3e Technologies International, Inc.
FIPS 140-2
Non-Proprietary Security Policy
Level 2 Validation

Version 3.1

May 20, 2004

Glossary of terms

AP	Access Point
CO	Cryptographic Officer
DH	Diffie Hellman
DHCP	Dynamic Host Configuration Protocol
DMG	Dual Mode Gateway
DMZ	De-Militarized Zone
IP	Internet Protocol
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
HTTPS	Secure Hyper Text Transport Protocol
LAN	Local Area Network
MAC	Medium Access Control
NAT	Network Address Translation
PRNG	Pseudo Random Number Generator
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SRDI	Security Relevant Data Item
SSID	Service Set Identifier
TLS	Transport Layer Security
WAN	Wide Area Network
WLAN	Wireless Local Area Network

1. Introduction

1.1. Purpose

This document describes the non-proprietary cryptographic module security policy for 3e Technologies International's wireless gateway products, the *3e-521NP, 3e-522FIPS, 3e-530NP and 3e-531AP Wireless Gateways* (HW P/Ns 3e-521NP, 3e-522FIPS, 3e-530NP, and 3e-531AP; Firmware Version 2.6), hereafter known as the 3e-DMG (Dual Mode Gateway). This policy was created to satisfy the requirements of FIPS 140-2 Level 2. This document defines 3eTI's security policy and explains how the 3e-DMG Wireless Gateways meet the FIPS 140-2 security requirements.

The figures below show the 3e-521NP, 3e-522FIPS, and 3e-531NP Gateways. The 521NP and 530NP look identical and so only one picture is included.

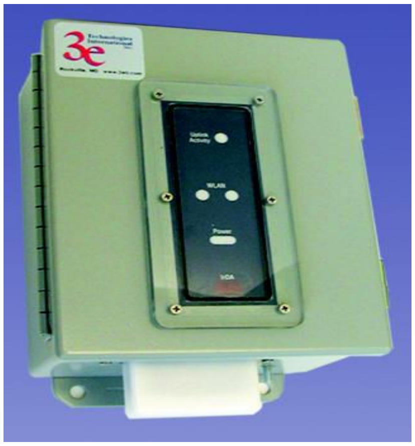


Figure A: 3e-521NP /530NP Gateway

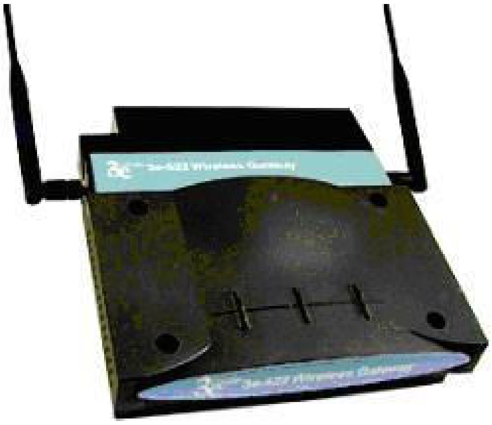


Figure B: 3e-522FIPS Gateway

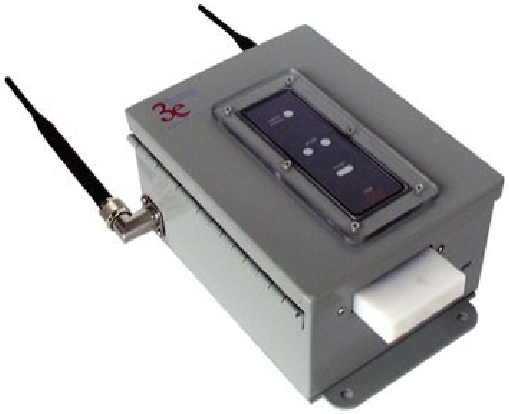


Figure C: 3e-531AP Gateway

The cryptographic module security policy consists of a specification of the security rules, under which the cryptographic module shall operate, including the security rules derived from the requirements of the standard. Please refer to FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules* available on the NIST website at http://csrc.nist.gov/cryptval/.

1.2. Definition

The 3e-DMG Wireless Gateway is a device which consists of electronic hardware, embedded software and strong metal case. For purposes of FIPS 140-2, the module is considered to be a multi-chip standalone product. The 3e-DMG gateway operates as either a gateway connecting a local area network to wide area network (WAN) or as an access point within a local area network (LAN). The cryptographic boundary of the 3e-DMG Gateway is defined to be the entire enclosure of the Gateway. The 3e-DMG is physically bound by the mechanical enclosure which is protected by tamper evident tape.

3eTI Gateway software provides the following major services in FIPS mode:

- Wireless 802.11b Access Point functionality (bridging from the wired uplink LAN to the wireless LAN).
- DHCP service to the local LAN (allows a wired local LAN to exist over the local LAN interface).

The only difference between the 3e-521NP and 3e-530NP is the outer enclosure of the gateway. The 3e-521NP uses a steel enclosure and the 3e-530NP employs an aluminum enclosure.

The only difference between the 3e-521NP and 3e-531AP is the outer enclosure of the gateway. The 3e-521NP uses an internal antenna wireless card and the 3e-531AP uses external antennas.

1.3. Scope

This document will cover the secure operation of the 3e-DMG including the initialization, roles and responsibilities of operating the product in a secure, FIPS-compliant manner, and describe the Security Relevant Data Items (SRDIs).

The Gateway has three modes of operations which are listed in the table below:

Mode	FIPS Mode
Gateway Mode	No
AP / Bridging Mode (Mode 1)	No
AP /Bridging Mode (Mode 2)	Yes

Only the AP/Bridging - FIPS mode (Mode 2) is explained in this document. The other modes cannot be validated to FIPS 140-2 because they execute applications that use non-FIPS Approved cryptographic algorithms.

In order to enter FIPS mode, select the FIPS 140-2 Mode box on the Operation Mode page of the management GUI (see 3.3.1.3). This will force the gateway to return to factory defaults and then the gateway will reboot into FIPS mode. To leave FIPS mode, un-select the FIPS 140-2 Mode box and apply the changes. Once again, the gateway will restore factory defaults and then reboot into non-FIPS mode.

On transition between modes, the system is returned to factory defaults and all keys are zero-ized.

2. Roles, Services, and Authentication

The 3e-DMG supports four separate roles. The set of services available to each role is defined in this section. The 3e-DMG authenticates an operator's role by verifying his PIN or access to a shared secret.

2.1.1. Roles and Services

The 3eTI gateway supports the following authorized roles for operators:

Crypto Officer Role: The Crypto officer role performs all security functions provided by the Gateway. This role performs cryptographic initialization and management functions (e.g., module initialization, input/output of cryptographic keys and SRDIs, audit functions and user management). The Crypto officer is also responsible for managing the Administrator users. The Crypto officer must operate within the Security Rules and Physical Security Rules specified in Sections 3.1 and 3.2. The Crypto officer uses a secure web-based HTTPS connection to configure the Gateway. Only one Crypto Officer is defined in the Gateway. The Crypto Officer authenticates to the Gateway using a username and password.

Administrator Role: This role performs general Gateway configuration such as defining the WLAN, LAN and DHCP settings, performing self-tests and viewing system log messages for auditing purposes. No CO security functions are available to the Administrator. The Administrator can also reboot the Gateway if deemed necessary.

The Administrator must operate within the Security Rules a specified in Section 3.1 and always uses a secure web-based HTTPS connection to configure the Gateway. The Administrator authenticates to the Gateway using a username and password. Up to 5 operators who can assume the Administrator role can be defined. All Administrators are identical i.e. they have the same set of services available. The Crypto Officer is responsible for managing (creating, deleting) Administrator users.

The follow table outlines the functionalities that are provided by each role:

Categories	Features	Operator Roles											
		CryptoOfficer						Administrator					
		Show[1]	Set[2]	Add[3]	Delete[4]	Zeroize[5]	Default Reset[6]	Show[7]	Set[8]	Add[9]	Delete[10]	Zeroize[11]	Default Reset[12]
System Configuration													
• General	Hostname	X	X				X	X	X				X
	Domain name	X	X				X	X	X				X
	Date/Time	X	X				X	X	X				X
• WAN	DHCP client	X	X				X	X	X				X
	Static IP address	X	X				X	X	X				X
	10/100 MBps half/full duplex/auto	X	X				X	X	X				X
• LAN	IP address	X	X				X	X	X				X
• Operating Mode	Gateway	X	X				X	X	X				X
	AP / Bridging Mode – FIPS	X	X				X	X	X				X
	AP / Bridging Mode – Non-FIPS	X	X				X	X	X				X
Wireless Configuration													
• General	SSID	X	X				X	X	X				X
	Channel Number	X	X				X	X	X				X
	• Enable / Disable Auto Selection	X	X				X	X	X				X
	• Auto selection button	X	X				X	X	X				X
	Transmit Power Mode	X	X				X	X	X				X
	Fixed Power Level	X	X				X	X	X				X
	Beacon Interval	X	X				X	X	X				X
	RTS Threshold	X	X				X	X	X				X
	DTIM	X	X				X	X	X				X
	Basic Rates	X	X				X	X	X				X
	Preamble	X	X				X	X	X				X
	Enable / Disable Broadcast SSID	X	X				X	X	X				X
• Encryption	No Encryption	X	X				X	X					X
	Dynamic Key Management	X	X				X	X					X
	3DES	X	X			X	X	X					X

[1] *The operator can view this setting*

[2] *The operator can change this setting*

[3] *The operator can add a required input. For example: Adding an entry to the MAC address filtering table*

[4] *The operator can delete a particular entry. For example: Deleting an entry from the MAC address filtering table*

[5] *The operator can zeroize these keys.*

[6] *The operator can reset this setting to its factory default value. This is done by performing a zeroize*

[7] *The operator can view this setting*

[8] *The operator can change this setting*

[9] *The operator can add a required input. For example: Adding an entry to the MAC address filtering table*

[10] *The operator can delete a particular entry. For example: Deleting an entry from the MAC address filtering table*

[11] *The operator can zeroize these keys.*

[12] *The operator can reset this setting to its factory default value. This is done by performing a zeroize*

Categories	Features	Operator Roles											
		CryptoOfficer						Administrator					
		Show[1]	Set[2]	Add[3]	Delete[4]	Zeroize[5]	Default Reset[6]	Show[7]	Set[8]	Add[9]	Delete[10]	Zeroize[11]	Default Reset[12]
	AES (128-/192-256-bit)	X	X			X	X	X					X
• Bridging	Client Access	X	X				X	X	X				X
	Spanning Tree Protocol	X	X				X	X	X				X
• Encryption	No Encryption	X	X				X	X					X
	3DES	X	X		X	X	X	X					X
	AES (128-/192-256-bit)	X	X		X	X	X	X					X
• MAC Address Filtering	Enable/Disable	X	X				X	X					X
	Add/Delete entry			X	X								
	Allow/Disallow Filter	X	X				X	X					X
• Rogue AP Detection	Enable/Disable	X	X				X	X	X				X
	Known AP MAC address			X	X								
	Email / Display rogue AP	X	X				X	X	X				X
Service Settings													
• DHCP Server	Enable / Disable	X	X				X	X	X				X
	Starting / Ending IP address	X	X				X	X	X				X
• Print Server	Enable/ Disable	X	X				X	X	X				X
User Management													
• List All Users		X		X	X		X	X					X
• Add New User			X										
Monitoring/Reports													
• System Status	Security Mode	X											
	Current Encryption Mode	X											
	Bridging encryption mode	X											
	System Uptime	X											
	Total Usable memory	X											
	Free Memory	X											
	Current Processes	X											
	Other Information	X											
	Network interface status	X											
• Bridging Status	Status of Layer 2 bridge devices	X						X					
• Wireless Clients	MAC Address (manfr's name)	X						X					
	Received Signal Strength	X						X					
	TX rate	X						X					
• Rogue AP List	AP MAC address	X						X					
	SSID	X						X					
	Channel	X						X					
	Signal	X						X					
	Noise	X						X					
	Type	X						X					
	Age	X						X					
	WEP	X						X					
• DHCP Client List	Client Hostname	X			X			X			X		
	IP Address	X			X			X			X		
	MAC Address (manfr's name)	X			X			X			X		
• System Log	Date/Time/Message	X			X			X			X		
• Web Access Log		X			X			X			X		

Categories	Features	Operator Roles											
		CryptoOfficer						Administrator					
		Show[1]	Set[2]	Add[3]	Delete[4]	Zeroize[5]	Default Reset[6]	Show[7]	Set[8]	Add[9]	Delete[10]	Zeroize[11]	Default Reset[12]
• Network Activities		X			X			X			X		
System Administration													
• Firmware Upgrade		X						X					
• Self-Test		X						X					
• Factory Defaults		X						X					
• Reboot		X						X					
• Utilities	Ping Traceroute	X X						X X					

User Role: This role is assumed by the wireless client workstation that uses static or dynamic key AES or 3DES encryption to communicate wirelessly with the Gateway AP. Authentication is implicitly selected by the correct knowledge of the static key, or for dynamic key encryption, EAP-TLS authentication is performed and the client uses its public key certificate to authenticate itself. The static key (TDES or AES key) is configured on the Gateway by the Crypto officer. The static key must be pre-shared between the Gateway and User. The Gateway supports 128 Users (client workstations) if MAC address filtering is disabled. If MAC address filtering is enabled, only 60 Users are allowed.

