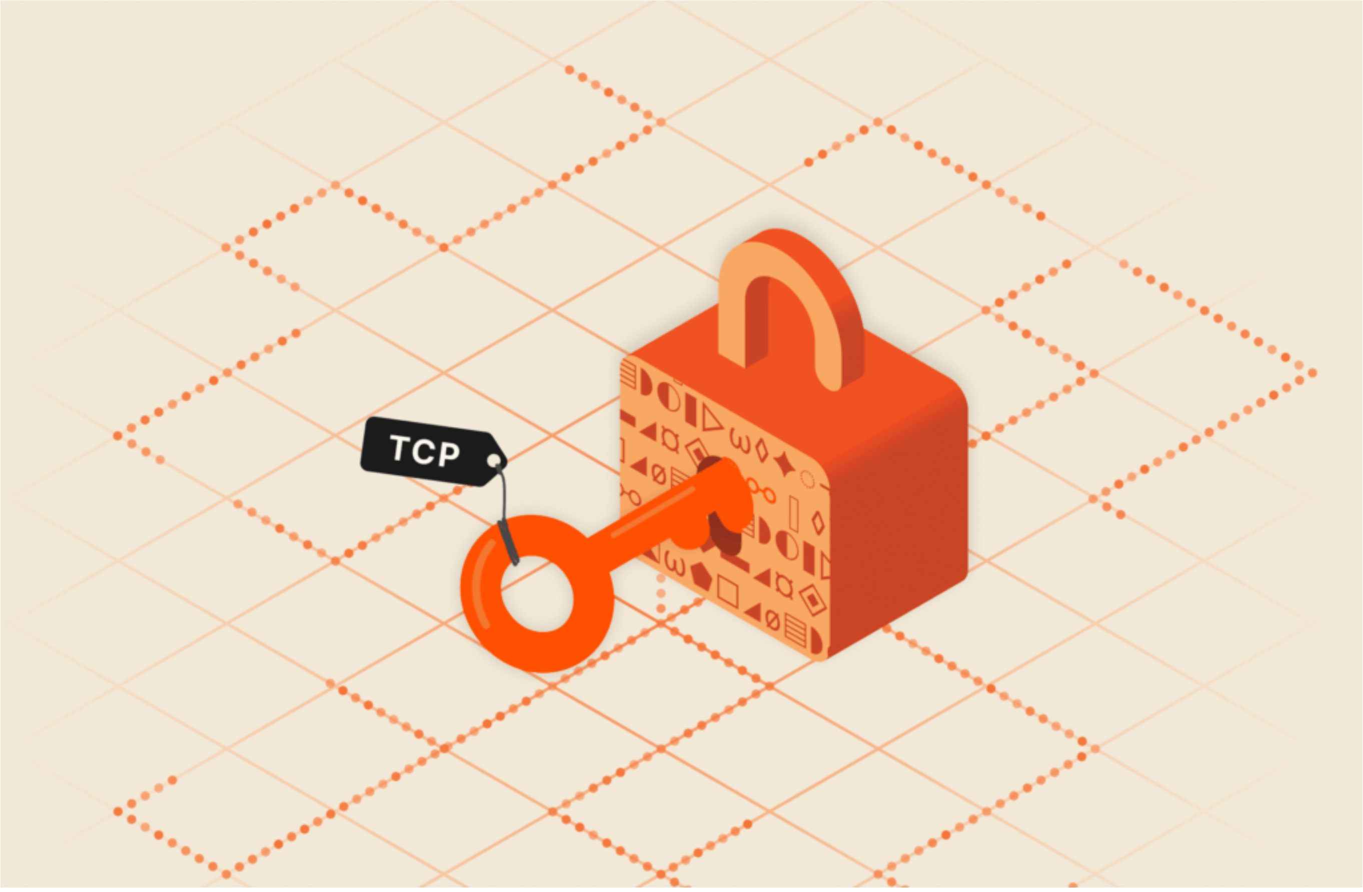
LDAPS Port Number: TCP 636



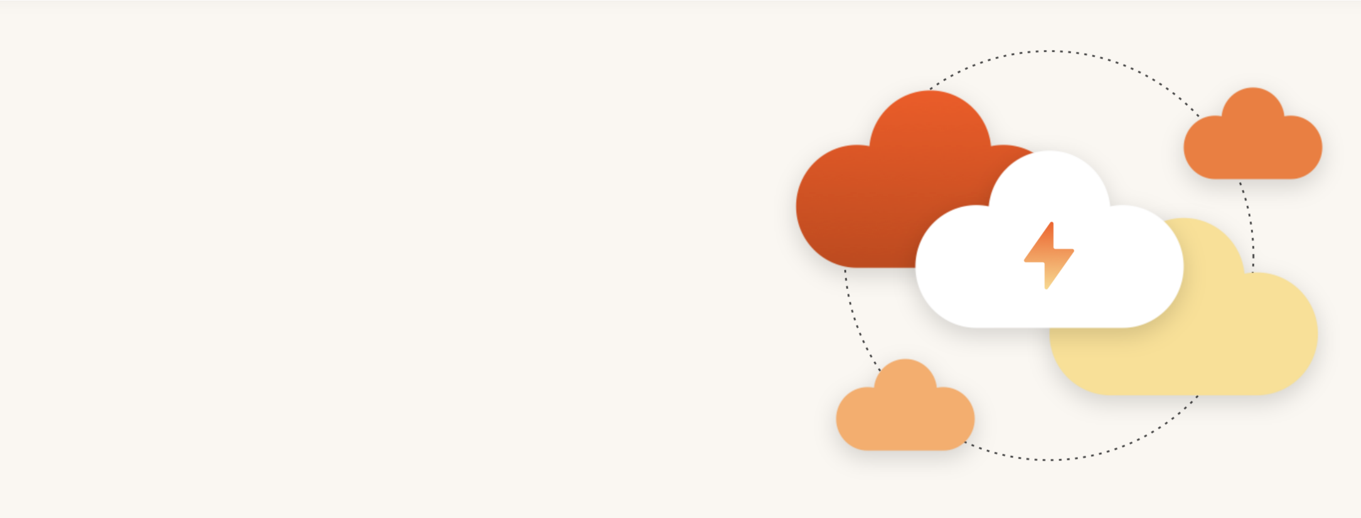
If you have LDAPS deployed on your network, you can install it with the default port or use an alternative port for queries. The default port allocated for LDAPS is the encrypted port 636, but administrators can use the alternative unencrypted port 389 for cleartext queries.

