Configuring the appliance

Slide 1

Tivoli

IBM

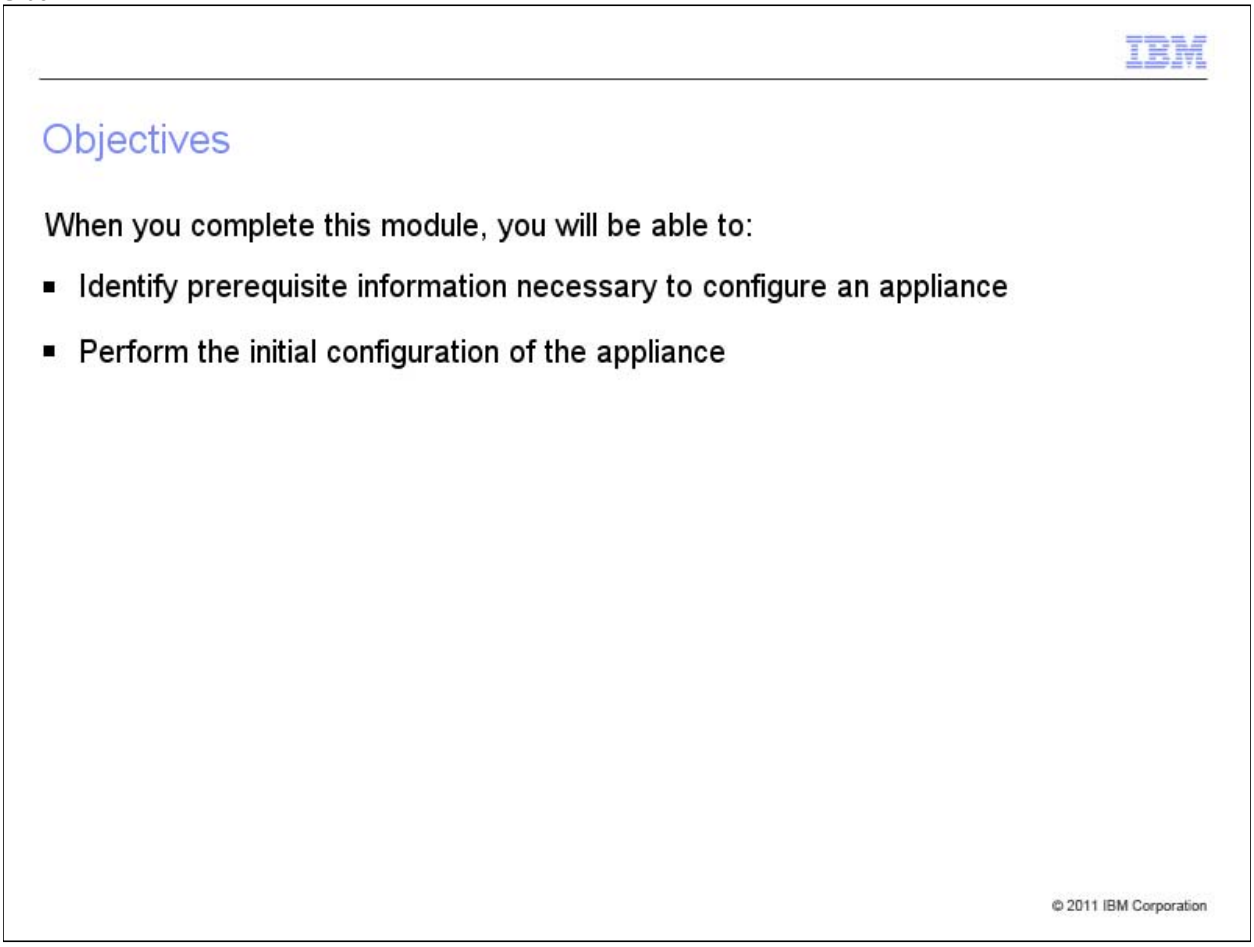
IBM Security Network Intrusion Prevention System V4.1

Configuring the appliance

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.