The only service available to the User role is the ability to send data to and through the 3e-DMG. All data is sent in the form of 802.11b wireless packets. All wireless communication is encrypted using either 3DES or AES encryption (based upon Gateway configuration). In bypass mode plaintext packets can also be sent to the Gateway

Security Server Role: This role is assumed by the authentication server, which is a self-contained workstation connected to the Gateway over the Ethernet Uplink WAN port. The security server is employed for authentication of wireless clients and key management activities. The Security Server is used only during dynamic key exchange. The Security Server authenticates using a shared secret which is used as an HMAC-SHA1 key to calculate the keyed hash of messages sent to the Gateway during dynamic key exchange. The Security Server IP address and password are configured on the Gateway by the Crypto Officer. Only one Security Server is supported.

The Security Server performs following services:

a) Authenticate wireless clients for the Gateway

b) Perform a DH key exchange with the Gateway to negotiate an AES key

c) Send unicast key to the Gateway encrypted with the AES key negotiated using a DH key exchange

2.1.2. Authentication Mechanisms and Strength

The following table summarizes the four roles and the type of authentication supported for each role:

Role	Type of Authentication	Authentication Data
Crypto Officer	Identity-based	Userid and password
Administrator	Identity-based	Userid and password
User	Role-based	Static Key (TDES or AES)
User	Role-based	CA signature (RSA with SHA-1)
User	Role-based	MAC address and CRC
Security Server	Role-based	HMAC SHA1 (Shared secret)

The following table identifies the strength of authentication for each authentication mechanism supported:

Authentication Mechanism	Strength of Mechanism
Userid and password	Minimum 6 characters => 72^6 = 1.39E11
Static Key (TDES or AES)	TDES (192-bits) or AES (128, 192, or 256-bits)
HMAC SHA-1 shared secret	Minimum 6 characters => 72^6 = 1.39E11
CA signature	128-bit
MAC address (6 bytes) and CRC (4 bytes)	10 bytes (80-bits).

3. Secure Operation and Security Rules

In order to operate the 3e-DMG securely, each operator should be aware of the security rules enforced by the module and should adhere to the physical security rules and secure operation rules detailed in this section.

3.1. Security Rules

The following 3e-DMG security rules must be followed by the operator in order to ensure secure operation:

1. Every operator (Crypto Officer or Administrator) has a user-id on the 3e-DMG. No operator will violate trust by sharing his/her password associated with the user-id with any other operator or entity.
2. The Crypto Officer will not share any key, or SRDI used by the 3e-DMG with any other operator or entity.
3. The Crypto Officer will not share any MAC address filtering information used by the 3e-DMG with any other operator or entity.

4. The operators will explicitly logoff by closing all secure browser sessions established with the 3e-DMG.
5. The operator will disable browser cookies and password storing mechanisms on the browser used for web configuration of the Gateway.
6. The Crypto officer is responsible for inspecting the tamper evident seals on a daily basis. A compromised tape reveals message "OPENED" with visible red dots. Other signs of tamper include wrinkles, tears and marks on or around the label.
7. The Crypto Officer should change the default password when configuring the Gateway for the first time. The default password should not be used.

3.2. Physical Security Rules

The following section contains detailed instructions to the Crypto Officer concerning where and how to apply the tamper evident seals to the Gateway enclosure, in order to provide physical security for FIPS 140-2 level 2 requirements.

Tools:

Wire Cutters (wire seal removal)

Materials:

Gateway, 3eTI – Quantity: 1
Seal, Tape, Tamper-evident – Quantity: 3
Isopropyl Alcohol Swab
3M Adhesive Remover (citrus or petroleum based solvent)

Installation – Tamper-evident tape

1. Locate on Gateway the placement locations of tamper-evident tape seals. (3 locations as shown in Figure 1, 2, and 3 for the 3e-521NP, 3e-531NP, and 3e-530NP and 4 locations as shown in Figures 4, 5, and 6 for the 3e-522FIPS).
2. Thoroughly clean area where tamper-evident tape seal is to be applied with isopropyl alcohol swab. Area must be clean of all oils and foreign matter (dirt, grime, etc.)
3. Record tracking number from tamper-evident tape seal.
4. Apply seal to locations on the 3e-521NP, 3e-531AP, and 3e-530NP Gateways as shown in Figures 1, 2, and 3. For the 3e-522FIPS Gateway seals must be applied as shown in Figures 4, 5, and 6. It is important to ensure that the seal has equal contact area with both top and bottom housings.
5. After application of seals to the Gateway, apply pressure to verify that adequate adhesion has taken place.

Removal – Tamper-evident tape

1. Locate on Gateway locations of tamper-evident tape seals. (3 locations as shown in Figures 1, 2, and 3 for the 3e-521NP, 3e-531AP, and 3e-530NP and 4 locations as shown in Figures 4, 5, and 6 for the 3e-522FIPS)

2. Record tracking numbers from existing tamper-evident tape seal and verify physical condition as not tampered or destroyed after installation.
3. Cut tape along seam of Gateway to allow opening of enclosure.
4. Using 3M adhesive remover or equivalent, remove residual tamper-evident seal tape. (three locations as shown in Figures 1, 2, and 3 for the 3e-521NP, 3e-531AP, and 3e-530NP and 4 locations as shown in Figures 4, 5, and 6 for the 3e-522NP)

This picture shows the physical interface side of the 3e-521NP3e-531AP, and 3e-530NP Gateway enclosure with tamper-evident seal.

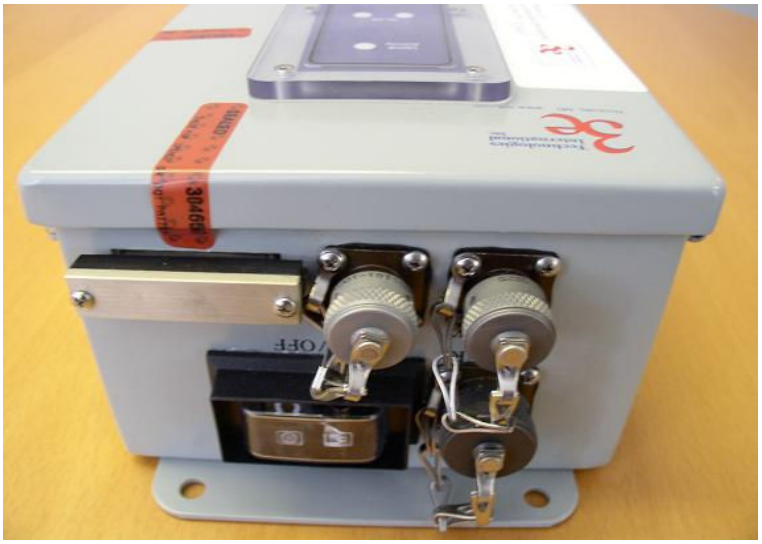


Figure 1

Side-view of the 3e-521NP, 3e-531AP, and 3e-530NP Gateway with tamper-evident seal:

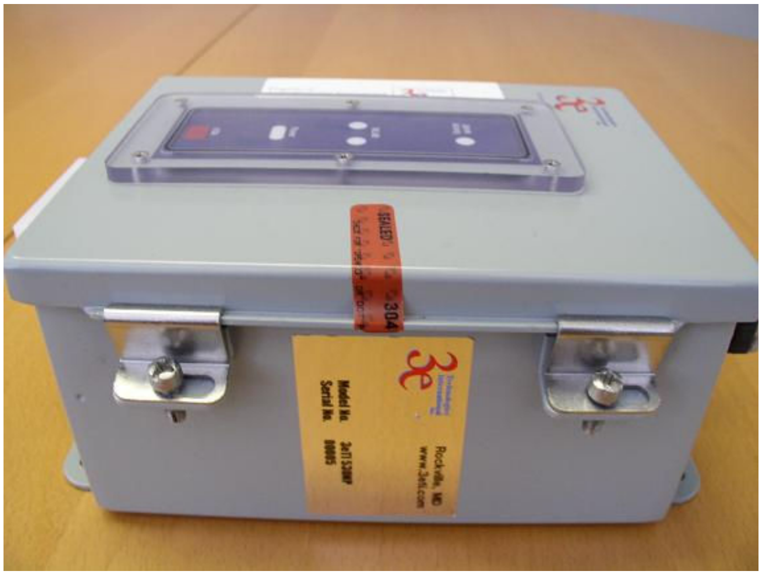


Figure 2

End-view of the 3e-521NP, 3e-531AP and 3e-530NP Gateway showing WLAN port and tamper-evident seal:

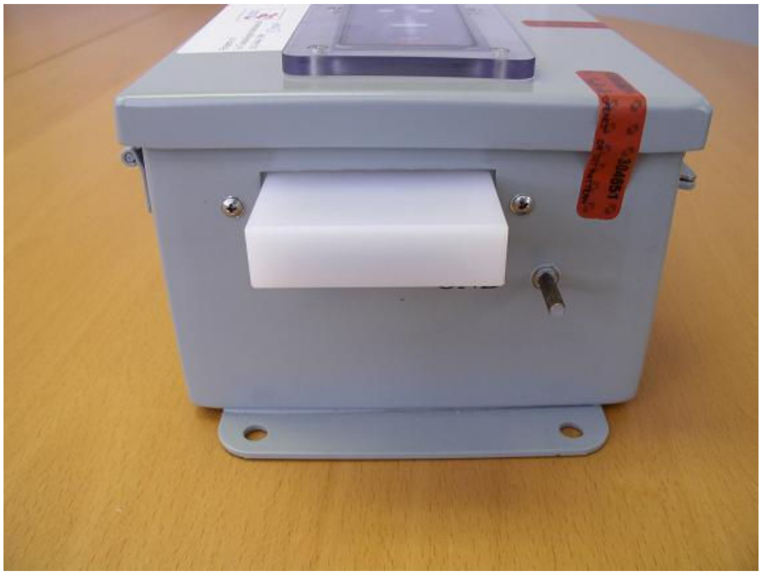


Figure 3

This picture shows the bottom view of the 3e-522FIPS Gateway, with tamper-evident tape covering the wall-hanging openings to prevent access to any internal circuitry.

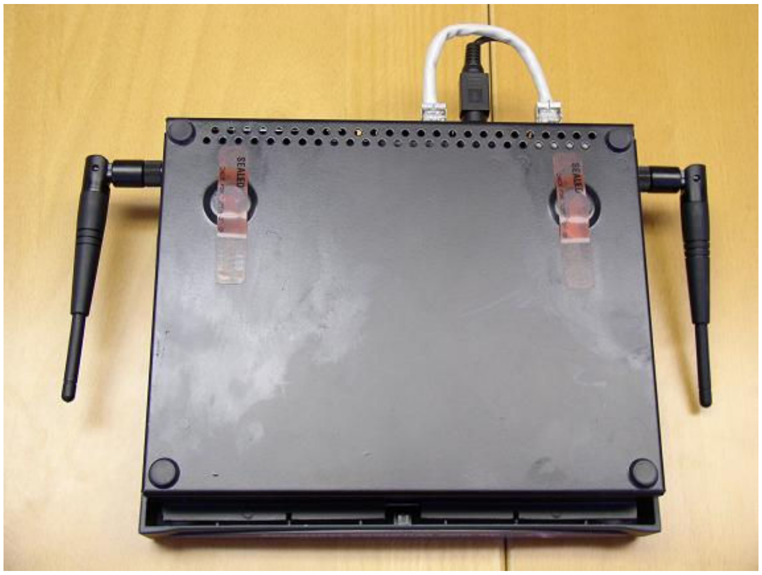


Figure 4

This picture shows the top right side of the 3e-522FIPS Gateway with tamper-evident tape securing the outer enclosure.