What Is LDAPS?

Lightweight directory access protocol over SSL (LDAPS) is a vendor-neutral method for connecting computers and network resources. As with any other network service, LDAPS runs on an open port for computers and network infrastructure to query for information. When a user needs to connect to a service on the network (e.g., an email server or a printer), the workstation queries the LDAPS directory to get information about the service to then connect to it. To connect to the LDAPS directory, a workstation connects using the configured port. The default port for LDAPS is 636.

What Protocol Does LDAPS Usually Use?

LDAP itself is a protocol, but the "S" in the acronym stands for Secure Socket Layer (SSL). Microsoft supports LDAPS queries on UDP, but it's usually configured to use TCP. UDP is a "send and forget" method for sending messages without validating that it was successful. TCP, however, is a connection-oriented protocol that ensures data is sent and received before releasing the connection. UDP is faster but less reliable, and TCP takes time for a connection but validates data transmission. Administrators can use either protocol, but TCP is the most commonly used protocol.



Why Do Protocols Have Default Ports?

Protocols need at least one port to establish data transmission between sender and receiver, and the default is usually the most common and set up during installation. The sender uses a port to send data, and the receiver listens on a configured port. Ports allow computers to differentiate between types of communications. Administrators can close ports to stop communication and secure a computer.

Computers have port numbers 0 to 65,535 available. The Internet Assigned Numbers Authority (IANA) assigns default ports, but an application can configure any port when it installs on a computer. Port numbers 0 to 1023 are reserved for well-known protocols, and ports 1024 to 49151 are reserved for developers to configure their custom applications. Only one protocol can be configured on each port.

What Is the Default LDAPS Port Number?

Administrators can choose from two ports when configuring LDAPS. The default port is 636, which means that if you don't configure LDAPS to use a specific port, the installation process assigns 636 automatically. The 636 port is encrypted, so traffic between workstations and the LDAPS server is encrypted and cannot be read if an attacker eavesdrops on the network.

The alternative port is 389. The 389 port uses TLS, which is an upgraded version of SSL, but there is a caveat: The connection is unencrypted and then can be encrypted with TLS. It's the more insecure of the two options, but you may have situations where you need cleartext querying. For example, if you integrate it with Active Directory, you need port 389 opened.

LDAPS supports both TCP and UDP, and TCP is the common protocol for querying. Microsoft Active Directory requires both TCP and UDP, so again, if you have a Windows domain server with Active Directory activated, you'll need both protocols.

Oracle Database as a Service Products and LDAPS

When you use several proprietary services on your network, LDAPS makes it easier to integrate different environments. Oracle in a Windows network environment is one example of when LDAPS is beneficial. Instead of requiring users to authenticate into multiple environments, LDAPS can be used to catalog multiple services across different servers and networks—Oracle included.

When you have an Oracle Database as a Service (DBaaS) server in the cloud, you can integrate your local user accounts with your cloud database environment with LDAPS. Oracle incorporates LDAPS into its Oracle Internet Directory (OID) service. You can incorporate OID into your DBaaS environment, and it will connect to the Oracle service and allow users to query it for information about services.

Recommendations for Administrators:

1. **Enable and Enforce LDAPS:** Ensure that all LDAP communications are conducted over SSL/TLS by configuring directory services to use LDAPS on port 636. This setup encrypts the data in transit, protecting it from potential interception.
2. **Update Client Applications:** Verify that all client applications interacting with directory services are configured to use LDAPS. This may involve updating connection strings and ensuring that the clients trust the server's SSL/TLS certificate.
3. **Implement Network Security Controls:** Configure firewalls and network security groups to allow traffic only on port 636 for LDAP communications. Additionally, consider restricting access to specific IP addresses to minimize exposure.
4. **Regularly Update and Patch Systems:** Keep all systems, especially those handling authentication and directory services, up-to-date with the latest security patches to protect against known vulnerabilities.

By adhering to these updated practices, organizations can significantly enhance the security of their directory services, ensuring that LDAP communications are protected against evolving threats.

Conclusion

If you want to integrate an Oracle database server in the cloud—or any DBaaS service—LDAPS makes it easier to integrate the database environment with any operating system environment. It will allow easier communication between network resources and user workstations. You can use either port, but c