

## Restore the appliance to factory default (configured)

---

Slide 1

Tivoli

IBM

IBM Security Network Intrusion Prevention System V4.1

Restore the appliance to factory default (configured)



This is a self-running demonstration that shows you how to complete a task.  
Controls are available at the bottom of the screen.

© Copyright IBM Corporation 2011 All rights reserved.

## **Restore the appliance to factory default (configured)**

---

Slide 2



### Objectives

When you complete this module, you should be able to perform the following tasks:

- Define the factory default restoration options
- Restore the appliance to the factory default settings and maintain some settings

© 2011 IBM Corporation

## Restore the appliance to factory default (configured)

---

Slide 3



### Restoring the appliance

There are two options you can use to restore your IBM Security Network Intrusion Prevention appliance to the default settings:

- **Restore the appliance to factory default (configured)**, which preserves:
  - User name and password
  - Network configuration
  - Host configuration such as the appliance host name and domain name
- **Restore the appliance to factory default (unconfigured)**, which removes all of the appliance settings

**Note:** You can restore the appliance using either the management port or console port.

© 2011 IBM Corporation

## Restore the appliance to factory default (configured)

---

Slide 4

The screenshot shows the 'IBM Proventia GU1000 Setup' interface. At the top, it says 'IBM Proventia GU1000 Setup'. Below that is a 'Configuration Menu' box containing a list of options: 1) Appliance Information, 2) Appliance Management, 3) Agent Management, 4) Network Configuration, 5) Time Configuration, and 6) Password Management. A blue 'Logout' button is at the bottom of the menu. Below the menu, instructions state: 'Use <ENTER> key to select, <TAB> to navigate, Use number keys to jump to menu item number'. There are two callout boxes: a yellow one on the left pointing to the list with the text 'Press the down arrow once.', and a light blue one at the top right with the text 'This demonstration shows you how to restore the appliance and preserve the appliance user name and password, network information, and host information.' A second light blue callout box at the bottom center contains the text 'You must log on to IPS Setup to restore the appliance. This task has been performed for you.'

IBM Proventia GU1000 Setup

Configuration Menu

-> 1) Appliance Information  
2) Appliance Management  
3) Agent Management  
4) Network Configuration  
5) Time Configuration  
6) Password Management

Logout

Use <ENTER> key to select, <TAB> to navigate,  
Use number keys to jump to menu item number

Press the down arrow once.

This demonstration shows you how to restore the appliance and preserve the appliance user name and password, network information, and host information.

You must log on to IPS Setup to restore the appliance. This task has been performed for you.

## Restore the appliance to factory default (configured)

---

Slide 5

IBM Proventia GUI1000 Setup

Configuration Menu

- 1) Appliance Information
- > 2) Appliance Management
- 3) Agent Management
- 4) Network Configuration
- 5) Time Configuration
- 6) Password Management

