Ports to Open to allow MM to operate in Secure Environments

Migration Manager must be able to connect to the internet in order to communicate with various services required by the product.

If a machine is located within a very secure network environment, some of these ports maybe blocked by default, preventing MM from functioning correctly. These must be opened by your IT Administrator.

⊗ Obviously if you are located in a temporary location like a Library, Airports, Hospitals etc, you won't be able to arrange for these ports to be opened. In these circumstances if accessing Migration Manager was critical you would need to tether the Laptop to your mobile phone to access Migration Manager.

* Using your Mobile Phone's data to connect Migration Manager can use substantial data.

1. URLs required to be open

The following URLs and Ports need to be open to validate the MM license, download updates, communicate with the Department etc

immi.gov.au:80, 443

*.immi.gov.au:80, 443 (e.g legend.immi.gov.au)

*.migrationmanager.com.au:80,443

migrationmanager.com.au:80,443

mmportal.com.au:80, 443

vpslb.migrationmanager.com.au: 80, 443

vetassess.com.au:80, 443

[**https://api.xero.com:**](https://api.xero.com) **443**

skillassess.com: 80, 443 (for VETASSESS)

afpnationalpolicechecks.converga.com.au: 80, 443 (for AFP check)

mmcpd.net.au:80, 443

mmcpd.com:80, 443

mmcpd.cloud: 80, 443

://api.raygun.com 443

mmportalapi.com 80, 443

mmquestionportalapi.com.au 80, 443

2. Ports open for Migration Manager Cloud clients

If you are a Cloud client and we are hosting your Migration Manager SQL Database on our Microsoft Azure SQL Cloud Server, then the following ports need to be open to be able to connect to the Database:

SQL Ports 1433, 1434 (in and out for TCP and UDP)