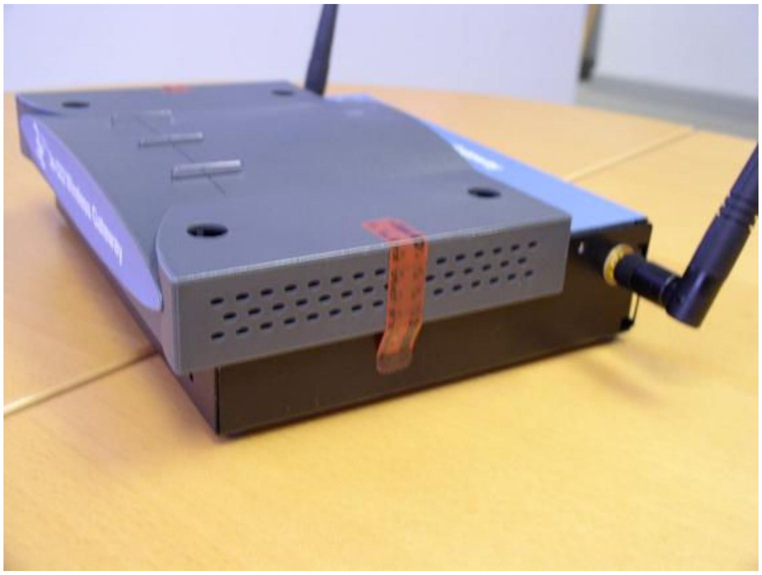


Figure 5

This picture shows the top left side of the3e-522FIPS Gateway with tamper-evident tape securing the outer enclosure.

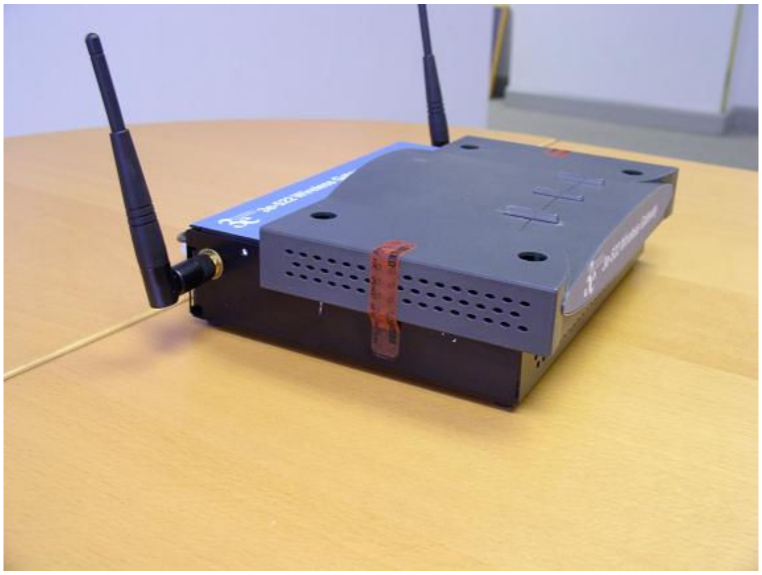
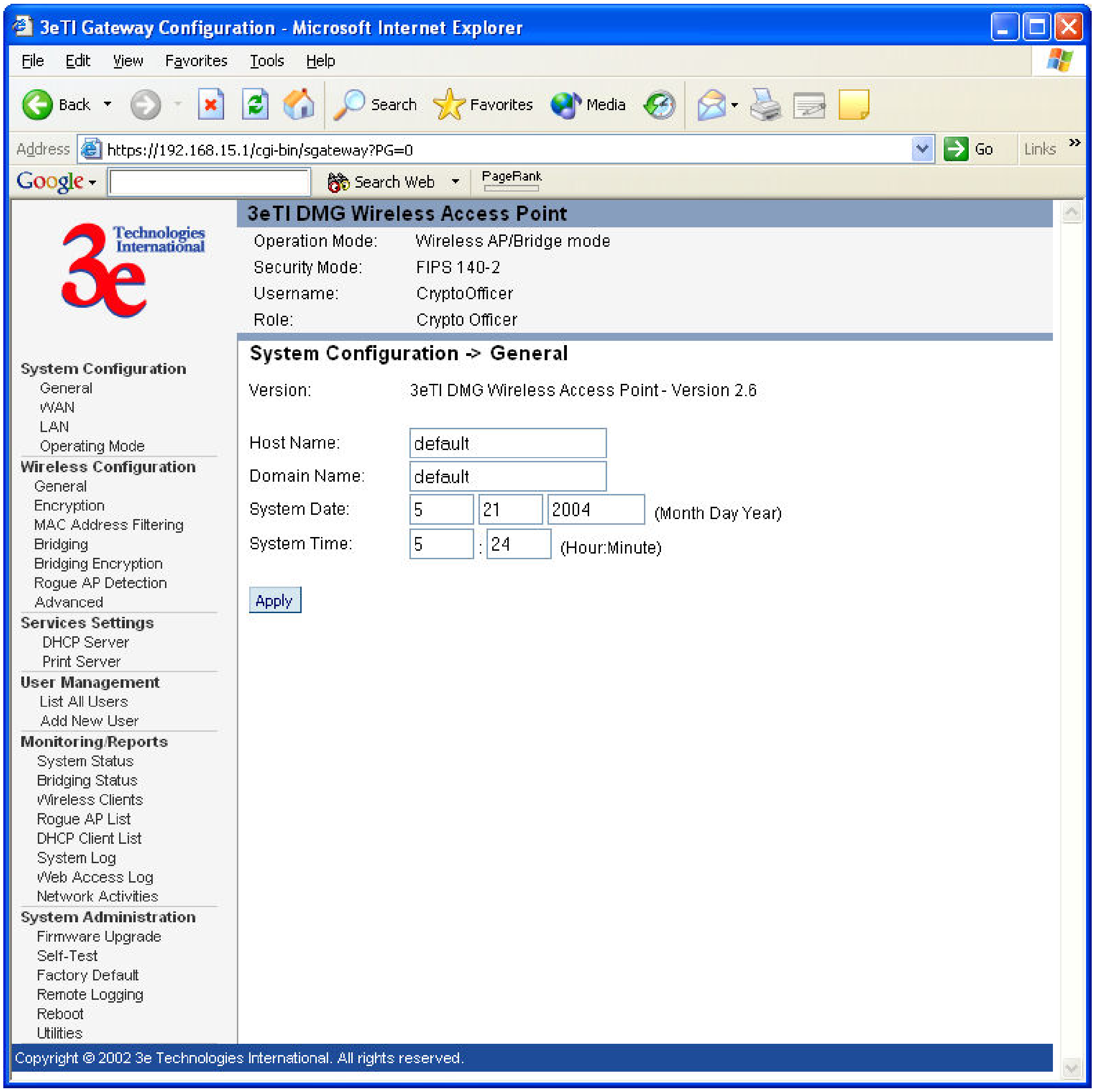


Figure 6

3.3. Secure Operation Initialization

There is a default Crypto Officer password, which can be used to access the configuration pages using HTTPS from any browser. The LAN port by default is configured with the IP address 192.168.15.1.

Using any browser, open the page https://192.168.15.1 to access the Gateway configuration. The main configuration page is shown below:



3eTI DMG Wireless Access Point

Operation Mode:	Wireless AP/Bridge mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer

System Configuration -> General

Version: 3eTI DMG Wireless Access Point - Version 2.6

Host Name: default

Domain Name: default

System Date: 5 21 2004 (Month Day Year)

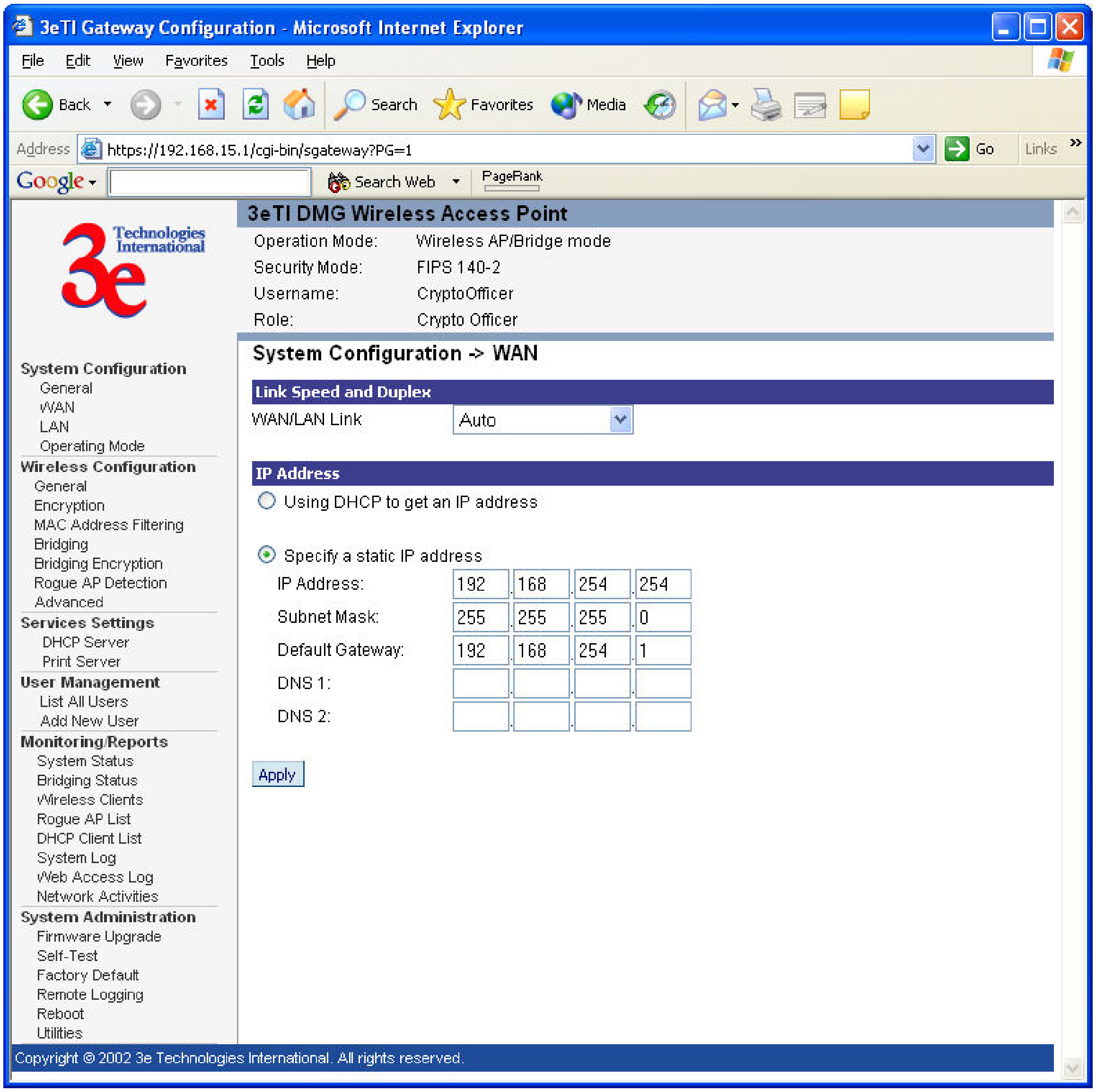
System Time: 5 : 24 (Hour:Minute)

Copyright © 2002 3e Technologies International. All rights reserved.

3.3.1. System Configuration

3.3.1.1. WAN Configuration

The IP address of the WAN interface can be configured with Static IP address or by using DHCP to obtain an IP address.



