



# FEDERAL SIGNAL



## DTX-RG-301W Operations Manual (Software Release 3.0)

# ***DTX SERIES***

©2010 Federal Signal Corporation  
2645 Federal Signal Drive, University Park, IL 60484-3167  
708-534-3400

255395A  
REV. A 1010  
Printed in U.S.A.



# TABLE OF CONTENTS

<b>Chapter 1: Radius Gateway Quick Config .....</b>	<b>6</b>
Tools Needed .....	6
Connecting to the Gateway for Configuration .....	6
<b>Chapter 2: Web Interface Administration.....</b>	<b>7</b>
System Menu .....	7
Change Password (System -> Change Password) .....	7
Gateway Admin Users (System -> Gateway Admin Users) .....	7
Clock (System -> Clock) .....	7
Identity & Location (System -> Identity & Location) .....	7
Resources (System -> Resources) .....	7
Syslog (System -> Syslog) .....	8
Logging Rules (System -> Logging Rules).....	8
Remote Syslog Settings (System -> Remote Syslog Settings).....	8
Backup/Restore (System -> Backup/Restore) .....	8
Reboot Gateway (System -> Reboot Gateway).....	8
Reset Configuration (System -> Reset Configuration) .....	8
<b>Chapter 3: Web Interface WAN Menu .....</b>	<b>9</b>
WAN Menu.....	9
Wifi Configuration.....	9
Wifi IP Address.....	9
3G Configuration.....	10
DNS .....	10
<b>Chapter 4: Web Interface LAN Menu .....</b>	<b>11</b>
LAN Menu .....	11
IP Address / DHCP Server .....	11
DHCP Leases.....	11
<b>Chapter 5: Web Interface Tools Menu .....</b>	<b>12</b>
Tools Menu.....	12
Ping (Tools -> Ping).....	12
IP Scan (Tools -> IP Scan).....	12
Netwatch (Tools -> Netwatch).....	13
<b>Chapter 6: Web Interface Advanced Menu .....</b>	<b>14</b>
Advanced Menu.....	14
Firewall Filter (Advanced -> Firewall Filter).....	14
Firewall Netmap (Advanced -> Firewall Netmap).....	15
Destination NAT (Advanced -> NAT (DST-NAT)).....	15
Source NAT (Advanced -> NAT (SRC-NAT)) .....	16
Interface List (Advanced -> Interface List).....	17
IP Addresses (Advanced -> IP Addresses).....	17
Management Ports (Advanced -> Management Ports) .....	17
PPTP Clients (Advanced -> PPTP Clients).....	18
Static DNS (Advanced -> Static DNS) .....	18
Static Routes (Advanced -> Static Routes) .....	19
<b>Chapter 7: Quick Troubleshooting .....</b>	<b>20</b>
<b>Appendix A: Subnet Mask to CIDR Network Number Conversion.....</b>	<b>21</b>
<b>Obtaining Technical Support and Service .....</b>	<b>22</b>
<b>Returning a Product to Federal Signal .....</b>	<b>22</b>

## Limited Warranty

The Mobile Systems Division of Federal Signal Corporation warrants each new product to be free from defects in material and workmanship, under normal use and service, for a period of one year on parts replacement and factory-performed labor from the date of delivery to the first user-purchaser. Warranty on hardware may be extended when an annual maintenance agreement is purchased for up to five years from date of delivery. This warranty includes one year software support via telephone and software upgrades. Warranty on the DTX Series software can be extended as long as an annual maintenance agreement is purchased.

During this warranty period, the obligation of Federal Signal is limited to repairing or replacing, as Federal Signal may elect, any part or parts of such product which after examination by Federal Signal discloses to be defective in material and/or workmanship.

Federal Signal will provide warranty for any unit which is delivered, transported prepaid, to the Federal Signal factory or designated authorized warranty service center for examination and such examination reveals a defect in material and/or workmanship.

This warranty does not cover travel expenses, the cost of specialized equipment for gaining access to the product, or labor charges for removal and re-installation of the product. The Federal Signal Corporation warranty shall not apply to components or accessories that have a separate warranty by the original manufacturer.

This warranty does not extend to any unit which has been subjected to abuse, misuse, improper installation or which has been inadequately maintained, nor to units which have problems related to service or modification at any facility other than Federal Signal factory or authorized warranty service centers. Moreover, Federal Signal shall have no liability with respect to defects arising in products through any cause other than ordinary use (such as, for example, accident, fire, lightning, water damage, or other remaining acts of God).