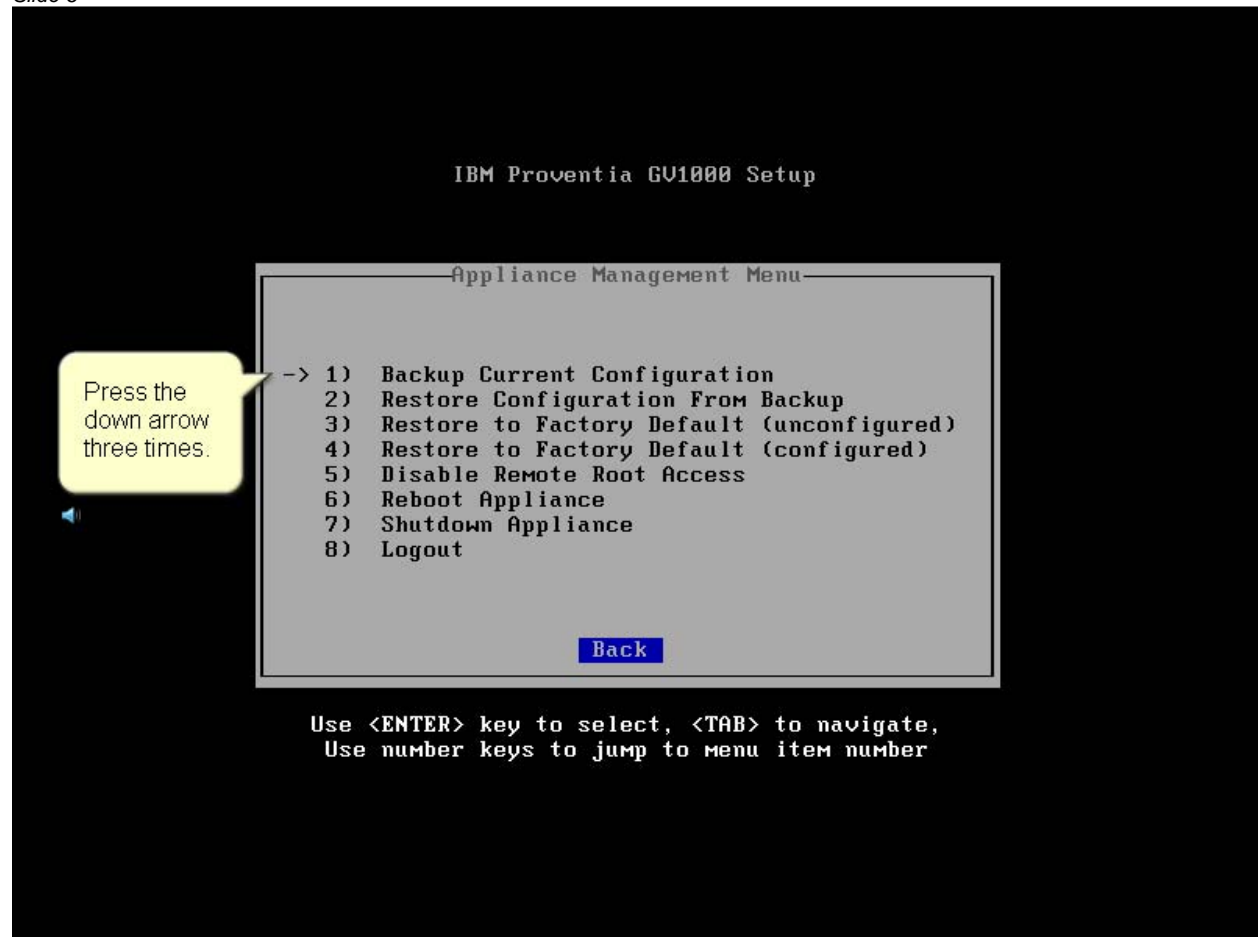
Logout

Use <ENTER> key to select, <TAB> to navigate,  
Use number keys to jump to menu item number

## Restore the appliance to factory default (configured)

---

Slide 6



The screenshot shows a terminal window titled "IBM Proventia GUI1000 Setup". Inside, there is a menu titled "Appliance Management Menu" with the following options:

- > 1) Backup Current Configuration
- 2) Restore Configuration From Backup
- 3) Restore to Factory Default (unconfigured)
- 4) Restore to Factory Default (configured)
- 5) Disable Remote Root Access
- 6) Reboot Appliance
- 7) Shutdown Appliance
- 8) Logout

A yellow callout box on the left contains the text: "Press the down arrow three times." with an arrow pointing to the first menu item. A blue "Back" button is located at the bottom of the menu box. Below the menu box, instructions read: "Use <ENTER> key to select, <TAB> to navigate, Use number keys to jump to menu item number".