3eTI DMG Wireless Access Point

Operation Mode:	Wireless AP/Bridge mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer

System Configuration -> WAN

Link Speed and Duplex

WAN/LAN Link: Auto

IP Address

○ Using DHCP to get an IP address

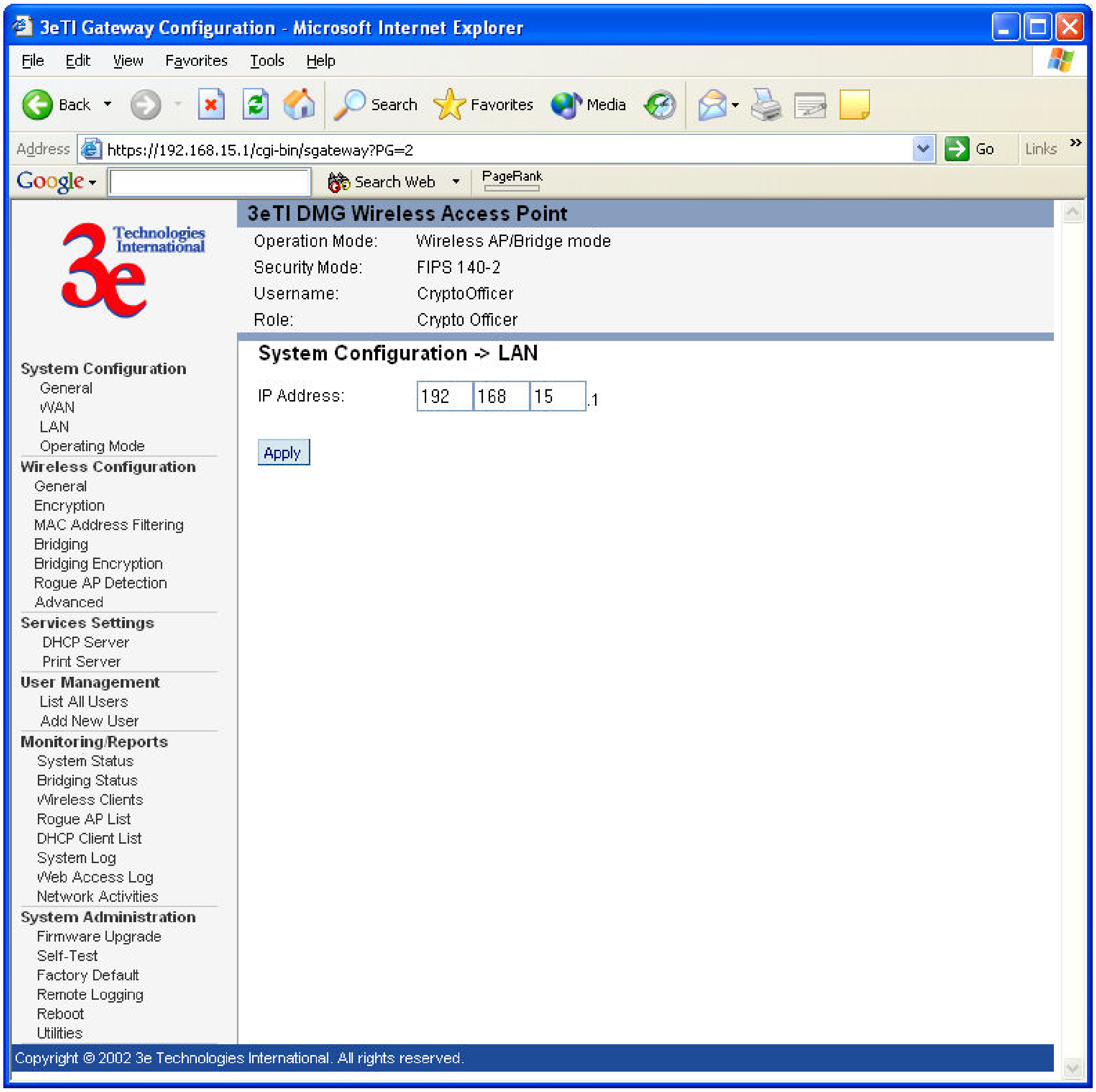
● Specify a static IP address

IP Address:	192	168	254	254
Subnet Mask:	255	255	255	0
Default Gateway:	192	168	254	1
DNS 1:				
DNS 2:				

Copyright © 2002 3e Technologies International. All rights reserved.

3.3.1.2. LAN Configuration

The IP address of the LAN interface can be configured with a static IP address, by using the link under System Configuration.



3eTI DMG Wireless Access Point

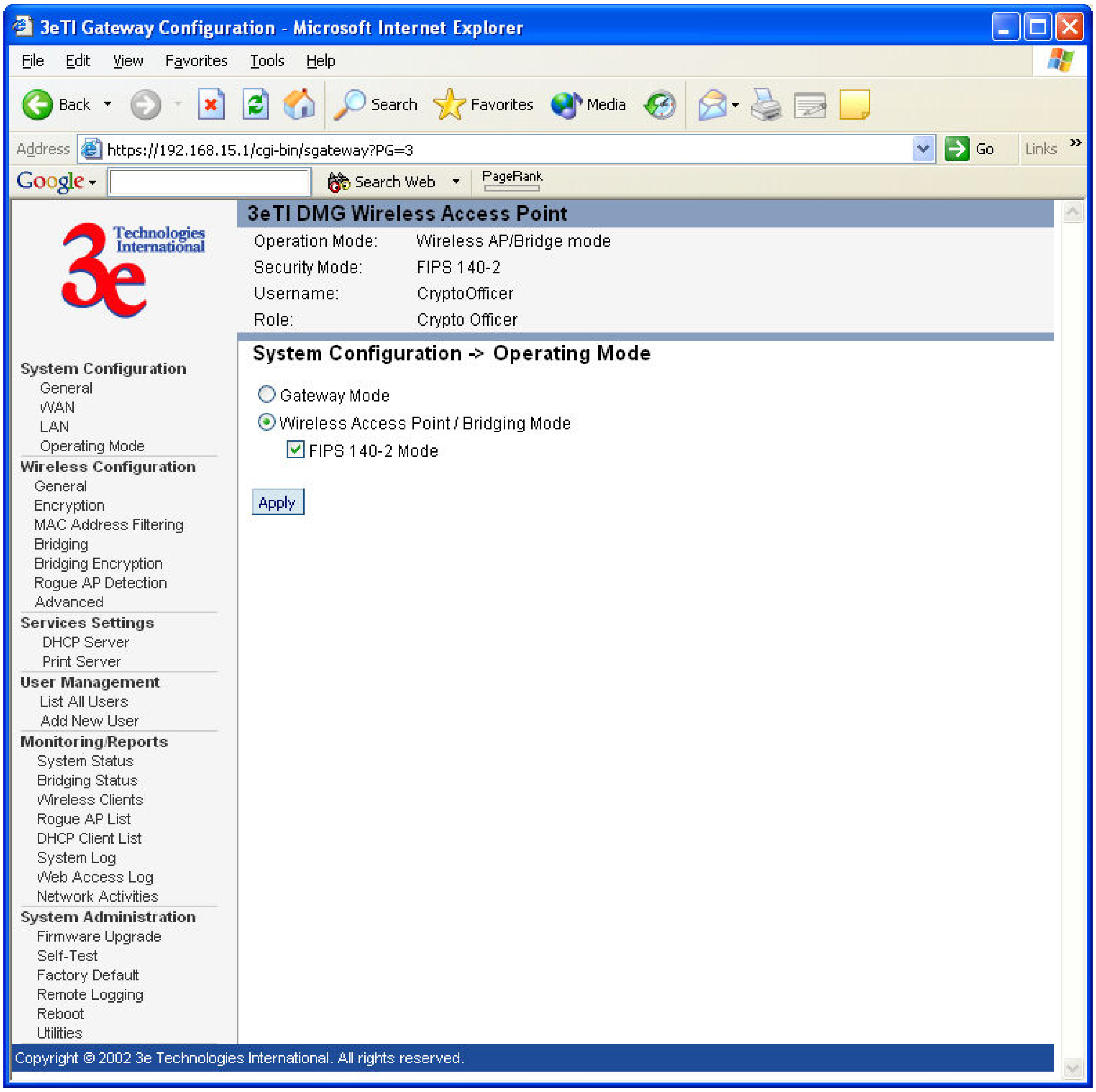
Operation Mode: Wireless AP/Bridge mode
Security Mode: FIPS 140-2
Username: CryptoOfficer
Role: Crypto Officer

System Configuration -> LAN

IP Address: 192 . 168 . 15 .1

3.3.1.3. Operating Mode

The gateway can be configured in *Gateway Mode – **non-FIPS**, Wireless Access Point/Bridging Mode – **FIPS** and Wireless Access Point/Bridging Mode- **non-FIPS*** by using the Operating Mode link. It is important to note that the unit will be reset to factory default when the Operating mode is changed.



3eTI DMG Wireless Access Point

Operation Mode:	Wireless AP/Bridge mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer

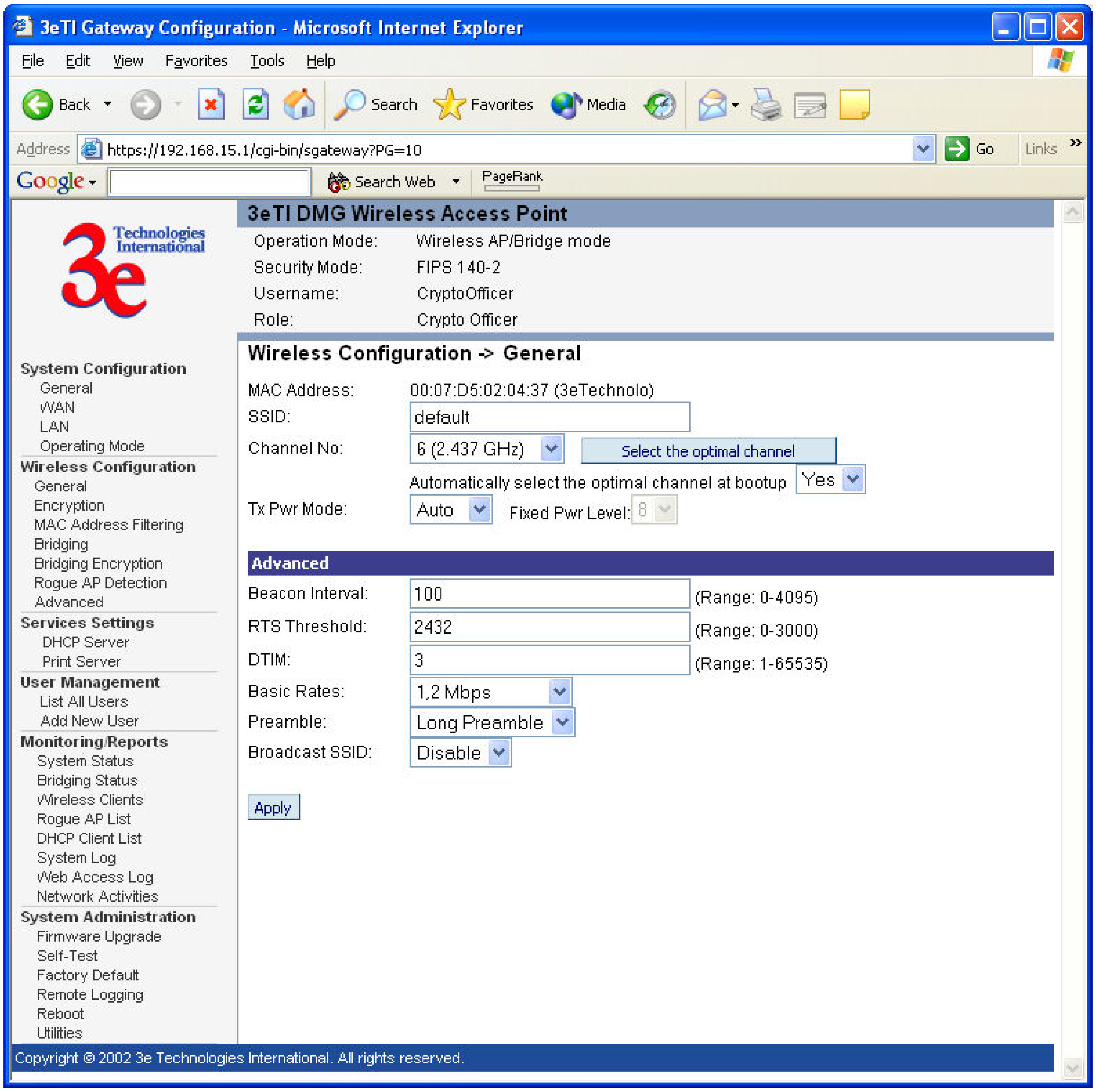
System Configuration -> Operating Mode

○ Gateway Mode
● Wireless Access Point / Bridging Mode
☑ FIPS 140-2 Mode

3.3.2. Wireless Configuration

3.3.2.1. General

This screen can be used to configure the access point's wireless settings like SSID, channel and transmit power.



https://192.168.15.1/cgi-bin/sgateway?PG=10

3eTI DMG Wireless Access Point

Operation Mode: Wireless AP/Bridge mode
Security Mode: FIPS 140-2
Username: CryptoOfficer
Role: Crypto Officer

Wireless Configuration -> General

MAC Address: 00:07:D5:02:04:37 (3eTechnolo)
SSID: default
Channel No: 6 (2.437 GHz)
Automatically select the optimal channel at bootup: Yes
Tx Pwr Mode: Auto   Fixed Pwr Level: 8

Advanced

Beacon Interval: 100 (Range: 0-4095)
RTS Threshold: 2432 (Range: 0-3000)
DTIM: 3 (Range: 1-65535)
Basic Rates: 1,2 Mbps
Preamble: Long Preamble
Broadcast SSID: Disable

Copyright © 2002 3e Technologies International. All rights reserved.

3.3.2.2. Encryption

No Data Encryption

Factory default sets the encryption to "*No Data Encryption*". This results in all wireless traffic being sent in plaintext form.