THERE ARE NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL FEDERAL SIGNAL BE LIABLE FOR ANY LOSS OF PROFITS OR ANY INDIRECT OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY SUCH DEFECT IN MATERIAL WORKMANSHIP.

# Safety Message to Installers of Federal Signal DTX Series Systems and Options

## WARNING

**People's lives depend on your proper installation and servicing of our products. It is important to read and follow all instructions shipped with this product. In addition, listed below are some other important safety instructions and precautions you should follow:**

- To properly install a vehicular camera system, you must have a good understanding of automotive electrical systems along with proficiency in the installation and use of safety warning equipment.
- Read and follow all safety and operating instructions before installing, configuring, or operating the DTX Series system. Safety and operating instructions are also located in the DTX Series software interface and can be accessed by clicking the Help button.
- DO NOT install equipment or route wiring in the deployment path of an airbag.
- If a seat is temporarily removed, verify with the vehicle manufacturer if the seat needs to be recalibrated for proper airbag deployment.
- Locate the camera(s), monitor, voltage regulator, inertia sensor, and digital video recorder (as applicable) so the VEHICLE and SYSTEM can be operated safely under all driving conditions. The mounting of the camera(s) is particularly important in order to obtain the largest field of view, which will in turn maximizes the effectiveness of the system.
- When drilling into a vehicle structure, be sure that both sides of the surface are clear of anything that could be damaged. Remove all burrs from drilled holes. To prevent electrical shorts, grommet all drilled holes through which wiring passes. Also ensure that the mounting screws do not cause electrical or mechanical damage to the vehicle.
- DTX Series system may fail to operate as intended if configured incorrectly. Configuration should only be performed by personnel thoroughly familiar with the DTX operating instructions and the intended method of use.
- DTX Series system must be correctly configured per the user's specific application before it is placed into use. Configuration should only be performed after thoroughly reading this manual, the as well as the configuration and user's manuals. Always test the DTX Series system for proper operation after programming and before placing it into use.
- Do not open the camera element, wireless or in-car microphone, or control box. There are no user-serviceable parts inside and opening any component will void the warranty.
- You should frequently inspect the camera system to ensure that it is operating properly and that it is securely attached to the vehicle. The front face of any installed cameras should be kept clean and free from any accumulated dirt or grime so that the cameras may provide the clearest image. Obstructions to the camera image limit the effectiveness of the system.
- File these instructions in a safe place and refer to them when maintaining and/or reinstalling the product.

**Failure to follow all safety precautions and instructions may result in property damage, serious injury, or death to you or others.**

# Chapter 1: Radius Gateway Quick Config

## *Tools Needed*

The following items will be needed for initial gateway configuration:

- Desktop or laptop computer with a network card and web browser with JavaScript enabled.
- CAT5 network cable



## *Connecting to the Gateway for Configuration*

The physical connections to be made for initial configuration are:

- Using the other CAT5 cable, connect the computer to port Eth2 of the gateway.
- To log on, open a web browser and go to location <http://10.255.255.254>
- The default username is admin. The default password is blank.



Username:

Password:

**Note:** All Ethernet ports on the gateway support automatic MDI/MDI-X crossover detection. So, there is no need to be concerned about crossover or straight-through CAT5 cables when making network connections.

## Chapter 2: Web Interface Administration

### *System Menu*

The system menu controls the system-wide features of the gateway.



#### **Change Password (System -> Change Password)**

This link allows the currently logged in administrative user to change their password.

#### **Gateway Admin Users (System -> Gateway Admin Users)**

This link allows management of available gateway administrative users. By default, the admin user is the only user available.

#### **Clock (System -> Clock)**

This link sets the internal clock of the gateway. The time zone and active NTP servers can also be defined.

#### **Identity & Location (System -> Identity & Location)**

This link allows internal identification variables to be set. This is useful to keep track of gateway identity and location information if many gateways are deployed in diverse locations.

#### **Resources (System -> Resources)**

This link shows run-time information of the gateway including up time, CPU load, and hard drive space.

**Syslog (System -> Syslog)**

This link displays the currently available internal syslog.

