Devolutions

Remote Desktop Manager Now Complies with FIPS 140-2 Annex A Approved Encryption Functions

TWE ARE PLEASED TO ANNOUNCE THAT THE LATEST EDITION OF REMOTE DESKTOP MANAGER 2022.1

We are pleased to announce that the latest edition of Remote Desktop Manager 2022.1 is now compliant with FIPS 140-2 Annex A approved encryption functions.

What Is FIPS 140-2 Annex A?

FIPS 140-2 is a well-known NIST standard that establishes security requirements for cryptographic modules in government agencies. The Annex A "Approved Security Functions for FIPS PUB 140-2" defines the list of approved security functions that are considered secure for highly sensitive environments. To ensure that Remote Desktop Manager complies with restrictions in these environments, we have aligned it with the standard's approved security functions for encryption at rest and in transit.

How to Enable FIPS-Only Mode

Remote Desktop Manager will automatically switch to FIPS-enabled mode on operating systems running Windows with enforced FIPS-only algorithms configuration, and if the authentication mode for Remote Desktop Manager is Application Password. Using entries that do not natively support FIPS-only approved security functions will still be available by design. This is because, as a comprehensive and versatile remote connection solution, we must also continue supporting unsecure connections (e.g., Telnet). However, to maintain FIPS compliance, users must restrict usage of server-side algorithms to FIPS 140-2 Annex A security functions. Security functions used for encryption in FIPS-only mode are detailed in our official document, "Security Model and Encryption," which is available on our website: https://devolutions.net/security.

Supported Entries and Data Source

FIPS-only mode supports both RDP and SSH protocols. However, in order to operate SSH protocol, it requires manual configuration to authorize approved security functions. Please consult our online help section for a step-by-step guide: https://kb.devolutions.net/kb_ssh_configuration_rdm_fips140_2_compliance.html. Supported data sources include MSSQL Server and DVLS — both over TLS. This protocol is handled natively by the operating system to use approved security functions when configured in FIPS-only mode.

What If I Am Not Using FIPS-Only Mode?

Users are not obligated to comply with FIPS 140-2. Remote Desktop Manager remains highly secure, and it uses strong, industry-approved encryption to provide a high degree of confidentiality and integrity for data in transit and at rest. More details on our encryption standards are available in our official document, "Security Model and Encryption," which is available on our website: https://devolutions.net/security.