ANYWHERE

MEX Data Hosting FAQs

INFRASTRUCTURE + AVAILABILITY

Who provides the infrastructure services?
We utilise the Microsoft Azure platform.

What is your SLA's for uptime and recovery?
Guaranteed 99%

Is the Hosting environment located within Australia?
Yes, all our components that make up the Hosting environment are located within the Australia East *(Sydney)* and Australia South East *(Melbourne)* Regions.

Is the service provided internationally?
Yes, MEX has servers located within Australia as the primary default location, with others located within US and Europe. Services can be created/operated from within any location that Microsoft offers.

Here is a link to available **Azure international data centres**. Do note that additional charges will be applied to these centres.

What is a typical access link for a hosted customer?
All hosted customers are given a unique link based off their company name and using a sub-domain of the MEX main domain. For example, ***ABC Maintenance*** would get ***abcmaintenance.mex.com.au*** as a link to their live system.

Is the environment hosted on a shared or dedicated server?
Hosting offers two options: A Shared server with a maximum of 50 customers on each box or a dedicated server with customer specific server and security settings applied.

What are the current shared server specifications?
One of our shared servers would typically be running the following specifications:

- Intel Xeon Platinum 8272CL CPU @ 2.60Ghz
- 8core CPU
- 32GB RAM
- Windows Server 2019 Datacentre
- SQL Server 2019 Enterprise

A dedicated server's specifications are customised to suit the customer's needs and are charged accordingly.

Do you have an Infrastructure Diagram available to view?
Yes, refer to the **MEX Data Hosting Network Diagram**.

Is the MEX database located on the web server or a separate database server?
All of the components that make up the MEX application are installed on the same server. Including the web files and SQL Server components.

Is a test environment available?
Yes, what better way to experience the MEX Hosted system than to try it out for yourself. MEX offers a full trial of the hosted system. Using your own data, our test environment can be set up to meet your needs. Allowing you to test the service with ease allowing the tester to make an informed decision on whether or not the MEX Hosted service is right for them.

Azure

With MEX Data Hosting We Guarantee 99% Uptime

We utilise the industry leader's solution of Microsoft Azure to ensure your database is hosted with the upmost flexibility and security!

ANYWHERE

MEX Data Hosting FAQs

NETWORK

How is the network secured?

The Hosting network is secured by installing and maintaining Azure's industry-standard firewall configurations to protect data, and MEX avoids the use of vendor-supplied passwords and other security defaults.

Is the data encrypted in transit between the client browser and web server?

By default, all MEX Hosted sites are set up with HTTPS. If you do require the HTTP site link, we can also provide this, but is not recommended for security reasons. No additional encryption is applied.

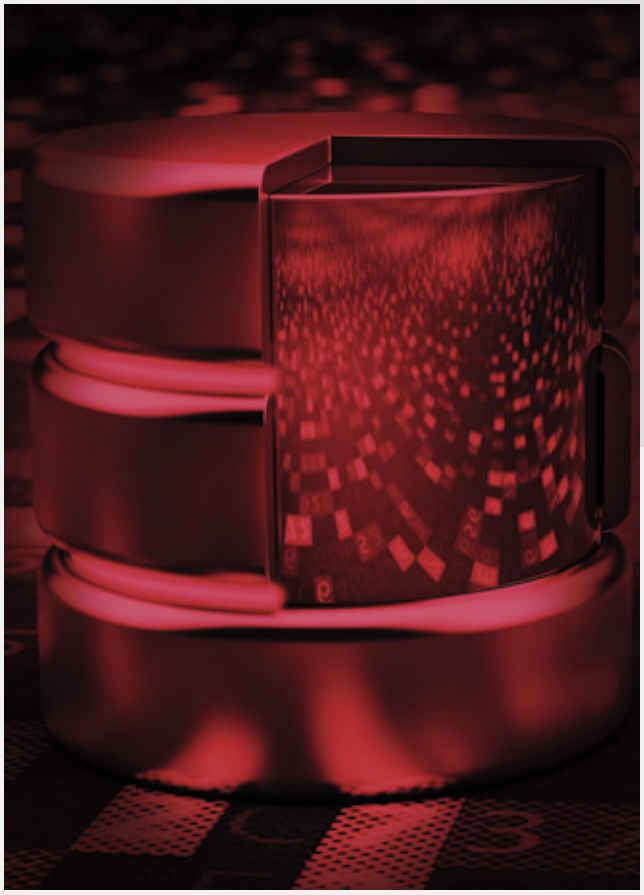
Are all default ports blocked/disabled?

By default, we enable Port 80 (HTTP), Port 443 (HTTPS) and RDP Port (this is only accessible from within the MEX Network). HTTP connections are enabled as they are required to force all connections to HTTPS via redirecting, which is also enabled by default.