**Logging Rules (System -> Logging Rules)**

This link defines where and how syslog messages should be handled. By default, messages stored to disk will have the file name of "log". To store messages on a remote syslog server, configure the IP address and UDP port of the server in System -> Logging Actions screen.

**Remote Syslog Settings (System -> Remote Syslog Settings)**

This link defines the remote syslog settings.

**Backup/Restore (System -> Backup/Restore)**

This link allows for backup and restore functionality. Restore actions can be performed between different gateways of the same model. Restore will fail if the model numbers are different.

**Reboot Gateway (System -> Reboot Gateway)**

This menu item reboots the gateway.

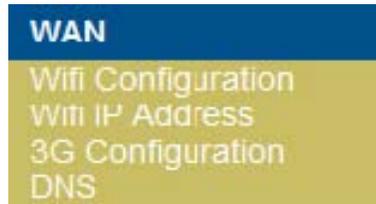
**Reset Configuration (System -> Reset Configuration)**

This feature resets the gateway to factory defaults.

# Chapter 3: Web Interface WAN Menu

## WAN Menu

The WAN Menu is where the RG-301wmr will connect to a wireless network and setup for 3G network.



## Wifi Configuration

The Wifi Configuration is used as a bridge to connect to the wireless network. To setup the connection makes sure that Enabled is set for Yes, specify the SSID that the RG-301wmr is to connect to, and select the encryption for the wireless network. Click Save to save these changes to the device.

### Wifi Configuration

Enabled: Yes ▾  
Regulatory Domain: United States ▾  
SSID: ssid  
Encryption: None ▾  
None  
WEP  
WPA-PSK  
WPA2-PSK

## Wifi IP Address

Once the wifi bridge SSID has been configured the gateway can be set up with a static IP address or DHCP address from the wireless network.

### Wifi IP Address

Connection Type: Static ▾  
IP Address:   
Subnet Mask: 255.255.255.255 ▾  
Default Gateway:   
Save

### Wifi IP Address

Connection Type: DHCP Client ▾  
Use Peer DNS: No ▾  
DHCP Address:  
Default Gateway:  
DHCP Server:  
Status:  
Expires:  
Save

Note: To verify connectivity to the wireless network go to System then click Status to see the status of the connection as either Connected or Disconnected. If there is a connection and IP address will show, otherwise it will show as Disconnected.

## 3G Configuration

The 3G Configuration is setup uses either the Sprint 598 or the Verizon 760 3G USB card.  
Setup: 1) Connect the 3G USB card into once of the front USB ports 2) From the 3G Configuration menu, select the proper USB card and IP address will show, otherwise it will show as Disconnected.

# 3G Configuration

**3G USB Card:**  

- None
- Sprint USB 598
- Verizon USB 760

## DNS

This screen stores the primary and secondary DNS server settings.

# DNS Configuration

**Primary DNS:**

**Secondary DNS:**

## Chapter 4: Web Interface LAN Menu

### LAN Menu

The LAN menu will show the configurable DHCP server range and current DHCP leases.



### IP Address / DHCP Server

This section gives you the ability to change the LAN settings for the gateway and devices that will connect to the gateway.

## LAN IP Address and DHCP Server

Router LAN IP Address:	<input type="text" value="10.11.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
DHCP Server Starting IP:	<input type="text" value="10.11.1.10"/>
DHCP Server Ending IP:	<input type="text" value="10.11.1.250"/>
Lease Time (hh:mm:ss):	<input type="text" value="1:00:00"/>
<input type="button" value="Save"/>	

Note: The DHCP pool and the Router LAN IP must be on the same subnet. If changes are made to this section, you will need to renew your IP address before you continue to have access to the gateway again.

### DHCP Leases

This section shows the current leases from the gateway to DHCP devices connected to the gateway.

## LAN DHCP Leases

MAC Address	IP Address	Status	Expiration
00:A0:D1:83:E7:12	10.11.1.249	bound	00:36:40

## Chapter 5: Web Interface Tools Menu

### *Tools Menu*

The Tools Menu contains useful tools for monitoring and troubleshooting guest and equipment connectivity.

- **Ping (Tools -> Ping)**

## Ping Tool

**Ping Address:**

**Interface:**  ▾

**Arp Ping:**

- Enter the equipment IP address
- If desired, tick the ARP Ping checkbox. ARP Ping does a ping by ARP address instead of IP address. It is required that the address being pinged be on the same subnet as the interface doing the pinging.
- Click the "Ping" button.

