



# GarrettCom<sup>®</sup>

*Industrial Networking at Its Best<sup>SM</sup>*

## Magnum Network Software – DX

### Software Release Notes

Software Revision 3.0.1 RC5

GarrettCom, Inc.

[www.GarrettCom.com](http://www.GarrettCom.com)

[www.GarrettCom.com/techsupport](http://www.GarrettCom.com/techsupport)

email: [support@GarrettCom.com](mailto:support@GarrettCom.com)

This document contains Confidential information or Trade Secrets, or both, which are the property of GarrettCom. This document may not be copied, reproduced or transmitted to others in any manner, nor may any use of the information in the document be made, except for the specific purposes for which it is transmitted to the recipient, without the prior written consent of GarrettCom.

Copyright 2010, GarrettCom.

All Rights Reserved

# Release 3.0.1 RC5 Release Notes

---

*The following notes describe significant changes in MNS-DX version 3.0.1 RC5 (since version 2.1.1 RC2).*

## 1.0 INTRODUCTION

The following notes contain details related to the MNS-DX v3.0.1 RC5 software release. MNS-DX v3.0.1 RC5 includes three main enhancements over MNS-DX v2.1.1 RC2 as follows:

- Support for the new DX940 hardware platform
- Support for tiered software feature sets through the use of “license keys”
- Enhanced IPsec and VPN implementation

## 2.0 NEW FEATURES

### 2.1 DX940 Support

A new hardware platform has been developed, the DX940, which is supported in v3.0.1 RC5 software. The initial DX940 supports the following port configurations:

- 2 Gigabit Ethernet Ports can be configured as
  - 2 SFP (multi-mode or single-mode fiber) or
  - 2 Fixed Copper
- 4 Fast Ethernet Ports can be configured as
  - 4 SFP (multi-mode or single-mode fiber) or
  - 4 Fixed Copper
- 4 DB-9 Serial Ports can be configured as
  - 4 RS-232/485 software selectable ports or
  - No ports populated

Please contact your GarrettCom sales representative or reference the GarrettCom website at <http://www.garrettcom.com/dx940.htm> for further details on the DX940 offering.

### 2.2 License Keys

Beginning with MNS-DX v3.0.1 RC5, customers will be given the choice of purchasing the appropriate mix of software license keys along with their DX router hardware. The license keys sets are summarized below:

**MNS-DX** is the base software license key that comes standard with all DX units and includes capabilities such as:

- Ethernet ports can be configured as switched ports or routed ports or combinations
- Serial ports can be software configurable as RS232 or RS485 ports
- RSTP supports RSTP-2004 (802.1w) & STP (802.1d), provides resilient Ethernet networks
- Routing features support RIP and RIP-II for routed ports
- VRRP – Virtual Router Redundancy Protocol provides router redundancy for Ethernet LAN devices
- DHCP Server and Client – provides DHCP services or queries for IP addresses
- Remote Access for secure administration is via SSH and optionally via telnet
- VLANs (802.1q) supports tagged based VLANs as access VLANs or trunk ports
- SNMP supports v1, v2 and v3 – for managing the device using Network Management Systems
- Event log locally stored provides a log of the most recent events
- SNTP provides time synchronization with NTP/SNTP servers
- Modbus interoperability over Ethernet or serial ports (RS232 or RS485)
- QoS prioritization to traffic using QoS and DiffServ tags across a network, and across a WAN port
- Trouble shooting is made easy with a built in protocol analyzer

**MNS-DX-SECURE** is an optional license key that can be purchased to add extra security features to the base MNS-DX such as IPSec, VPN, firewall, encryption and authentication needed for industrial cyber security. These extra Security features are unlocked via a licensed software key. MNS-DX-SECURE license key includes:

- IPSec VPN support with proven interoperability and conformance to industry standards
- Firewall provides stateful firewall rules for traffic flows or for IP streams or ports
- RADIUS provides management authentication via a RADIUS Server
- Configurable Login Banner message presented before user login to deter unauthorized users
- Secure Serial SSL connectivity to encrypt data
- Syslog operation enables logs to be collected by syslog servers for analysis
- SSH Port Forwarding allows secure access to less secure devices on the network
- Ethernet port security

**MNS-DX-ADVVAR** is an optional license key that can be purchased to add the advanced routing options of OSPF and BGP to the base MNS-DX. These Advanced Routing features are unlocked via a licensed software key.