All SQL Ports are disabled by default, should there be a need for any of these ports, MEX Data Hosting admins will need to be consulted.

Are load balancers implemented in order to control data traffic, protect the web infrastructure and manage certificates?

No, Load balancers aren't in use. The access to each server is controlled by DNS rules and all traffic for each customer is directed to the appropriate server. However, each server is replicated to a secondary datacentre, ready to failover if required.



What mechanisms do you have in place to protect infrastructure and applications from cyber threats (i.e. Anti-Virus, Host Intrusion, Personal Firewall, etc)?

As the MEX Hosted service uses the Azure platform, all servers are secured through Microsoft's industry leading security infrastructure and firewalls including:

- Disk encryption using the BitLocker feature
- Industry-standard monitoring products
- Microsoft Antimalware Software that helps to identify & remove viruses, spyware & other malicious software.

MEX Makes It Simple

ANYWHERE

MEX Data Hosting FAQs

BACKUP

Are backups in place? If so, how often are backups taken and kept?

Full server backups occur daily and are kept in a secure vault for 30 days before being overwritten.

Can the customer have an influence on the time and scope of the data backup? To what extent?

Customers can request to have separate backup schedules set up on the hosted service. This is dictated by what server your system is hosted on and will come at an extra cost.

Is encryption used to protect data at rest (db, files, backup media)? What type of encryption method is used?

Yes, all backups are encrypted within the backup vault using Storage Service Encryption (SSE).

All backups are encrypted in a vault using Storage Service Encryption (SSE)

DISASTER RECOVERY + REDUNDANCY

What level of redundancy do you have on the hosted server?

Full server replication occurs in real-time to a secondary data center, this copies over the entire system including databases and web files. From a Recovery Point Objective (RPO), this real time replication will give our customers the ability to continue to use the system after a disaster with the most up to date data available.

How often is the redundancy configuration tested?

Every 6 months a live failover test is conducted on the MEX Hosted Service. This test is carried out at off peak times allowing for our administrators to ensure that redundancies will work when we call upon them.

What is the Recovery Time Objective (RTO)?

In the event of a sudden loss of service, MEX aims to have customers back up and running in 1 hour.

ANYWHERE
MEX Data Hosting FAQs

ADMINISTRATION + MONITORING

Is there 24/7 monitoring of the availability of infrastructure for services and resources?
The MEX Hosted platform is monitored around the clock with a number of different surveillance approaches used to ensure the system is up and running as it should. Our admins use an internal application that allows for the responsive management of all servers wherever required. We also utilise the built in Azure resource monitoring to provide real-time resource usage/history. On top of that we also utilise a third-party service that pings the servers and alerts as soon as they are unresponsive.

Is there a dedicated team or individual who manages the Hosting Infrastructure, including patch management?
Yes, the MEX Cloud Administrators are responsible for the Hosting Platform and performing system updates.

What is the process for notifying customers when an unexpected and planned outage occurs?
The Hosting status page will be updated prior (if planned), during and after an outage has occurred. This is also accompanied by an alert email in most cases. Phone and/or email support will be available by the MEX Support Team. For example our hosting box 1:
https://www.mex.com.au/Services/DataHostingStatus/hosting-box-1

SECURITY

What procedures are in place for monitoring/reviewing security?
We monitor the servers manually, performing specific checks each day. In addition to this, we utilise the MS Azure Security alerts and recommendations.

Is the MEX Hosting Service Azure Protected or Azure Classified?
Azure has been certified for both Unclassified: Dissemination Limiting Markers (DLM) and PROTECTED data.

Do you support Single Sign On integration? i.e SAML, WS Federation, AzureAD etc.
Yes, the MEX application allows customers to specify an Identity Provider (such as ADFS) that MEX 15 can authenticate against, utilising your choice of either WS-Federation or SAML 2.0 protocols. This option can be setup on request on the MEX Hosted platform.

The MEX Hosting Platform is monitored around the clock with intensive surveillance

Does scheduled Penetration Testing occur?
Yes, we perform a yearly Penetration Test (PenTest) through an accredited third-party PenTest specialist. The results of these tests used to secure not just the MEX Hosted platform but also the MEX application. The last PenTest was conducted in February 2021.

Is it possible to carry out pre-announced penetration tests of the platform?

Yes, a pre-announced test is possible and will need to be organised through the MEX Data Hosting administration team. Additional costs will be charged for such a test to be conducted.

Is a user management process established?
Yes - Each server has one user account. There are only two cloud admins at MEX who access these servers.

Does MEX have any ownership over the data stored on the Hosting Infrastructure?
No, all data entered within the MEX database and/or uploaded to the Hosting platform is owned by the company utilising the application as detailed in the MEX Terms & Conditions.