### **IP Scan (Tools -> IP Scan)**

This screen is used to scan ip ranges of users or devices on the guest network. It does an ARP ping on the selected interface. Results are displayed below the form.

## IP Scan Tool

**Interface:**  ▾

**Start IP Address:**

**End IP Address:**

**Timeout:**  ▾

## Netwatch (Tools -> Netwatch)

The Netwatch screen defines which IP addresses are watched and monitored. When devices become unreachable from the gateway, the status will show Down in this dialog. To add a new device, click the "Add Netwatch IP" link. Devices may be edited or deleted by clicking on the respective links for the desired device.

### Netwatch Tool

IP Address	Interval	Timeout (ms)	Status	Since	Comment
10.17.5.235	00:01:00	3000	up	jun/18/2010 06:38:00	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.236	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.237	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.238	00:01:00	3000	up	jun/17/2010 05:50:00	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.239	00:01:00	3000	down	jan/01/1970 19:00:42	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.240	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.241	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.242	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.243	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.244	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.245	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.246	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.247	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.248	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.249	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.250	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.251	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.252	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.253	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>
10.17.5.254	00:01:00	3000	up	jun/17/2010 05:50:03	Guest Network Device <a href="#">[Edit]</a> <a href="#">[Delete]</a>

[\[Add Netwatch IP\]](#) 

## Chapter 6: Web Interface Advanced Menu

### Advanced Menu

The Advanced Menu controls advanced gateway features and functions.

#### DNS Cache (Advanced -> DNS Cache)

This screen displays the internal gateway DNS Cache with the option to flush the cache.

### DNS Cache

[\[Flush DNS Cache\]](#)

Name	Type	Data	TTL
254.255.255.10.in-addr.arpa	PTR	login.radiusgateway.com	1d00:00:00
a.blip.tv.edgesuite.net	CNAME	a460.g.akamai.net	00:10:02
a.friendfinderinc.com.edgesuite.net	CNAME	a841.x.akamai.net	00:24:06
a.fsdn.com.edgekey.net	CNAME	e872.g.akamaiedge.net	04:37:17
a6.emitrk.com	CNAME	fingerprint-production-62721138.us-east-1.elb.amazonaws.com	00:14:56

#### Firewall Filter (Advanced -> Firewall Filter)

The Firewall Filter drops network traffic on the forward chain according to the specified rules. Traffic may be dropped by source IP, source mac address, destination IP, protocol and port or many of the above.

### Firewall Filter

Src IP	Src MAC	Dst IP	Protocol:Port	Pkt Count	Comment
		1.1.1.1		0	<a href="#">[Edit]</a> <a href="#">[Delete]</a>

[\[Add New Filter Rule\]](#)

To add a new rule, click the "Add New Filter Rule" link. Define the desired rule and click the "Add Filter Rule" button.

### Add Filter Rule

**Source IP:**

**Source MAC Address:**

**Destination IP:**

**Protocol : Dst Port:**  :

**Comment:**

### Firewall Netmap (Advanced -> Firewall Netmap)

The Firewall Netmap screen defines which public IP addresses are netmapped to which private IP addresses. This feature is useful when a device or workstation needs to be manually bypassed as a public IP address. Any VPN IP addresses defined in Guest Network ->VPN Mappings are also visible here in read-only mode.

## Firewall NETMAP

Public Address	Private Address	Comment	
66.77.88.99	10.11.1.12	DVR	[Edit] [Delete]
192.168.3.248	10.99.99.4	RADConfig-map-24	LOCKED
192.168.3.249	10.99.99.3	RADConfig-map-24	LOCKED
192.168.3.250	10.99.99.2	RADConfig-map-24	LOCKED

[\[Add New NETMAP Rule\]](#) 

To create a new Netmap rule, click the "Add New NETMAP Rule" link. Define the desired rule and click the "Add NETMAP Rule" button.

## Add NETMAP Rule

**External IP Address:**

**Internal IP Address:**

**Comment:**

 **Note:** When manually adding netmap entries, the public IP address should also be added to ether1 on the public internet interface

### Destination NAT (Advanced -> NAT (DST-NAT))

Destination NAT rules may be configured to permit external ports to map to internal devices and ports. Devices that are mapped externally in the Guest Network -> Devices configuration are also visible here. This screen may also be used to define extra port mapping rules for existing devices if needed.