## Restore the appliance to factory default (configured)

---

Slide 7

The screenshot shows a terminal window titled "IBM Proventia GUI1000 Setup". Inside the terminal, there is a menu titled "Appliance Management Menu" with the following options:

- 1) Backup Current Configuration
- 2) Restore Configuration From Backup
- 3) Restore to Factory Default (unconfigured)
- 4) Restore to Factory Default (configured)
- 5) Disable Remote Root Access
- 6) Reboot Appliance
- 7) Shutdown Appliance
- 8) Logout

A yellow callout box on the left side of the terminal window contains the text: "Verify that the arrow points to Restore to Factory Default (configured) and press Enter." An arrow points from the callout box to the fourth menu item.

At the bottom of the terminal window, there is a blue button labeled "Back".

Below the terminal window, there is a legend: "Use <ENTER> key to select, <TAB> to navigate, Use number keys to jump to menu item number".

## Restore the appliance to factory default (configured)

---

Slide 8





## Restore the appliance to factory default (configured)

---

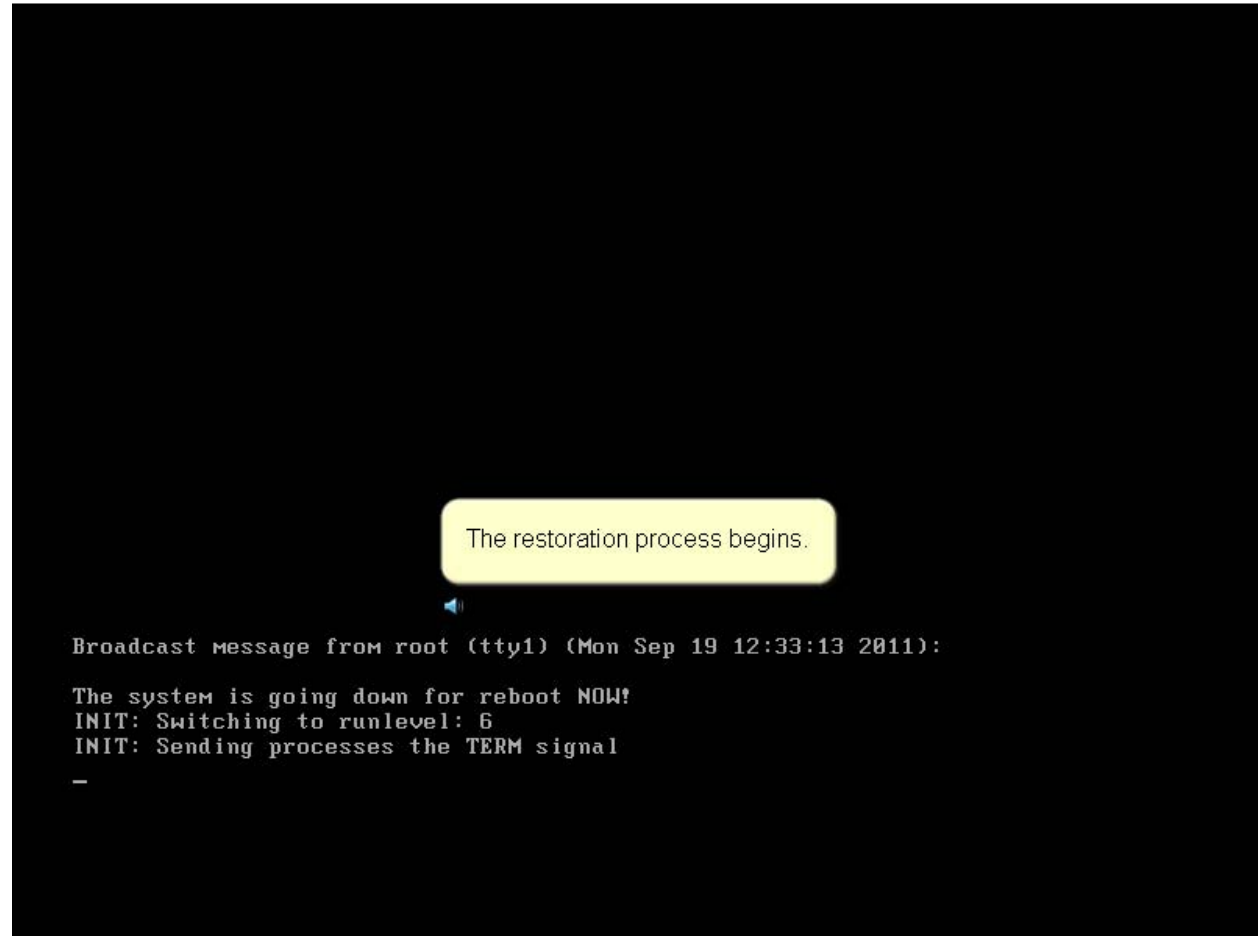
Slide 9



## Restore the appliance to factory default (configured)

---

Slide 10



## Restore the appliance to factory default (configured)

---

Slide 11

```
Broadcast message from root (tty1) (Mon Sep 19 12:33:13 2011):

The system is going down for reboot NOW!
INIT: Switching to runlevel: 6
INIT: Sending processes the TERM signal
Boot logging started on /dev/tty1(/dev/console) at Mon Sep 19 12:33:17 2011
Master Resource Control: previous runlevel: 3, switching to runlevel:6
Stopping accessMonitor: done
Stopping service anacron: - Warning: daemon not running. done
Shutting down httpd2 (waiting for all children to terminate) done
Shutting down service at daemon done
Shutting down CRON daemon done
Unloading iptables rules...ipv4...ipv6... done
Stopping iss-rrdd: done
issFipsd is already stopped: done
Stopping iss-dbd: done
Saving random seed done

Stopping provpktlogger: done
Shutting down SSH daemon done
Stopping issDaemon: _
```

## Restore the appliance to factory default (configured)

---

Slide 12

```
Shutting down service at daemon           done
Shutting down CRON daemon                 done