Dynamic Key Management

Using this configuration, the Crypto Officer can set per session keys dynamically.

The configuration entails the following:

Gateway Configuration:

- Configure the IP address of the radius server in the *Security Server IP Address* box.
- Configure the port number of the radius server.
- Configure the Radius Server password.
- Select the type of key. The options available are:
  - AES 128-bit key
  - AES 192-bit key
  - AES 256-bit key
  - 3DES key

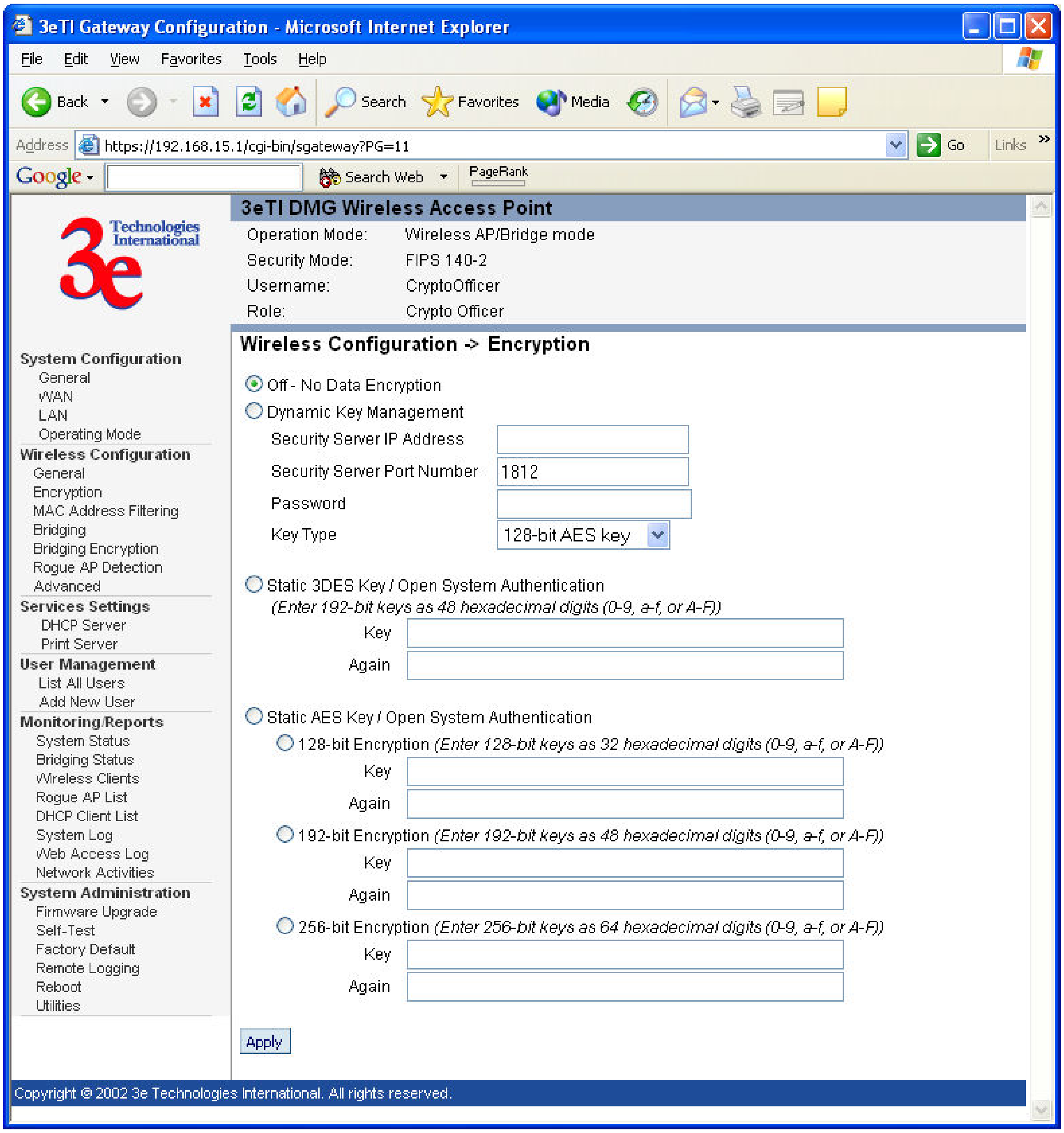
Static 3DES Key

The Crypto Officer can configure the AP to use static 3DES key (192-bit).

Static AES Key

The Crypto Officer can configure the AP to use static AES keys. The following AES keys can be configured:

- AES 128-bit key
- AES 192-bit key
- AES 256-bit key



3eTI Gateway Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://192.168.15.1/cgi-bin/sgateway?PG=11
Go Links
Google Search Web PageRank
Technologies International

3eTI DMG Wireless Access Point

Operation Mode:	Wireless AP/Bridge mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer

System Configuration
- General
- WAN
- LAN
- Operating Mode

Wireless Configuration
- General
- Encryption
- MAC Address Filtering
- Bridging
- Bridging Encryption
- Rogue AP Detection
- Advanced

Services Settings
- DHCP Server
- Print Server

User Management
- List All Users
- Add New User

Monitoring/Reports
- System Status
- Bridging Status
- Wireless Clients
- Rogue AP List
- DHCP Client List
- System Log
- Web Access Log
- Network Activities

System Administration
- Firmware Upgrade
- Self-Test
- Factory Default
- Remote Logging
- Reboot
- Utilities

Wireless Configuration -> Encryption

● Off - No Data Encryption

○ Dynamic Key Management

Security Server IP Address	
Security Server Port Number	1812
Password	
Key Type	128-bit AES key

○ Static 3DES Key / Open System Authentication

(Enter 192-bit keys as 48 hexadecimal digits (0-9, a-f, or A-F))

Key

Again

○ Static AES Key / Open System Authentication

○ 128-bit Encryption *(Enter 128-bit keys as 32 hexadecimal digits (0-9, a-f, or A-F))*

Key

Again

○ 192-bit Encryption *(Enter 192-bit keys as 48 hexadecimal digits (0-9, a-f, or A-F))*

Key

Again

○ 256-bit Encryption *(Enter 256-bit keys as 64 hexadecimal digits (0-9, a-f, or A-F))*

Key

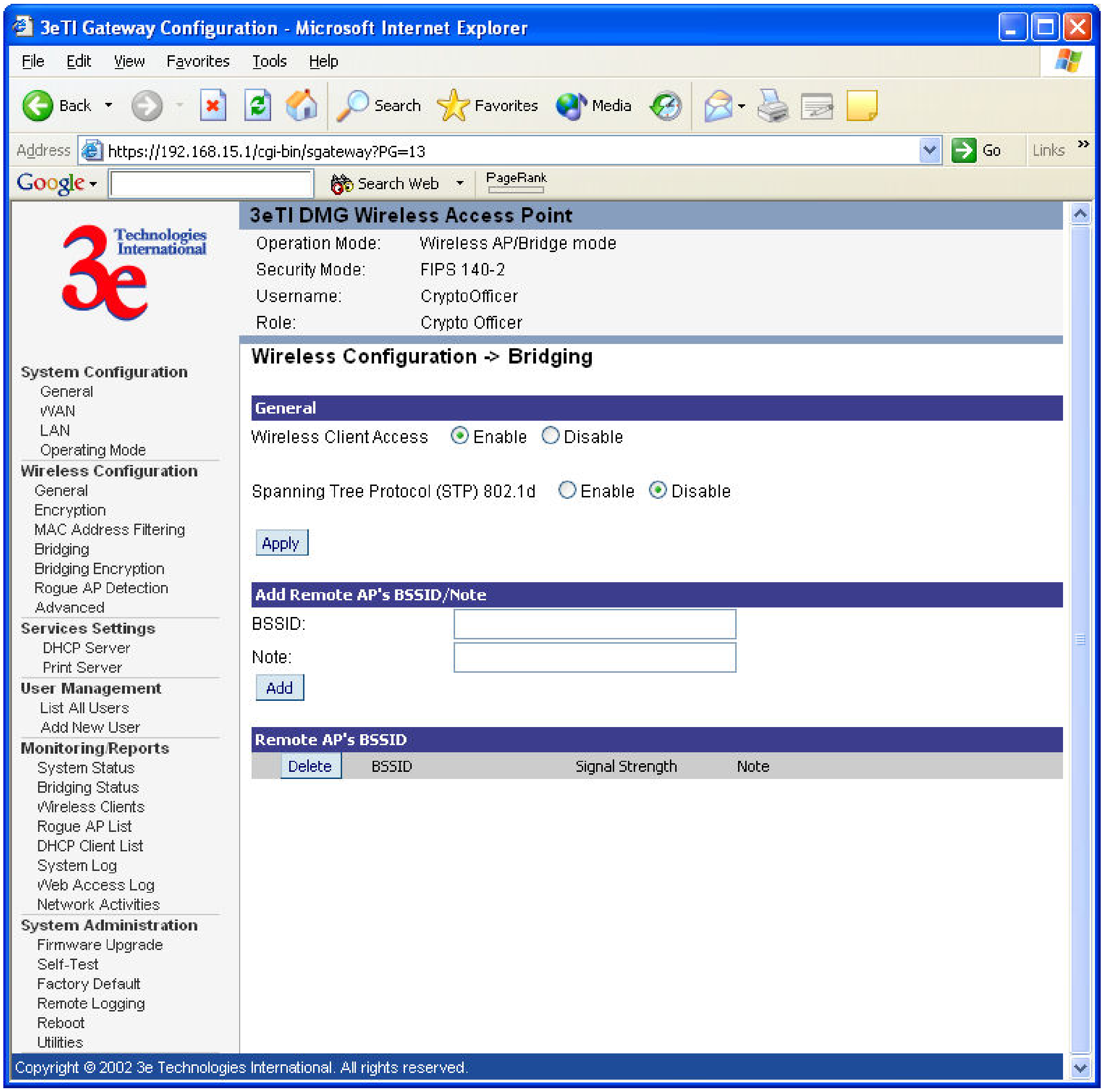
Again

Apply

Copyright © 2002 3e Technologies International. All rights reserved.

3.3.2.3. Bridging

This screen is used to configure the remote bridging devices. The MAC address of the remote bridge is needed to allow the two bridges to communicate.



Address: https://192.168.15.1/cgi-bin/sgateway?PG=13

3eTI DMG Wireless Access Point

Operation Mode:	Wireless AP/Bridge mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer

Wireless Configuration -> Bridging

General

Wireless Client Access ● Enable ○ Disable

Spanning Tree Protocol (STP) 802.1d ○ Enable ● Disable

Add Remote AP's BSSID/Note

BSSID:

Note:

Remote AP's BSSID

Delete	BSSID	Signal Strength	Note

Copyright © 2002 3e Technologies International. All rights reserved.

3.3.2.4. Bridging Encryption

No Data Encryption

Factory default sets the encryption to "*No Data Encryption*". This results in all bridging traffic being sent in plaintext form.