## Firewall DST-NAT

Ext Port	Protocol	Int Address	Int Port	Pkt Count	Comment	
8000	tcp	10.11.1.10	80	0	DVR	[Edit] [Delete]

[\[Add New DST-NAT Rule\]](#) 

To add a new Destination NAT rule, click the "Add New DST-NAT Rule" link.

# Add DST-NAT Rule

**External Port (1024-65535):**

**Protocol:**

**Internal IP Address:**

**Internal Port (0-65535):**

**Comment:**

- **External Port** - The external port to bind to the external IP address
- **Protocol** - Desired protocol (TCP or UDP)
- **Internal IP Address** - The internal IP address to map
- **Internal Port** - The internal port to map
- **Comment** - Human-readable comment for the destination NAT rule

## Source NAT (Advanced -> NAT (SRC-NAT))

Source NAT rules may be configured to NAT devices on a different subnet than the guest network has configured in the DHCP server settings.

## Firewall SRC-NAT (Masquerade)

Src Address	Src Subnet	Pkt Count	Comment
10.11.1.0	255.255.255.0	4871	RADConfig-masquerade hotspot network LOCKED
10.11.2.0	255.255.255.0	0	Another subnet [Edit] [Delete]
10.99.99.0	255.255.255.224	0	RADConfig-VPN NAT LOCKED

[\[Add New SRC-NAT Rule\]](#)

To add a new source NAT entry, click the "Add New SRC-NAT Rule" link.

## Add SRC-NAT (masquerade) Rule

**Source Address:**

**Source Subnet:**

**Comment:**

- **Source Address** - Network address for the new rule
- **Source Subnet** - Subnet mask for the new rule
- **Comment** - Human-readable comment for the source NAT rule

### Interface List (Advanced -> Interface List)

The interface list displays the name and MAC address of each physical interface on the gateway.

## Interface List

Name	MAC Address
ether1	90:F2:78:70:98:98
ether2	90:F2:78:7A:98:98
ether3	90:F2:78:7B:98:98
subscriberBridge	90:F2:78:7B:98:98

### IP Addresses (Advanced -> IP Addresses)

The IP Address screen displays IP addresses in use by the gateway itself. Most addresses in this list are not editable because they are modified in other configuration screens. However, if additional IP addresses are needed on some interface(s), they may be added here.

## IP Addresses

Interface	IP Address	Subnet Mask	Comment
subscriberBridge	10.11.1.1	255.255.255.0	RADConfig-Private IP User Space
ether2	10.30.0.10	255.255.255.0	RADConfig-LB Config Secondary
subscriberBridge	10.99.99.1	255.255.255.224	RADConfig-Public Pool IP
rgBridge	10.255.255.253	255.255.255.252	RADConfig-Web Server
ether1	192.168.3.102	255.255.255.0	RADConfig-LB Config Primary
ether1	192.168.3.248	255.255.255.0	RADConfig-map
ether1	192.168.3.249	255.255.255.0	RADConfig-map
ether1	192.168.3.250	255.255.255.0	RADConfig-map

[\[Add New IP Address\]](#)

### Management Ports (Advanced -> Management Ports)

This screen controls which ports are open for remote management. The checkbox next to each service controls whether it is enabled or disabled.

## Management Ports

Enabled	Service	Port
<input checked="" type="checkbox"/>	Telnet	<input type="text" value="23"/>
<input checked="" type="checkbox"/>	SSH	<input type="text" value="22"/>
<input checked="" type="checkbox"/>	FTP	<input type="text" value="21"/>
	HTTP/Web	<input type="text" value="80"/>

PPTP Clients (Advanced -> PPTP Clients)

## PPTP Clients

Client Name	Host	User	Online	Comment
PPTP server	1.1.1.1	user	no	PPTP Connection <a href="#">[Detail]</a>

[\[Add New PPTP Client\]](#)

To add a new PPTP client, click the "Add New PPTP Client " link.

### Add PPTP Client

**PPTP Client Name:**

**Host:**

**Username:**

**Password:**

**Comment:**

**MTU:**

**MRU:**

**Use Compression:**  ▾

**Use VJ Compression:**  ▾

**Use Encryption:**  ▾

**Change TCP MSS:**  ▾

### Static DNS (Advanced -> Static DNS)

Static DNS entries may be made on the gateway in order to manually define how users on the guest network resolve specific domain names. By default, the "login.radiusgateway.com" domain is defined to point to the internal web server. This feature may also be used to black-hole a specific domain for blocking purposes.