Unloading iptables rules..ipv4..ipv6...   done
Stopping iss-rrdd:                        done
issFipsd is already stopped:              done
Stopping iss-dbd:                         done
Saving random seed                        done

Stopping provpktlogger:                   done
Shutting down SSH daemon                  done
Stopping issDaemon:                      done
Stopping iss-lum:                         done

Stopping issppd:                          done
Shutting down syslog services             done
Shutting down network interfaces:
  eth0                                     done
  eth1                                     done
  eth2                                     done
  eth3                                     done
Shutting down service network . . . . . done
Shutting down HAL daemon                  done
Shutting down resource manager            done
Shutting down D-BUS daemon_
```

## Restore the appliance to factory default (configured)

---

Slide 13

```
eth0 done
eth1 done
eth2 done
eth3 done
Shutting down service network . . . . . done
Shutting down HAL daemon done
Shutting down resource manager done
Shutting down D-BUS daemon done
Running /etc/init.d/halt.local done
Sending all processes the TERM signal... done
Sending all processes the KILL signal... done
Turning off swap done
Set Hardware Clock to the current System Time done

Unmounting file systems
/dev/sda7 umounted
/dev/sda6 umounted
/dev/sda3 umounted
/dev/sda1 umounted
devpts umounted
debugfs umounted
sysfs umounted
/dev/sda5 umounted done
Stopping udevd: done
-
```

## Restore the appliance to factory default (configured)

---

Slide 14

```
eth2 done
eth3 done
Shutting down service network . . . . . done
Shutting down HAL daemon done
Shutting down resource manager done
Shutting down D-BUS daemon done
Running /etc/init.d/halt.local done
Sending all processes the TERM signal... done
Sending all processes the KILL signal... done
Turning off swap done
Set Hardware Clock to the current System Time done

Unmounting file systems
/dev/sda7 umounted
/dev/sda6 umounted
/dev/sda3 umounted
/dev/sda1 umounted
devpts umounted
debugfs umounted
sysfs umounted
/dev/sda5 umounted done
Stopping udevd: done
proc umounted
Please stand by while rebooting the system...
-
```

