Release Notes DM705-SUB 24.1

DATACOM

Eldorado, September 2017

Dear costumer,

DATACOM is glad to present DM705 firmware version 24.1, which applies to DM705-CPU128 only:

- **DM705-CPU128:**
  - File name: 0257-24_1.im
  - Date: Fri Sep 1 20:21:48 UTC 2017
  - SHA256: 71d9fbdeba23da32cfd9a2a708cd7241e4b8e7858c585f565881c0381d8029f6

Firmware Upgrade Procedure

Procedure required only for DM705-CPU128.

- For firmware upgrades from version 22.1 (or older) to 23.1 (or newer), it is required to perform a two-stage procedure, performing an upgrade to an intermediate version and then to the newest version

  Upgrading firmware stages:

  Stage 1: firmware upgrade from version 22.1 (or less) to 22.2 with subsequent reboot.

  Stage 2: firmware upgrade from version 22.2 to the latest version with subsequent reboot.

  Any doubt about the procedure above, contact DATACOM's Technical Support.

New Features

- Secure firmware upgrade using SFTP.
- Menus on terminal to list users and set users' permissions.
- Option to disable unsecure management protocols.
- Log deletion TRAP.
- TRAP for successful and fail login attempt.
- Support to add user notes.

Corrected Issues

- Do not allow empty passwords when creating new users.
- Logging when configuring SNMP, Network, NTP or boot parameters.
- SNMPv3 requisitions were not working properly after system date was changed.

Improvements

- More detailed user database modifications logs.
- User password policy was improved, for security reasons.
- Management connection is closed after an idle time of 10 minutes, for serial interface.

Management

- FW24.1 is fully supported by DmView versions 9.6.0-2 or higher. It's strongly recommended to update DmView to this version because FW24.1 contains new features that are incompatible with older DmView versions. The side effect will be the generation of polling in DmView indefinitely.

This new version will be available from September 2017. Additional information can be obtained by contacting DATACOM support (support@datacom.ind.br or +55 51 3933-3122).

Regards,

DATACOM

Detailed information

Secure firmware upgrade using SFTP.

The equipment now supports firmware upgrade via SFTP. As in the firmware upgrade via FTP, the user allowed to upload the image file is fixed, with name “adminftp” and a configurable password.

Since DmView version 9.6, the firmware will be sent via SFTP protocol (when supported in the equipment’s version), regardless of whether the unsecure protocols are disabled or not.

Menus on terminal to list users and set users’ permissions.

The same menus for user management available on DM800 were implemented on DM705.

The menu to list users shows the names and permissions of each user. In case the operator is not an administrator, he/she can still see his/her own name and permissions.

The permissions menu allow setting the “Administrator”, “Configuration” and “Tests” permissions, provided the operator is an administrator.

Option to disable unsecure management protocols.

This new feature allows enabling and disabling all strictly unsecure management protocols, such as telnet, FTP and the proprietary PCGA protocol.

The unsecure protocols can only be enabled/disabled simultaneously. All incoming/outgoing traffic on the aforementioned protocols’ ports will be dropped by the equipment.

Secure protocols, such as SSH and SFTP, will be always enabled.

For a fully secure operation mode, SNMP must be properly configured by disabling SNMPv1 and SNMPv2 and enabling SNMPv3 only, for both accessing the equipment and sending traps.

Log deletion TRAP.

In case an user delete the user logs, a trap and the corresponding log will be generated, indicating the name of the user which deleted the logs.

TRAP for success and fail login attempt.

Every time an attempt to authenticate on the equipment occurs, a trap will be generated, indicating the user's name and access method of the attempt. There are traps for both success and failure, and also a corresponding log message.

Support to add user notes.

The user can insert any notes using terminal. The notes are persistent across reboots and it will be synchronized between CPUs.

Do not allow empty passwords when creating new users.

The equipment allowed creating users with empty passwords, which were not able to login.

A password policy was implemented, which forces passwords to be 8 characters long.

Logging when configuring SNMP, Network, NTP or boot parameters.

If SNMP, Network(Router, RIP, OSPF), NTP or boot configuration is changed via terminal or DmView, a log will be generated: User <user> saved network config. Where <user> is the user name. A similar message will be generated for other configurations.

SNMPv3 requisitions were not working properly after system date was changed.

When the system date was changed with a big offset (the issue was deterministic for a value of one year or more), SNMP daemon stopped to answer get and set requisitions. Now, when system date is changed, manually or via NTP, SNMP daemon is restarted.

More detailed user database modifications logs.

Whenever an administrator modified the user database, there was no information which operation was done.

The additional messages have the format “User <oper> added user <user>”, where <oper> is the operator and <user> is the user being modified. Aside from “add” operation, there are logs for “delete”, “change password” and “set permissions”.

Management connection is closed after an idle time of 10 minutes, for serial interface.

In case a session on the serial interface was not closed, other users could connect in the serial interface and use that session.

Now, once a session on the serial becomes idle for 10 minutes, that section will be closed and a new login will be required.

User password policy was improved, for security reasons.

The password policy was improved for security reasons. When creating new users in the equipment, the user password must have 8 characters long and must contain at least one number, one special character, one uppercase and one lowercase letter. The valid special characters are shown on the configuration screens with inputs for password. **Please see known issues.*

Known issues

When adding a new user with a name longer than 8 characters, login may not be performed properly. Login can be denied for this user.