## Static DNS

DNS Name	Address		
blockeddomain.com	127.0.0.1	<a href="#">[Edit]</a>	<a href="#">[Delete]</a>
login.radiusgateway.com	10.255.255.254		

Static DNS entry added.

[\[Add New Static DNS Entry\]](#)

### Static Routes (Advanced -> Static Routes)

Static routes may be defined on the Static Routes screen. When adding new routes, a specific IP address or interface may be defined.

## Static Routes

Destination	Netmask	Gateway	Active	Comment
0.0.0.0	0.0.0.0	192.168.3.7	yes	RADConfig-Static Config
192.168.1.1	255.255.255.255	192.168.3.254	yes	[Edit] [Delete]

[Add New Route] 

## Add Static Route

**Destination:**

**Subnet Mask:**  

**Gateway:**  

**Comment:**

## **Chapter 7: Quick Troubleshooting**

<b>Problem</b>	<b>Troubleshooting Steps</b>
No lights on the gateway	Verify that the power is connected.
Unable to manage equipment that has been mapped.	Verify that the equipment is programmed with the proper subnet mask and default gateway.
Unable to remotely manage gateway	Verify that the gateway is not double-NATed. See network diagram in chapter 1. If it is double-NATed, ensure that the router facing the internet is passing the necessary ports (port 80 tcp is required minimum).

# Appendix A: Subnet Mask to CIDR

## Network Number Conversion

/17 32,768 255.255.128.0 128 /24 nets /18 16,384  
255.255.192.0 64 /24 nets /19 8,192 255.255.224.0 32 /24  
nets /20 4,096 255.255.240.0 16 /24 nets /21 2,048  
255.255.248.0 8 /24 nets /22 1,024 255.255.252.0 4 /24 nets  
/23 512 255.255.254.0 2 /24 nets /24 256 255.255.255.0 1  
/24 128 255.255.255.128 Half of a /24 /26 64 255.255.255.192  
Fourth of a /24 /27 32 255.255.255.224 Eighth of a /24 /28 16  
255.255.255.240 1/16th of a /24 /29 8 255.255.255.248 5 Usable  
addresses /30 4 255.255.255.252 1 Usable address /31 2  
255.255.255.254 Unusable /32 1 255.255.255.255 Single host

An online CIDR calculator is also available at <http://www.subnet-calculator.com/cidr.php>

**CIDR Total number Network Description:Notation: of  
addresses: Mask:**

/9 8,388,608 255.128.0.0 128 /16 nets /10 4,194,304  
255.192.0.0 64 /16 nets /11 2,097,152 255.224.0.0 32 /16  
nets /12 1,048,576 255.240.0.0 16 /16 nets /13 524,288  
255.248.0.0 8 /16 nets /14 262,144 255.252.0.0 4 /16 nets  
/15 131,072 255.254.0.0 2 /16 nets /16 65,536 255.255.0.0 1  
/16

## Obtaining Technical Support and Service

If a device of the DTX Series installed system does not operate properly and falls within the warranty coverage provided, or if further servicing assistance is needed for the DTX Series system, contact technical support at:

**Federal Signal Corporation**  
**2645 Federal Signal Drive**  
**University Park, IL 60484-3167**  
**Phone: (800) 433-9132**  
[empserviceinfo@fedsig.com](mailto:empserviceinfo@fedsig.com)

## Returning a Product to Federal Signal

Before returning a product to Federal Signal, call **800-264-3578** to obtain a Returned Merchandise Authorization number (RMA number). To expedite the process please be prepared with the following information:

- Your Federal Signal customer or account number
- The purchase order number under which the items were purchased
- The shipping method
- The model or part number of the product being returned
- The quantity of products being returned
- Drop ship information as needed
- Any estimate required

When you receive your RMA Number:

- Write the RMA number on the outside of the box of returned items
- Reference the RMA number on your paperwork inside of the box
- Write the RMA number down, so that you can easily check on status of the returned equipment

Send all material with the issued RMA Number to:

**Federal Signal Corporation**  
**2645 Federal Signal Drive**  
**University Park, IL 60484-3167**  
**Attn: Service Department**  
**RMA: # \_\_\_\_\_**



