# Saturn Studio — Credencial SQL Server



**SQL Server** es un motor de base de datos relacional de Microsoft, diseñado para gestionar volúmenes de información críticos con alta disponibilidad y seguridad. Para integrar este motor en sus flujos de trabajo, es imperativo configurar una credencial de conexión que actúe como el puente técnico entre el robot y el servidor.

## Obtención de Parámetros Técnicos

La información necesaria para establecer la conexión se encuentra centralizada en las herramientas de administración del servidor. Los datos presentados en su borrador han sido verificados y son técnicamente precisos según los estándares de Microsoft:

- **SQL Server Management Studio (SSMS):** Principal interfaz para identificar nombres de servidor y bases de datos.
- **SQL Server Configuration Manager:** Herramienta esencial para habilitar protocolos TCP/IP y verificar puertos activos.

## Parámetros de Configuración en el Módulo

Al registrar una nueva credencial, deberá completar los siguientes campos obligatorios y opcionales en la interfaz:

| Campo | Descripción Técnica | Formato de Ejemplo |
|---|---|---|
| **Server Address (*)** | Ubicación de red del servidor SQL. Puede ser IP, Hostname o Instancia. | 192.168.1.10 o SERVER\SQLEXPRESS |

| Campo | Descripción Técnica | Formato de Ejemplo |
| --- | --- | --- |
| **Port** | Canal de comunicación TCP. El valor estándar es **1433**. | 1433 |
| **User (*)** | Usuario con autenticación de SQL Server. Requiere **Modo Mixto** habilitado en el servidor. | db_robot_user |
| **Password (*)** | Contraseña del usuario de base de datos. | ******** |
| **Database** | Nombre del contenedor de datos. Si se omite, conecta a la base predeterminada (usualmente master). | Produccion_Ventas |

---

# Parámetros de Seguridad y Cifrado

El manejo de certificados y cifrado es crítico para el éxito de la conexión, especialmente en entornos corporativos o de nube:

### Encrypt Connection

Determina si el tráfico de datos entre el cliente y el servidor viaja cifrado mediante TLS.

- **True:** Habilita el cifrado. Si el servidor exige TLS y esta opción está apagada, la conexión fallará.
- **False:** Envía datos en texto plano (no recomendado para entornos fuera de una red local segura).

### Trust Server Certificate

Controla cómo se valida el certificado de seguridad del servidor.

- **True:** El cliente acepta el certificado del servidor sin validarlo contra una autoridad externa. Es común en desarrollo con certificados autofirmados.
- **False:** El cliente exige que el certificado sea emitido por una autoridad de confianza (CA). Es el estándar de seguridad para producción.

> **Regla Técnica:** La opción Trust Server Certificate solo entra en funcionamiento si Encrypt Connection está activo.

## Consideraciones de Red y Validación

Para asegurar que el comando de consulta funcione correctamente, verifique los siguientes puntos de infraestructura:

1. **Firewall:** El puerto **1433** debe permitir tráfico entrante y saliente, o bien, debe permitirse explícitamente el proceso sqlservr.exe.
2. **Conexiones Remotas:** Asegúrese de que SQL Server esté configurado para aceptar conexiones desde otras IPs (TCP/IP habilitado en Configuration Manager).
3. **Verificación Final:** Es obligatorio utilizar el botón **Test Connection**. Una prueba exitosa garantiza que el usuario tiene permisos de lectura/escritura y que el túnel de seguridad es compatible.

## Buenas Prácticas Generales

- **Principio de Menor Privilegio:** No utilice el usuario administrador sa. Cree un usuario dedicado con acceso exclusivo a las tablas que el robot necesita procesar.
- **Certificados en Producción:** En entornos críticos, evite el uso de Trust Server Certificate = True. Utilice certificados válidos para prevenir ataques de interceptación (MITM).
- **Puertos Estáticos:** Siempre que sea posible, especifique el puerto manualmente para evitar problemas de resolución en instancias con nombres dinámicos.