### **2.2.1 License Key Transition Strategy**

DX units shipped prior to the release v3.0.1 may be upgraded to MNS-DX v3.0.1 and will retain their full feature set and capabilities (all License Keys enabled). However, in future releases (e.g. v3.1.0), these units will revert to the basic MNS-DX (no MNS-DX-SECURE or MNS-DX-ADVVAR features will be present) license key level.

**Important Note:** Therefore, it is important that customers install the appropriate license keys once they have upgraded to v3.0.1.

Please contact your GarrettCom representative to obtain details on receiving the required License Keys. The proper License Keys can be installed via the CLI or Web interfaces

**2.2.2 “License Key” CLI commands**

Syntax:

license add <SECURE|ADVAR> <key>  
license show

Examples:

MagnumDX# license add SECURE #####

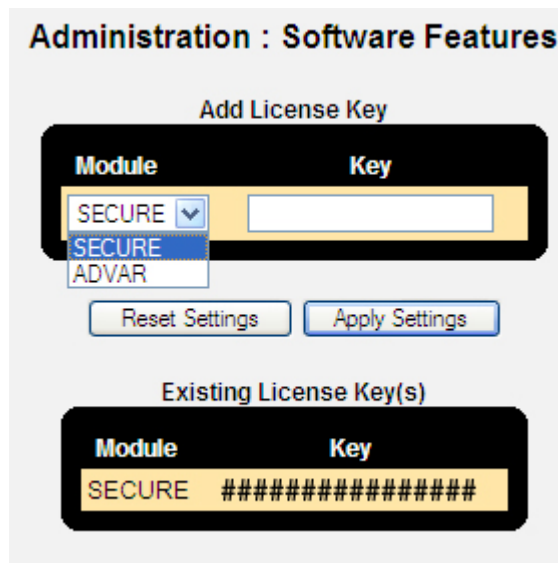
MagnumDX# license show

Feature Key

=====  
SECURE #####

**2.2.3 “License Key” Web interface**

There is a new page called "Administration : Software Features" that allows you to add new license keys and view existing license keys. This is where you can view the License Keys that are set (under Existing License Key(s) heading) in the DX unit or add the MNS-DX-SECURE or MNS-DX-ADVAR License Keys:



## 2.3 Enhanced IPsec and VPN implementation

V3.0.0 RC7 offers a new integrated IPsec library into the DX offerings but the user interface and configuration model remains unchanged. Users can upgrade from previous versions of the DX software and their configuration will be automatically migrated to 3.0.0. This release provides the following IPsec and VPN enhancements/capabilities:

- Adds AES256 and Blowfish encryption
- Adds SHA-2 hash (256 and 512 bit)
- Adds Diffie-Hellman (DH) groups 5 and 14
- Adds Bypass Firewall/NAT for VPN tunnels
- Maximum configurable VPN tunnels: 128
- Maximum configurable IKE peers: 8

### 2.3.1 Bypass Firewall/NAT

An option called Bypass Firewall/NAT has been added in the VPN tunnel configuration table. This option allows the user to select one of two forwarding behaviors for traffic received from a VPN tunnel:

"No". The packet forwarding from the tunnel continues to work as it did in previous DX software releases. That is, once a packet is decrypted and de-encapsulated, it is passed completely through the stack again. Thus, NAT and Firewall rules will be applied to the packet as if it were actually received on an external IP interface. This means that the NAT and firewall must be configured to deal appropriately with the decrypted packet as it emerges from the IPsec tunnel.