## Restore the appliance to factory default (configured)

---

Slide 15

```
Booting 'Proventia GU1000 Restore System Backup factory'
root (hd0,2)
Filesystem type is ext2fs, partition type 0x83
kernel /bzImage IssHighMem=100M rdinit=/fullrestore console=null backupslot=factory
  [[Linux-bzImage, setup=0x1c00, size=0x1649f41
initrd /initfs.gz
  [[Linux-initrd @ 0x1fc05000, 0x3ea109 bytes]

Uncompressing Linux... Ok, booting the kernel.
-
```

## Restore the appliance to factory default (configured)

---

Slide 16

```
Booting 'Proventia GV1000 Restore System Backup factory'

root (hd0,2)
Filesystem type is ext2fs, partition type 0x83
kernel /bzImage IssHighMem=100M rdinit=/fullrestore console=null backupslot=factory
  [[Linux-bzImage, setup=0x1c00, size=0x1649f41]
initrd /initfs.gz
  [[Linux-initrd @ 0x1fc05000, 0x3ea109 bytes]

Uncompressing Linux... Ok, booting the kernel.

done
Restoring OS and software:
Restoring /dev/sda1...done
Restoring /dev/sda3...done
Restoring /dev/sda5...\_
```



## Restore the appliance to factory default (configured)

---

Slide 17

```
Booting 'Proventia GV1000 Restore System Backup factory'

root (hd0,2)
Filesystem type is ext2fs, partition type 0x83
kernel /bzImage IssHighMem=100M rdinit=/fullrestore console=null backupslot=factory
  [[Linux-bzImage, setup=0x1c00, size=0x1649f41]
initrd /initfs.gz
  [[Linux-initrd @ 0x1fc05000, 0x3ea109 bytes]

Uncompressing Linux... Ok, booting the kernel.

done
Restoring OS and software:
Restoring /dev/sda1...done
Restoring /dev/sda3...done
Restoring /dev/sda5...done
Restoring /dev/sda6...done
Restoring cache filesystem structure...done
Creating swap space...done
Configuring boot loader..._
```

## Restore the appliance to factory default (configured)

---

Slide 18

```
GNU GRUB version 0.97 (638K lower / 1046464K upper memory)
```

```
Proventia GV1000 Linux-up (2.6.16.46-363-up)
Proventia GV1000 Linux-smp (2.6.16.46-363-smp)
Proventia GV1000 Create System Backup 0
Proventia GV1000 Restore System Backup 0
Proventia GV1000 Restore Factory Image (unconfigured)
```

Use the ↑ and ↓ keys to select which entry is highlighted.  
Press enter to boot the selected OS or 'p' to enter a  
password to unlock the next set of features.

The highlighted entry will be booted automatically in 3 seconds.

## Restore the appliance to factory default (configured)

---

Slide 19

```
Using tsc for high-res timesource
Console: colour UGA+ 80x25
Dentry cache hash table entries: 131072 (order: 7, 524288 bytes)
Inode-cache hash table entries: 65536 (order: 6, 262144 bytes)
Memory: 102400k highmem reserved for ISS buffer at 37fff000
Memory: 930384k/1048576k available (1993k kernel code, 14940k reserved, 613k data, 188k init, 131012k highmem)
Checking if this processor honours the WP bit even in supervisor mode... Ok.
Calibrating delay using timer specific routine.. 4004.92 BogoMIPS (lpj=8009855)
Security Framework v1.0.0 initialized
Mount-cache hash table entries: 512
CPU: L1 I cache: 32K, L1 D cache: 32K
CPU: L2 cache: 256K
CPU: L3 cache: 4096K
Intel machine check architecture supported.
Intel machine check reporting enabled on CPU#0.
CPU: Intel(R) Xeon(R) CPU           E5504  @ 2.00GHz stepping 05
Checking 'hlt' instruction... OK.
checking if image is initramfs...it isn't (bad gzip magic numbers); looks like a
n initrd
Freeing initrd memory: 2744k freed
not found!
ENABLING IO-APIC IRQs
..TIMER: vector=0x31 apic1=0 pin1=2 apic2=-1 pin2=-1
-
```