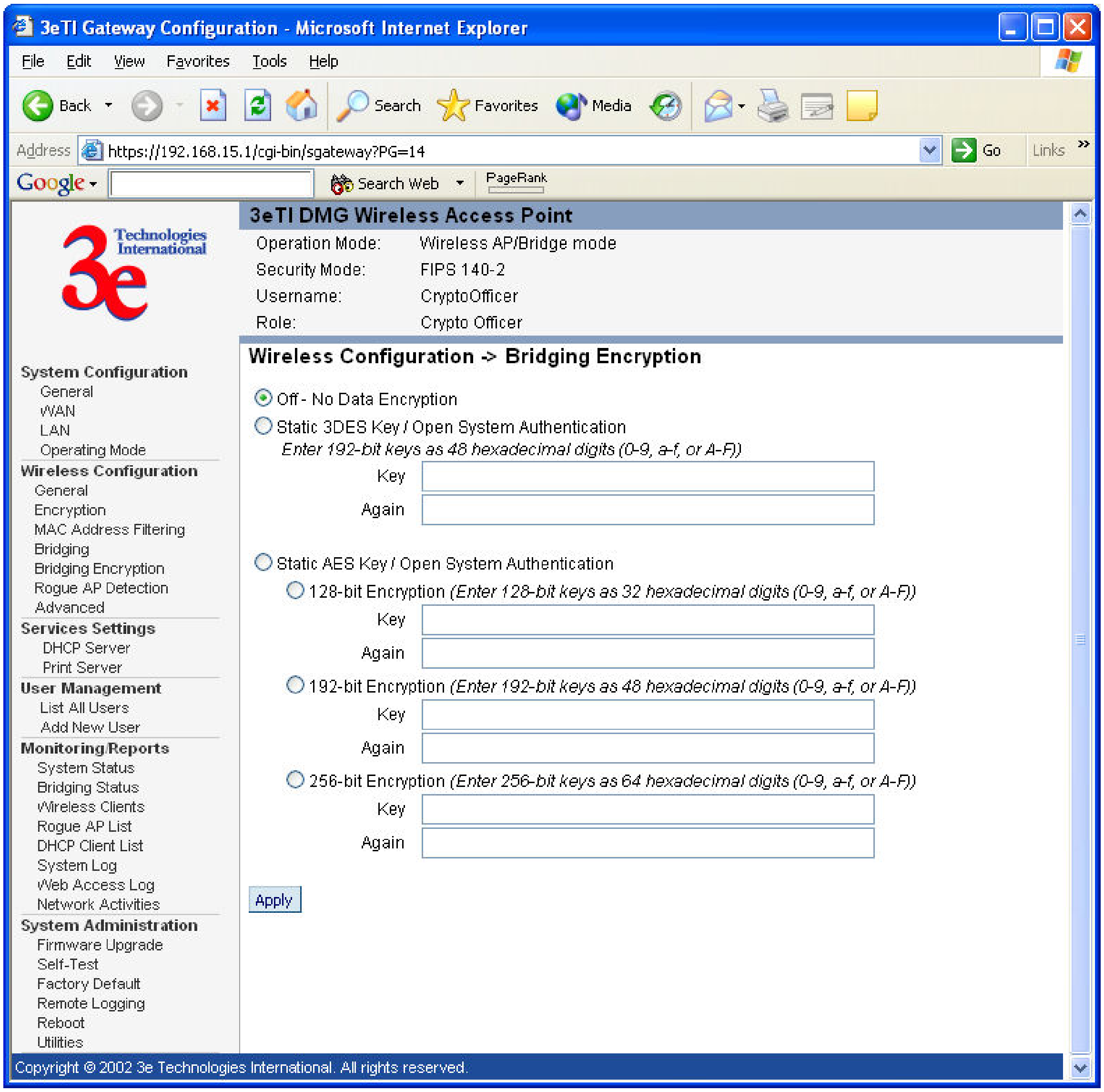
Static 3DES Key

The Crypto Officer can configure the bridge to use static 3DES key (192-bit).

Static AES Key

The Crypto Officer can configure the bridge to use AES keys. The following AES keys can be configured:

- AES 128-bit key
- AES 192-bit key
- AES 256-bit key



3eTI DMG Wireless Access Point

Operation Mode:	Wireless AP/Bridge mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer

Wireless Configuration -> Bridging Encryption

● Off - No Data Encryption

○ Static 3DES Key / Open System Authentication

Enter 192-bit keys as 48 hexadecimal digits (0-9, a-f, or A-F)

Key

Again

○ Static AES Key / Open System Authentication

○ 128-bit Encryption *(Enter 128-bit keys as 32 hexadecimal digits (0-9, a-f, or A-F))*

Key

Again

○ 192-bit Encryption *(Enter 192-bit keys as 48 hexadecimal digits (0-9, a-f, or A-F))*

Key

Again

○ 256-bit Encryption *(Enter 256-bit keys as 64 hexadecimal digits (0-9, a-f, or A-F))*

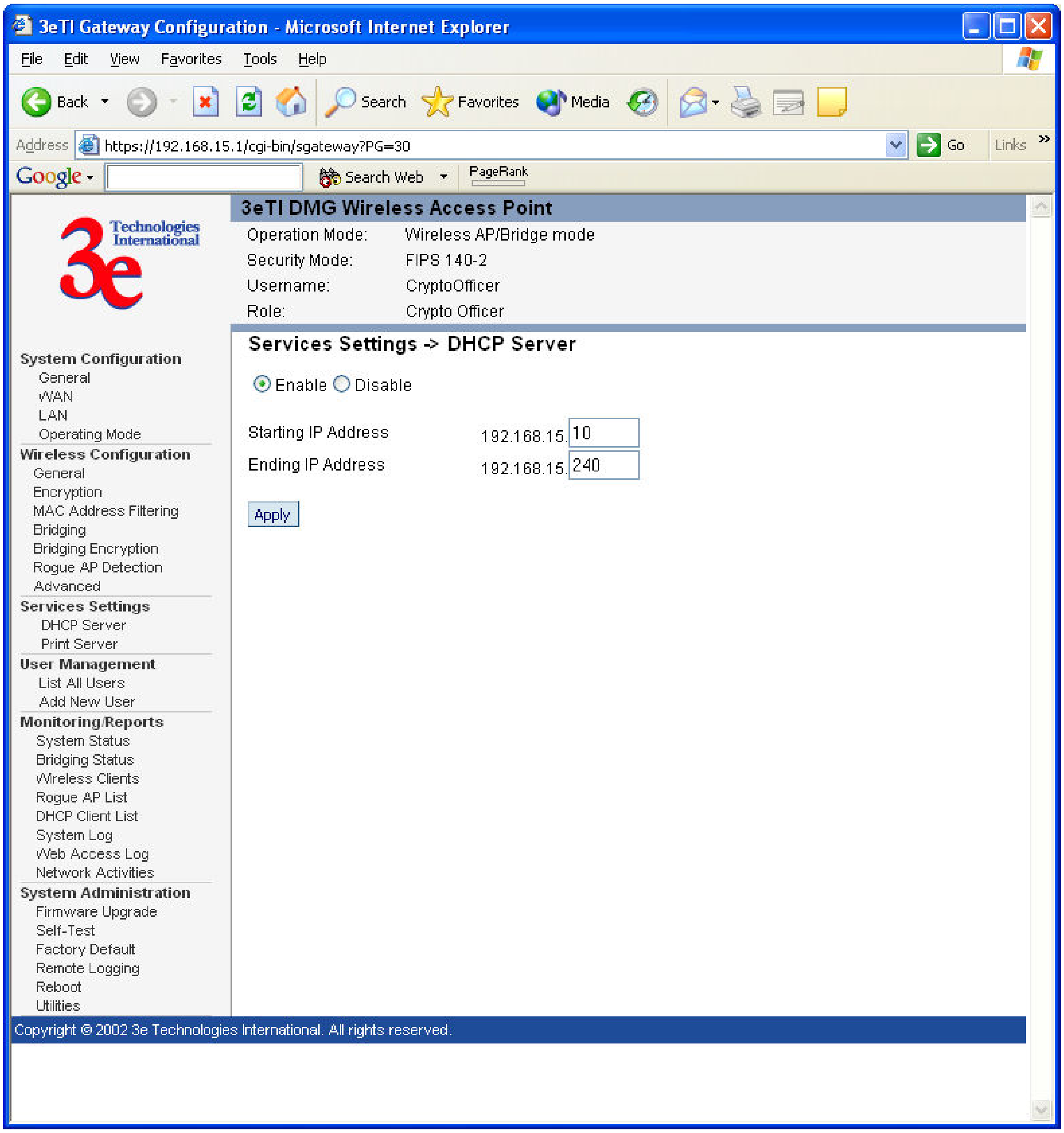
Key

Again

3.3.3. Services Settings

Using this link, the DHCP server for the LAN port can be configured.

- The DHCP server can be enabled or disabled.
- The IP address range can be configured.



3eTI DMG Wireless Access Point

Operation Mode:	Wireless AP/Bridge mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer

Services Settings -> DHCP Server

● Enable ○ Disable

Starting IP Address	192.168.15. 10
Ending IP Address	192.168.15. 240

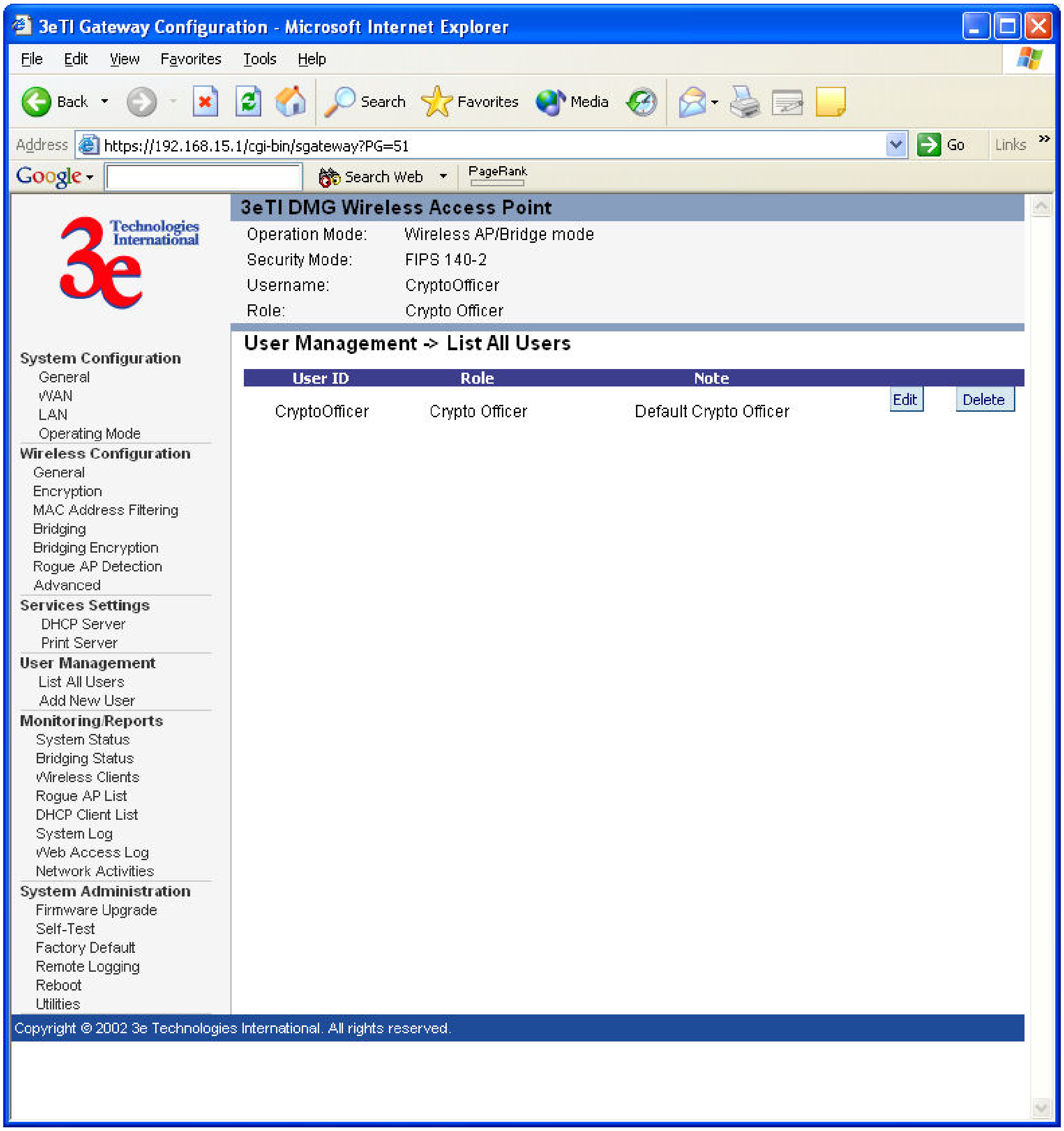
Apply

Copyright © 2002 3e Technologies International. All rights reserved.

3.3.4. User Management

3.3.4.1. List All Users

A list of the Crypto Officer and Administrator(s) by user ID is included.