"Yes". This is a new forwarding behavior that allows the decrypted and de-encapsulated packet to simply continue its processing in the IP stack. The packet is NOT passed back through the stack and therefore bypasses the typical NAT and Firewall input processing. This effectively allows the router to filter unwanted packets coming from the public network while implicitly allowing all traffic that was sent through the tunnel.

### 2.3.2 “Bypass Firewall/NAT” CLI commands

The addition of the Bypass Firewall/NAT feature has expanded the “vpn tunnel” command to include the ability to set the proper Bypass Firewall/NAT setting. The default setting is No.

The Bypass Firewall/NAT feature can be set to Yes either by entering a new VPN tunnel definition using the ***add tunnel*** command as follows:

Syntax:

```
MagnumDX(vpn)# add tunnel <src address> <src mask> <dest address> <dest mask> <gateway address> bypass <y or n>
```

Or you can use the *edit tunnel* command as follows:

```
MagnumDX(vpn)# edit tunnel <tunnel id>
[src-address <A.B.C.D>]
[src-mask <A.B.C.D>]
[dst-address <A.B.C.D>]
[dst-mask <A.B.C.D>]
[gateway <A.B.C.D>]
[profile <profile-name>]
[authentication <authentication-method-name>]
[bypass <y|n>]
<cr>
```

### 2.3.3 “Bypass Firewall/NAT” WEB Interface

The addition of the Bypass Firewall/NAT feature has expanded the Security:VPN:Tunnels page to allow viewing and setting of the Bypass Firewall/NAT feature as follows:

**Security : VPN : Tunnels**

Add Tunnel

Source Address	Source Mask	Destination Address	Destination Mask	Destination Gateway	Profile	Authentication	Bypass FW/NAT?
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Default	Default	No

Existing Tunnels

ID	Source Address	Source Mask	Destination Address	Destination Mask	Destination Gateway	Profile	Authentication	Bypass FW/NAT?	Delete
1	1.1.1.1	255.255.255.255	2.2.2.2	255.255.255.255	3.3.3.3	Default	Default	Yes	<input type="checkbox"/>
2	4.4.4.4	255.255.255.255	5.5.5.5	255.255.255.255	6.6.6.6	Default	Default	No	<input type="checkbox"/>

## 3.0 QUALITY ENHANCEMENTS

- 3.1 Pings to an Ethernet interface that is in a down state will now return the proper response of “Host unreachable”.
- 3.2 The “Ethernet clear statistics” command now properly clears the specified Ethernet port statistics.

- 3.3** The DX unit would reboot when multiple ports were entered into the “VLAN set” command. This has been resolved.
- 3.4** If you deleted a VID from the DX it would still stay active until you performed a system reboot. This has been resolved and is no longer active after it has been deleted.
- 3.5** Improved VPN re-key operation to minimize traffic loss.
- 3.6** Resolved issue where you were unable to change the WAN mode setting between T1 and E1 via the CLI.
- 3.7** Resolved several cases where terminal server sessions started using SSH port forwarding did not always close properly.
- 3.8** The software now saves active event files prior to system reboots so that the information is no longer lost.
- 3.9** The W2 port statistics on the DX1000 now reflect the true W2 statistics and are not a copy of the W1 statistics as in previous versions.
- 3.10** SSH sessions no longer have a fixed timeout of 1 hour.
- 3.11** The DX has been enhanced to now log Loop Up/Loop Down events.
- 3.12** Disabling OSPF on a PPP interface no longer causes a system problem.
- 3.13** Resolved the issue of a WAN port, that was running OSPF, displaying a default metric of 75 but really using a metric of 1.
- 3.14** Resolved issue with SSH port forwarding to a non-existent device.
- 3.15** Resolved issue where a Frame Relay DLCI could be configured on a WAN port that was defined for PPP operation.
- 3.16** Any port forwarding SSH session will automatically use a setting of “no idle timeout” value instead of using the session timeout setting that is used for any user sessions to the DX CLI or GUI.