# SQL Azure Secrets

Last updated by | Subbu Kandhaswamy | Jan 20, 2022 at 8:11 AM PST

Contents



## Azure Internal Information

Please do not disclose internal details about SQL Database to customers. This includes the following types of information (but is not intended to be an exclusive list):

- Number of machines in the datacenter
- Specs (CPUs, memory, disks, ...) on the machines
- Machine names
- Internal IP Addresses
- SQL errorlogs
- Number of instances on a Node
- Internal tools output
- Performance Pool (SLO) internal details
- Internal project names like SAWA, Sterling,Malmo etc.
  When in doubt, ask our leaders at SQL ST Cloud WASD Leads to get and okay before sending SQL Azure datacenter details in email or on customer visible troubleshooting logs.

## Use of Customer Credentials

- Microsoft personnel, agents, and contingent staff are prohibited from using accounts to troubleshoot issues on behalf of customers! You should never solicit the use of customer credentials to troubleshoot an issue on their behalf. If a customer provides you an account to troubleshoot on their behalf, you should decline and you can state it is against Microsoft policy to do so.
- If you ever receive credentials from a customer, you should delete them from your email and request deletion from all support systems (e.g., CAP/MSSOLVE). You should also request that the customer delete the credentials that were sent to you.
- Microsoft personnel, agents and contingent staff must never share their individual user account or password with anyone and must never allow another person to use their account, even if that other person is a Microsoft agent or engineer! Account IDs and passwords should never be written down or stored in a fashion in which they can be disclosed or accessed.

- There is no distinction between a test or production environment - use of customer credentials by Microsoft personnel, agents or contingent staff in either environment is prohibited!

- You can use a remote access tool like LogMeIn to access a customer's system, with the customer typing in their credentials, however, you should always follow the remote access rules and procedures. In addition, if support is being provided for a cloud services, the operations team may be able to access the account on the backend without using customer's credentials.

**How good have you found this content?**