubiquiti AirOS SSH polling instance	22	TCP - SSH
Ubiquiti EdgeOS polling instance	161	UDP - SNMP
Ubiquiti HTTP stats scraper	80	TCP - HTTP
Ubiquiti LiteStation2 polling instance	161, 22	UDP - SNMP, TCP - SSH
Victron Energy system (deprecated)	22	TCP - SSH
VM host polling instance	161	UDP - SNMP
Wenco FMS DB polling instance	1433	TCP - MSSQL
WMI Version polling instance	135	TCP - 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

7. Appendix D – 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 Backend polling engine tab le above for the correct username/polling credentials to provide.

8. Appendix E – 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):

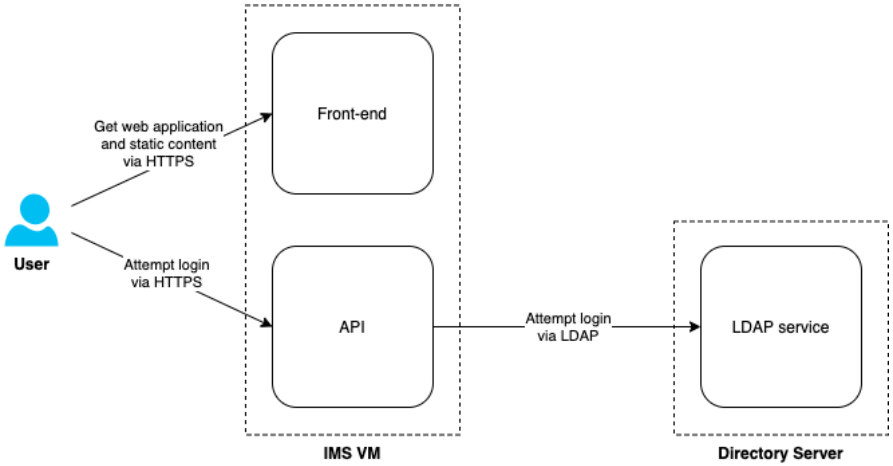
- Read-only
- Read-write
- Manager

The permissions for the Read-write role can be configured to suit a particular permission scheme. Read-only and Manager role permissions are fixed.

The table below describes the default mapping of permissions to roles:

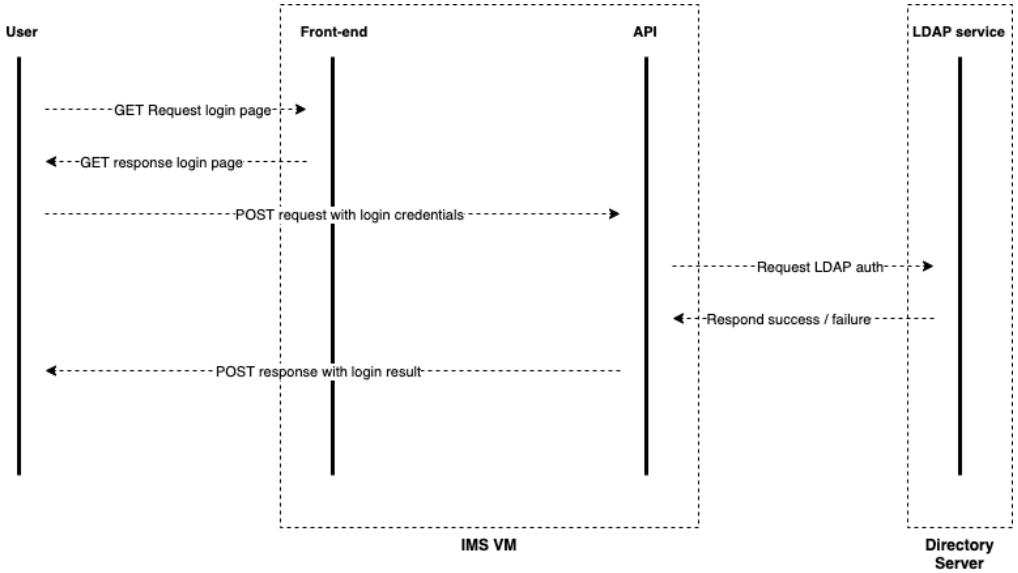
Permissions	IMS Roles		
	Read-only	Read-write	Manager
View everything			
Create / edit / delete dashboard tabs			
Create / edit / delete own reports			
Create / edit / delete tickets			
Create / edit / delete triggers			
Snooze / acknowledge alerts			
Create / edit / delete Assets, IP devices, Interfaces, 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 illustrates 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 illustrates 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.