3eTI DMG Wireless Access Point

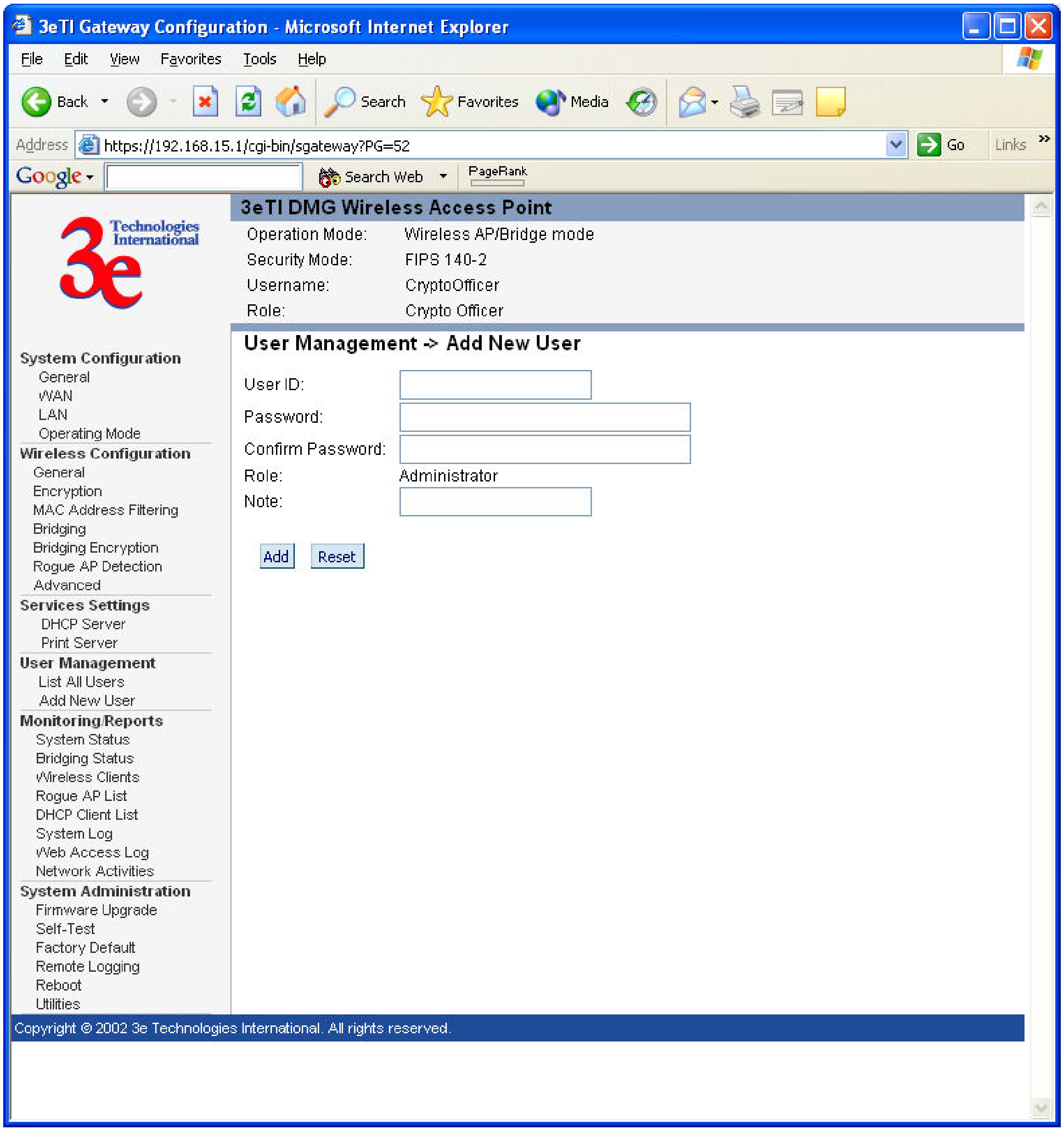
Operation Mode:	Wireless AP/Bridge mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer

User Management -> List All Users

User ID	Role	Note		
CryptoOfficer	Crypto Officer	Default Crypto Officer	Edit	Delete

3.3.4.2. Add New User

Only Crypto Officer is able to add a new user (Administrator) to the Gateway.



3eTI Gateway Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links
Google
Search Web
PageRank

https://192.168.15.1/cgi-bin/sgateway?PG=52

3eTI DMG Wireless Access Point

Operation Mode:	Wireless AP/Bridge mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer

User Management -> Add New User

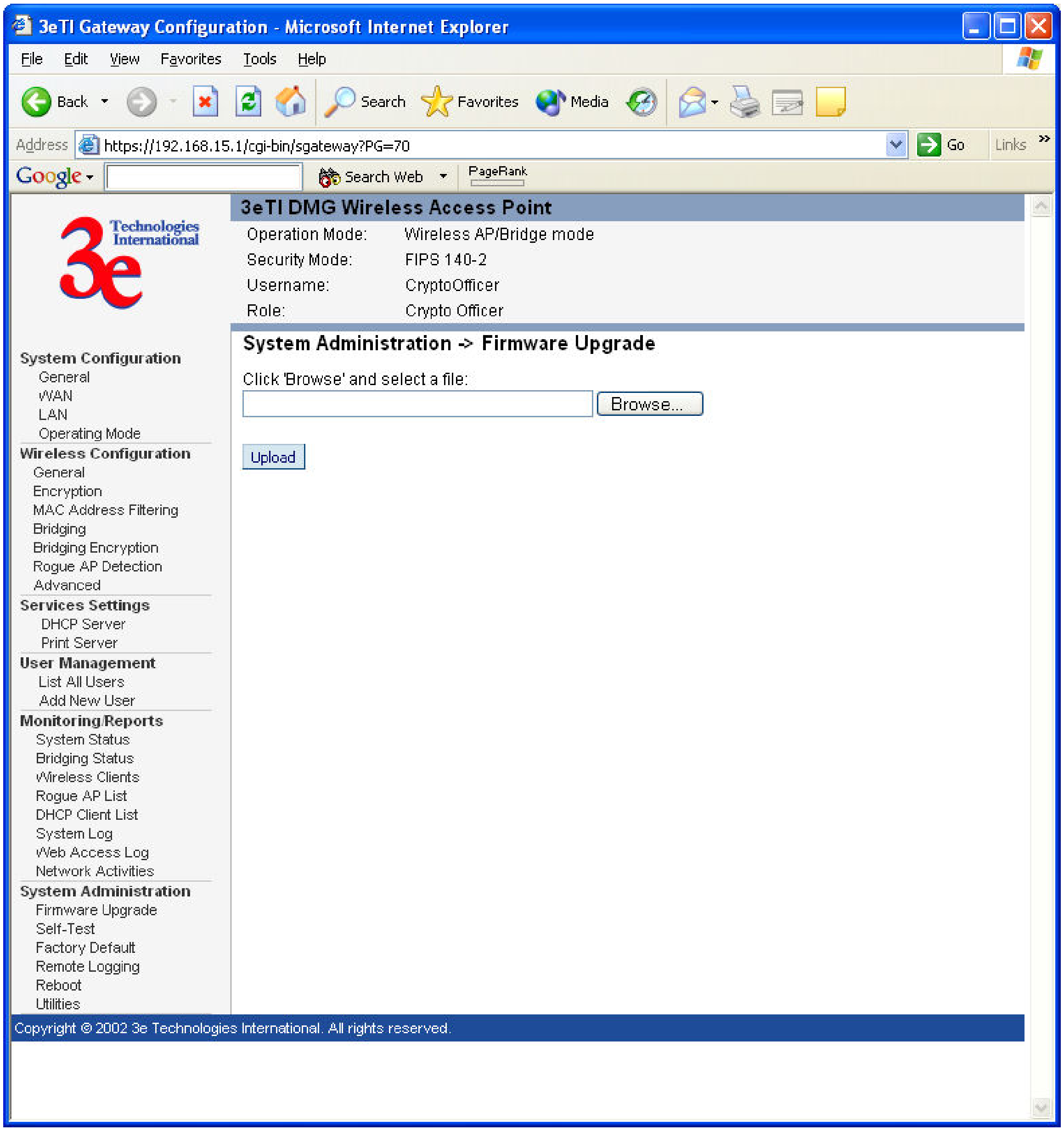
User ID:	
Password:	
Confirm Password:	
Role:	Administrator
Note:	

Copyright © 2002 3e Technologies International. All rights reserved.

3.3.5. System Administration

3.3.5.1. Firmware Upgrade

Only the Crypto Officer can select a file to upload for firmware upgrade.



3eTI DMG Wireless Access Point

Operation Mode: Wireless AP/Bridge mode
Security Mode: FIPS 140-2
Username: CryptoOfficer
Role: Crypto Officer

System Administration -> Firmware Upgrade

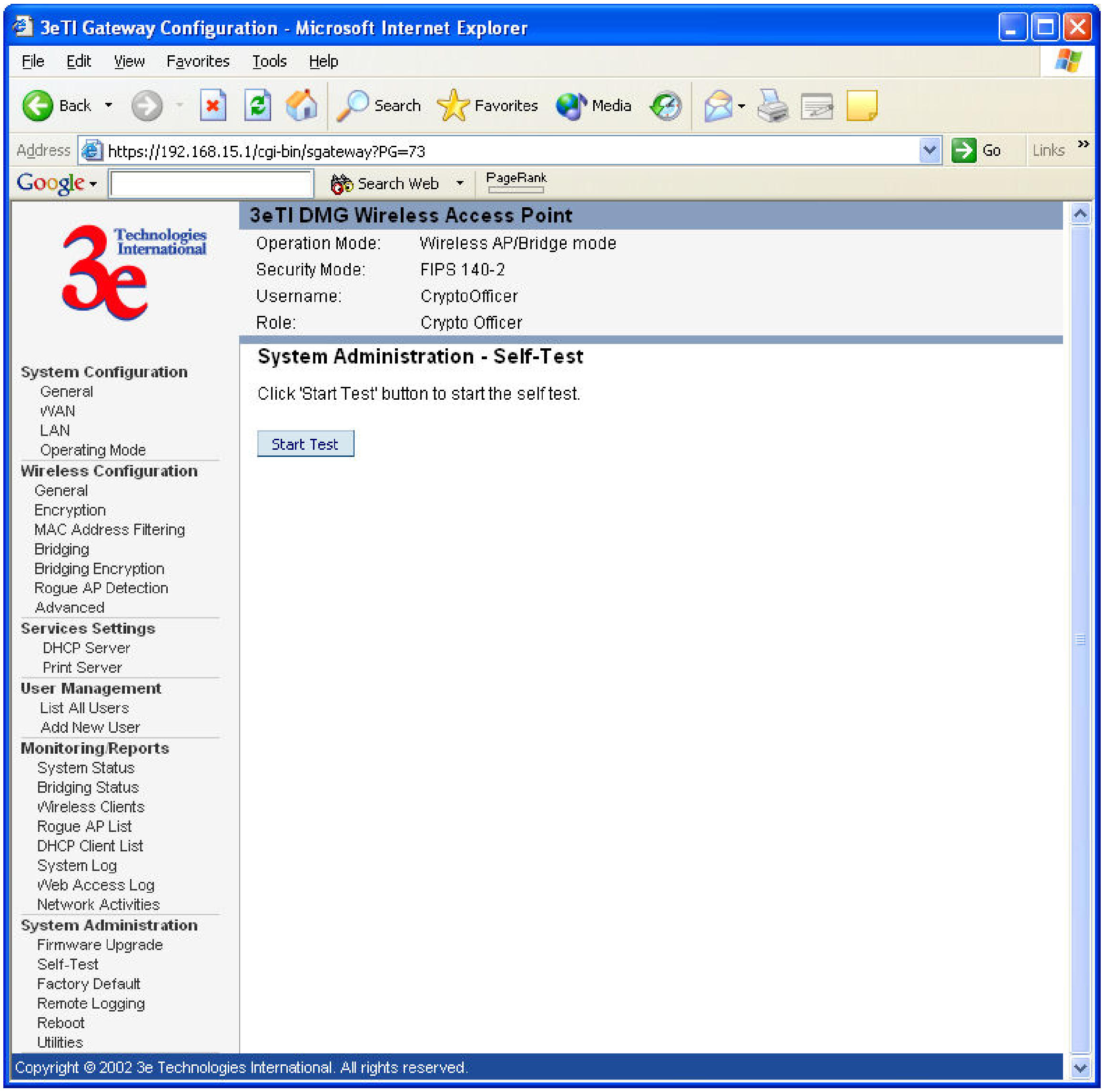
Click 'Browse' and select a file:

Copyright © 2002 3e Technologies International. All rights reserved.

3.3.5.2. Self-Tests

Both Crypto Officer and Administrators can initiate the self-test suite.

The test takes few seconds to complete. A beep will be heard at the end of the test and the result will be displayed. The self-test suite covers AES, 3DES, SHA-1, HMAC SHA-1, PRNG, Diffie Hellman for Dynamic Key Exchange, RSA decryption and SHA1 algorithm for firmware integrity test.