## Restore the appliance to factory default (configured)

---

Slide 20

```
sda: cache data unavailable
sda: assuming drive cache: write through
SCSI device sda: 16777216 512-byte hdwr sectors (8590 MB)
sda: Write Protect is off
sda: cache data unavailable
sda: assuming drive cache: write through
sda: sda1 sda2 sda3 sda4 < sda5 sda6 sda7 >
sd 0:0:0:0: Attached scsi disk sda
Uniform Multi-Platform E-IDE driver Revision: 7.00alpha2
ide: Assuming 33MHz system bus speed for PIO modes; override with idebus=xx
VMware vmxnet virtual NIC driver
ACPI: PCI Interrupt 0000:02:00.0[A] -> GSI 18 (level, low) -> IRQ 59
Found vmxnet/PCI at 0x2024, irq 59.
features: ipCsum zeroCopy partialHeaderCopy jumboFrame tso lpd
numRxBuffers = 150, numRxBuffers2 = 600
ACPI: PCI Interrupt 0000:02:01.0[A] -> GSI 19 (level, low) -> IRQ 67
Found vmxnet/PCI at 0x20a4, irq 67.
features: ipCsum zeroCopy partialHeaderCopy jumboFrame tso lpd
numRxBuffers = 150, numRxBuffers2 = 600
ACPI: PCI Interrupt 0000:02:02.0[A] -> GSI 16 (level, low) -> IRQ 75
Found vmxnet/PCI at 0x2424, irq 75.
features: ipCsum zeroCopy partialHeaderCopy jumboFrame tso lpd
numRxBuffers = 150, numRxBuffers2 = 600
ACPI: PCI Interrupt 0000:02:03.0[A] -> GSI 17 (level, low) -> IRQ 51
-
```

## Restore the appliance to factory default (configured)

---

Slide 21

```
Found vmxnet/PCI at 0x24a4, irq 51.
features: ipChecksum zeroCopy partialHeaderCopy jumboFrame tso lpd
numRxBuffers = 150, numRxBuffers2 = 600
EXT3-fs: mounted filesystem with ordered data mode.
kjournald starting. Commit interval 5 seconds
INIT: version 2.86 booting
System Boot Control: Running /etc/init.d/boot
Mounting procfs at /proc done
Mounting sysfs at /sys done
Mounting debugfs at /sys/kernel/debug done
Mounting tmpfs at /dev done
Initializing /dev done
Mounting devpts at /dev/pts done
Boot logging started on /dev/tty1(/dev/console) at Mon Sep 19 12:35:28 2011
Configuring serial ports...
/dev/ttyS0 at 0x03f8 (irq = 4) is a 16550A
/dev/ttyS1 at 0x02f8 (irq = 3) is a 16550A
Configured serial ports done
EXT3 FS on sda5, internal journal
Activating swap-devices in /etc/fstab... done
/bin/mknod -m600 /dev/shm/root b 8 5
Checking root file system...
fsck 1.38 (30-Jun-2005)
/ (/dev/shm/root): clean, 26019/262656 files, 171898/524288 blocks done
Starting udevd _
```

