Devolutions

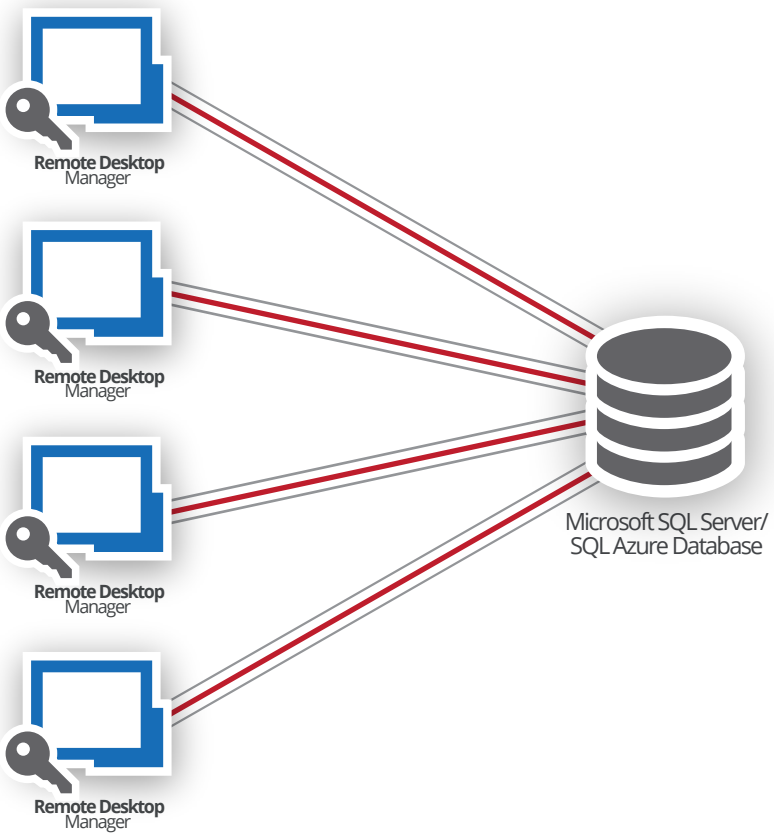
SECURITY MODEL AND ENCRYPTION

Devolutions

Security Model and Encryption

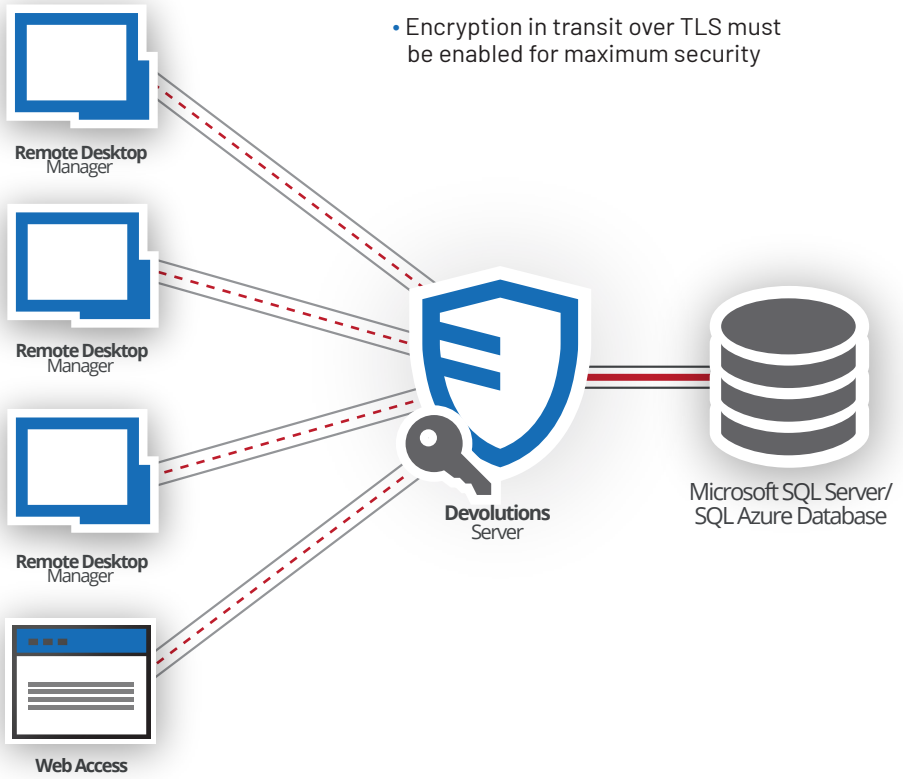
MULTI-USER Remote Desktop Manager

- Security Providers are used for encryption at rest
- Security Providers support passphrase and certificate secrets
- Clients must have network access to the database
- Data is protected using AES-256 with keys securely derived from Security Providers' secrets.
- Encryption in transit is optional



MULTI-USER Devolutions Server

- Encryption at rest is performed by DVLS server.
- Clients only need to have network access to DVLS
- Data is protected using secure XChachaPoly1305 encryption with key generated randomly on installation
- Custom user passwords are stored hashed using the secure key derivation function PBKDF2
- Encryption in transit over TLS must be enabled for maximum security



LEGEND : Encryption at Rest Encryption in Transit

FIPS 140-2 Annex A Compliance

Remote Desktop Manager 2022.1 and above

RDM complies with FIPS 140-2 Annex A Compliance approved security functions for local encryption, encryption in transit, and both RDP and SSH connections only if authentication mode is set to Application Password and underlying system is configured to use Windows FIPS-only cryptography. Other operating systems, authentication modes and connection entries are not supported for FIPS-only mode.

Unsupported connection entries shall be controlled and restricted server-side to remain compliant.

Data (in transit)

Using OS-supported FIPS Compliant algorithms

MSSQL (over TLS)
DVLS (over TLS)

Local Data

AES-256-CBC-HMAC-SHA-256 Encrypt-then-MAC

Configuration File
Offline Cache

Supported Entries

Using OS-supported FIPS Compliant algorithms
RDP
TLS

Requires manual service configuration client/server system*
SSH

*SSH Configuration for RDM's FIPS140-2 Compliance:
https://kb.devolutions.net/kb_ssh_configuration_rdm_fips140_2_compliance.html