3eTI DMG Wireless Access Point

Operation Mode: Wireless AP/Bridge mode
Security Mode: FIPS 140-2
Username: CryptoOfficer
Role: Crypto Officer

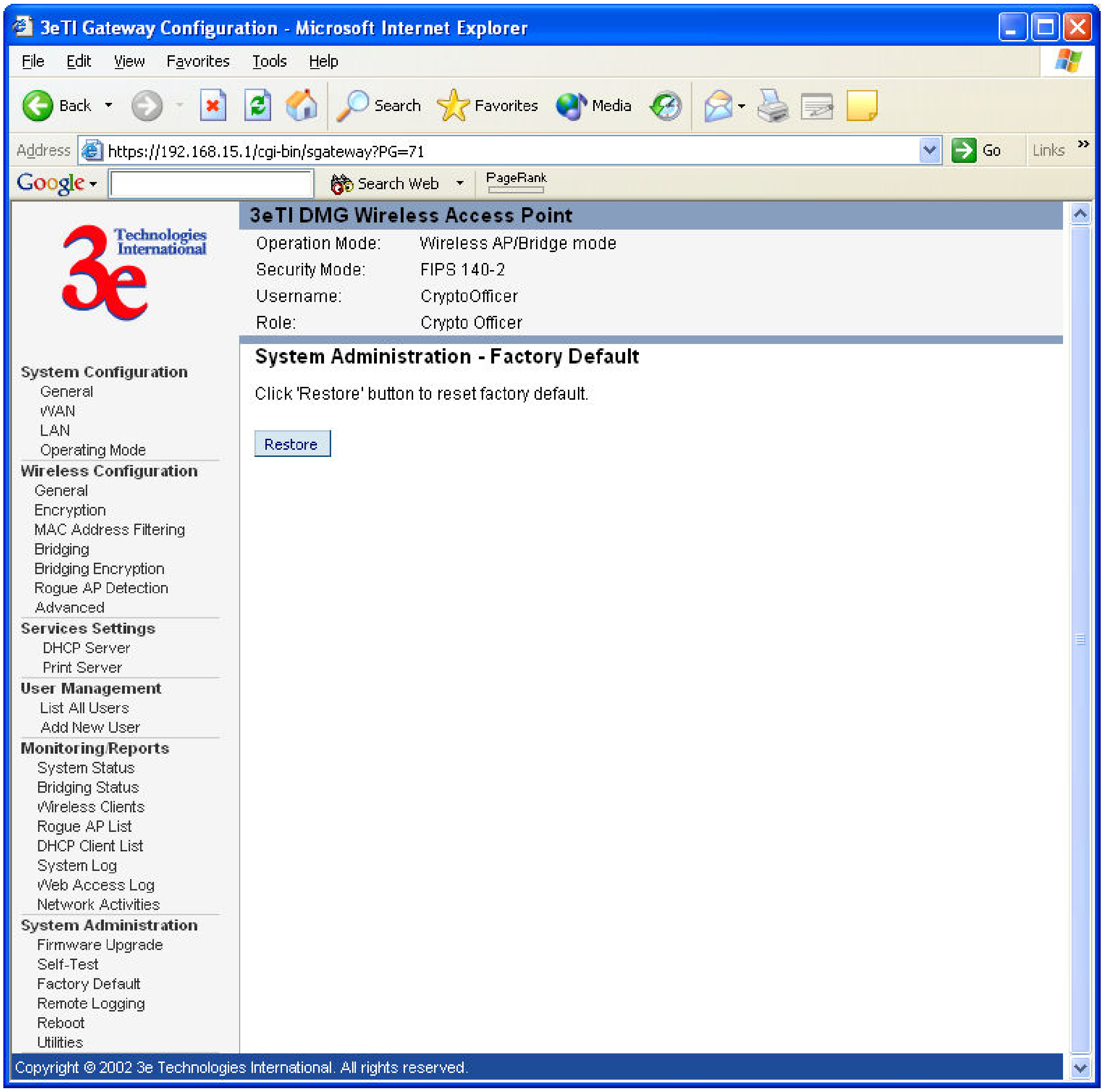
System Administration - Self-Test

Click 'Start Test' button to start the self test.

Copyright © 2002 3e Technologies International. All rights reserved.

3.3.5.3. Factory Default

Only the Crypto Officer can restore the Gateway to the factory default settings. For the 3e-522FIPS Gateway a Reset switch is provided on the back chassis that achieves the same goal. When this switch is depressed for 10 seconds or longer it resets the module back to factory default settings.



3eTI DMG Wireless Access Point

Operation Mode:	Wireless AP/Bridge mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer

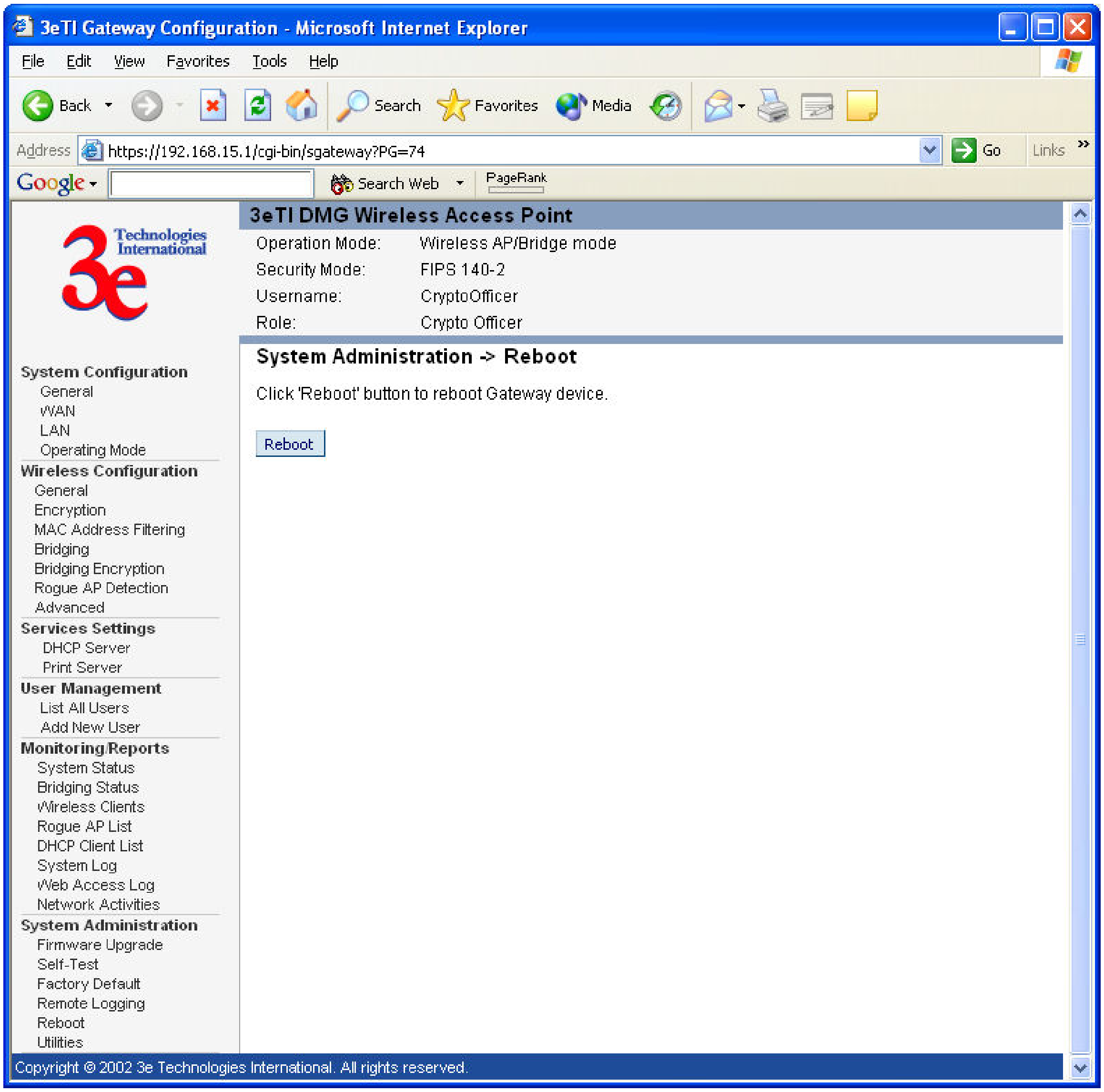
System Administration - Factory Default

Click 'Restore' button to reset factory default.

Copyright © 2002 3e Technologies International. All rights reserved.

3.3.5.4. Reboot

Both Crypto Officer and Administrators can reboot the Gateway.



https://192.168.15.1/cgi-bin/sgateway?PG=74

3eTI DMG Wireless Access Point

Operation Mode:	Wireless AP/Bridge mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer

System Administration -> Reboot

Click 'Reboot' button to reboot Gateway device.

Copyright © 2002 3e Technologies International. All rights reserved.

4. Security Relevant Data Items

This section specifies the 3e-DMG's Security Relevant Data Items (SRDIs) as well as the access control policy enforced by the 3e-DMG.

4.1. Cryptographic Algorithms

The 3e-DMG supports the following FIPS Approved cryptographic algorithms:

- TDES (ECB, CBC modes; 192-bit keysize)
- AES (ECB mode; 128, 192, 256-bit keysizes)
- SHA-1
- HMAC-SHA1

The 3e-DMG also supports the following non-FIPS cryptographic algorithms:

- Diffie Hellman (1024-bit modulus)[+]
- RSA decrypt (PKCS#1) for key un-wrapping[+]
- RC4 (used in WEP)
- MD5 hashing (used in MS-CHAP for PPPoE)
- DES (CBC) (used in SNMP v3)

4.2. Cryptographic Keys and SRDIs

The 3e-DMG contains the following security relevant data items:

Security Relevant Data Items	SRDI Description	Key Zero-izing
AES or 3DES Static Key	Data encryption/decryption using an AES static key (128, 192, or 256-bits) or 3DES static key (192-bits)	The keys can be zeroized through factory default or if CryptoOfficer changes keys.
AES or 3DES Dynamic Broadcast Key	Data encryption/decryption using an internally generated AES key (128, 192, or 256-bits) or 3DES (192-bits)	Key is zero-ized on a power-cycle, CryptoOfficer changes from DKE mode to static key mode, or re-applies DKE mode.
AES or 3DES Dynamic Unicast Key	Data encryption/decryption using an dynamically exchanged AES key (128, 192, or 256-bits) or 3DES (192-bits)	Key is zero-ized on a power-cycle, CryptoOfficer changes from DKE mode to static key mode, DKE mode is re-applied, or a client disassociates.
AES Internal Key	Used to encrypt configuration file	Key is zero-ized when application is overwritten.

[+] Used in FIPS mode of operation.

AES Post-Authentication Key	AES Key used to decrypt the 3DES/AES Dynamic Unicast Key	Key is zero-ized on a power-cycle, CryptoOfficer changes from DKE mode to static key mode, or DKE mode is re-applied.
HMAC SHA-1 Key	Key used to verify firmware integrity and authenticity during firmware upgrade	Key is zero-ized when application is overwritten.
HMAC SHA-1 Shared Secret	Secret used to authenticate the Security Server	Key is zero-ized on a power-cycle, CryptoOfficer changes from DKE mode to static key mode, or DKE mode is re-applied.
TLS Session Key	TDES key used to encrypt/decrypt configuration sessions (via HTTPS)	This key is zeroized when the module is power cycled.
RSA Private Key	Used to decrypt pre-master key in TLS negotiation	N/A since the key is stored encrypted.
TDES Key	Used to encrypt private key file	Key is zero-ized when application is overwritten.
Crypto-officer password	CO Password	Zero-ized when password is changed.
Administrator password	Administrator Password	Zero-ized when administrator is deleted.
CA signature	User certificate (Dynamic Key Exchange)	Zeroized by power cycling the module
MAC address and CRC	User MAC (Bypass mode)	Zeroized by power cycling the module

4.3. Access Control Policy

The 3e-DMG maintains and enforces the access control policy for each SRDI stored within the module. These access control policies cannot be changed or modified by any role within the module. The permissions are categorized as a set of three separate permissions: read (R), write (W), execute (E). If no permission is listed, then the operator cannot access the SRDI. The following table defines the access that an operator has to each SRDI and through which services.

3e-DMG SRDI Roles and Services Access Policy	Security Relevant Data Item	AES or TDES Static Key	AES or TDES Dynamic Broadcast	AES or TDES Dynamic Unicast	AES Internal Key	AES Post-authentication Key	HMAC SHA-1 Key	HMAC SHA-1 Shared Secret	TLS Session Key	RSA Private Key	TDES Key	CO Password	Administrator Password	CA Signature	MAC address and CRC
Role/Service															
Crypto-officer Role															
System Configuration					E				E	E	E				
Wireless Configuration		W			E			W	E	E	E				
Service Settings					E				E	E					
User Management									E	E		W	W		
Monitoring/Reporting					E				E	E					
System Administration					E		E		E	E					
Administrator Role															
System Configuration					E				E	E					
Wireless Configuration					E				E	E					
Service Settings					E				E	E					
User Management									E	E			W		
Monitoring/Reporting					E				E	E					
System Administration					E				E	E					
User Role															
Sending data		E	E	E											E
Authentication Server Role															
Provides authentication				W		W		E						E	