## Restore the appliance to factory default (configured)

---

Slide 22

```
EXT3-fs: mounted filesystem with ordered data mode.
/dev/sda7 on /restore type ext3 (rw,acl,user_xattr)           done
NET: Registered protocol family 17
Setting up hostname 'sam'                                     done
Setting up loopback interface lo
lo IP address: 127.0.0.1/8                                     done

Setting up the hardware clock                                 done
Creating /var/log/boot.msg                                    done
Activating remaining swap-devices in /etc/fstab...           done
Setting up linker cache (/etc/ld.so.cache) using ldconfig    done
Setting scheduling timeslices                                 unused
Setting current sysctl status from /etc/sysctl.conf
kernel.core_uses_pid = 1
kernel.panic = 60
net.ipv4.conf.all.rp_filter = 1
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.neigh.default.gc_interval = 30
net.ipv4.neigh.default.gc_stale_time = 20
net.ipv4.neigh.default.gc_thresh1 = 512
net.ipv4.neigh.default.gc_thresh2 = 2048
net.ipv4.neigh.default.gc_thresh3 = 4096
vm.lowmem_reserve_ratio = 256 256 1 32                       done

-
```

## Restore the appliance to factory default (configured)

---

Slide 23

```
Executing /sbin/conf.d/SuSEconfig.groff...
Executing /sbin/conf.d/SuSEconfig.libxml2...
Executing /sbin/conf.d/SuSEconfig.news...
Installing new /etc/mntpsrvr
Executing /sbin/conf.d/SuSEconfig.perl...
Executing /sbin/conf.d/SuSEconfig.permissions...
Checking permissions and ownerships - using the permissions files
    /etc/permissions.d/iss_provos
    /etc/permissions
    /etc/permissions.easy
    /etc/permissions.local
setting /etc/shadow to root:shadow 0640. (wrong owner/group root:root permission
s 0644)
setting /etc/ssh/sshd_config to root:root 0640. (wrong permissions 0644)
Executing /sbin/conf.d/SuSEconfig.sortpasswd...
Executing /sbin/conf.d/SuSEconfig.words...
Executing /sbin/conf.d/SuSEconfig.zmessages...
Finished.
INIT: Entering runlevel: 3
Boot logging started on /dev/tty1(/dev/console) at Mon Sep 19 12:35:39 2011
Master Resource Control: previous runlevel: N, switching to runlevel:3
Starting service at daemon                               done
Starting D-BUS daemon                                   done
Starting service anacron:                                done
-
```

## Restore the appliance to factory default (configured)

---

Slide 24

```
Stop Unicode mode
Starting resource manager           done
Starting HAL daemon                 done
Loading iptables rules... ipv4... ipv6... done
Setting up network interfaces:
  lo
    IP address: 127.0.0.1/8         done
  eth0
    is down
  eth0
    done
  eth1
    is down
  eth1
    IP address: 192.168.5.110/24
/usr/sbin/mDNSResponder is already stopped: done
Starting iss-mdns:                 done
  eth2
    is down
  eth2
    IP address: 0.0.0.0/0         done
  eth3
    is down
  eth3
    IP address: 0.0.0.0/0         done
```

-



## Restore the appliance to factory default (configured)

Slide 25

```
The key's randomart image is:
+--[ RSA 1024]-----+
|+. .                    |
|o.                      |
| o.                     |
|..=o.                   |
|.E*. S                  |
|o+. . .                 |
|..=o. . +.              |
|  o   + o.              |
| . . .                  |
+-----+

Starting SSH daemon
FIPS mode enabled
*** IN FIPS MODE ***
Starting httpd2 (prefork)
/usr/sbin/MDNSResponder is already running:

Master Resource Control: runlevel 3 has been
Skipped services in runlevel 3:

IBM Internet Security Systems
Proventia GU1000

sam login: _
```

When you log in to the appliance, you are prompted to configure the date and time, agent name, and protection mode. You can also enable SiteProtector management.

done  
done  
unused  
reached  
issFIPSChecksum issFIPS

When the restoration is complete, the login prompt opens.

## Restore the appliance to factory default (configured)

---

Slide 26

### Trademarks, copyrights, and disclaimers

IBM, the IBM logo, ibm.com, and Tivoli are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at <http://www.ibm.com/legal/copytrade.shtml>

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.

© Copyright International Business Machines Corporation 2011. All rights reserved.