Slide 2


IBM
Objectives
When you complete this module, you will be able to:
Identify prerequisite information necessary to configure an appliance
Perform the initial configuration of the appliance
© 2011 IBM Corporation

Slide 3

IBM

Prerequisite appliance configuration data

There is some information you need before configuring the settings on a new appliance. This includes:

- Network configuration information for the appliance such as the:
  - IP address
  - Subnet mask
  - Default gateway
- Host configuration such as the appliance host name and domain name
- DNS configuration (if applicable)
- Protection mode for each network segment

Note: You can use the LCD panel to configure the appliance IP address, subnet mask, and gateway

© 2011 IBM Corporation

Slide 4

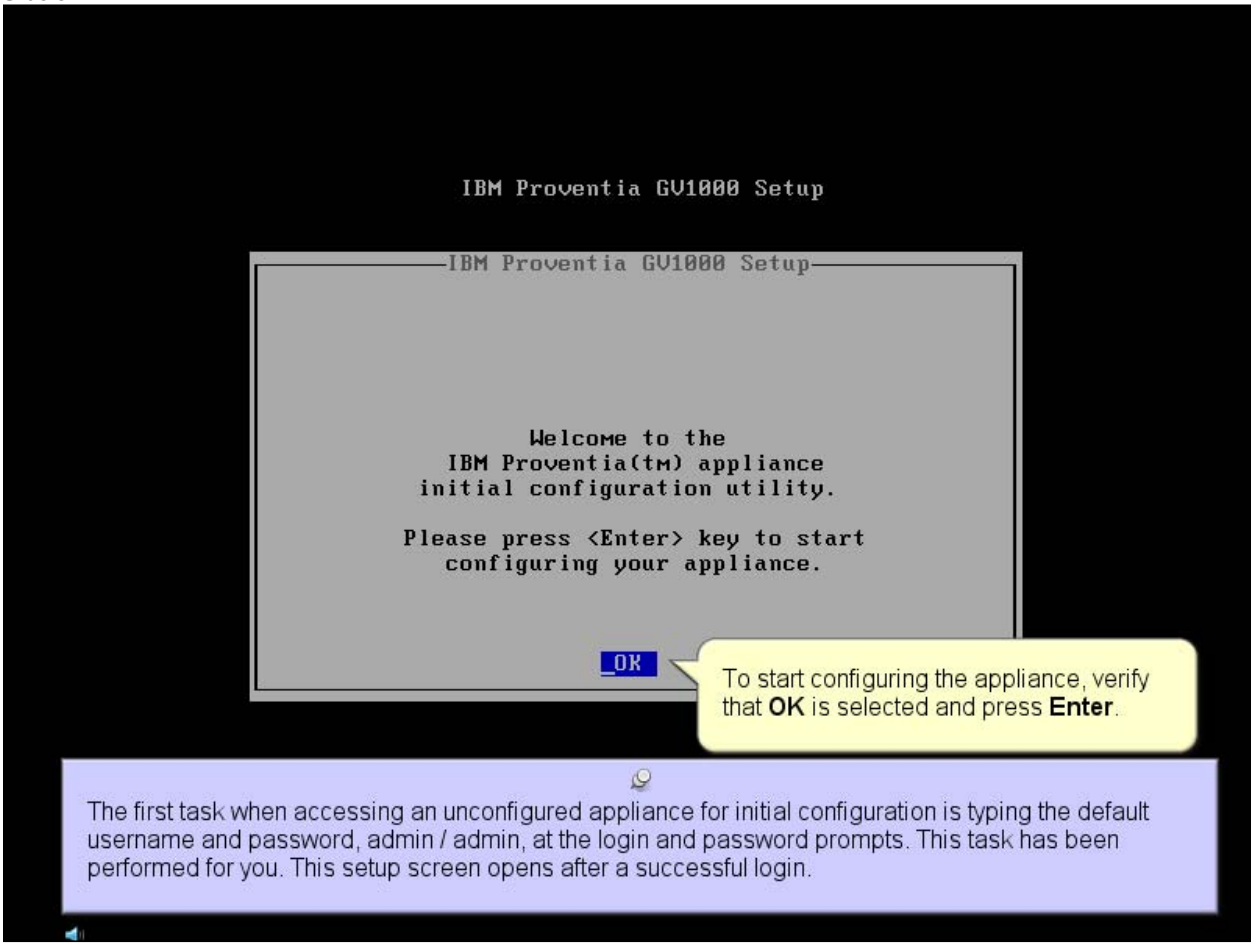
Proventia Setup utility

- The Proventia Setup utility is a text-only configuration program that starts after you log on to the appliance for the first time
- You use the Proventia Setup utility to perform these tasks:
  - Log on and change default passwords
  - Configure the network interface and host
  - Configure the date and time
  - Configure the agent name
  - Configure the segment settings

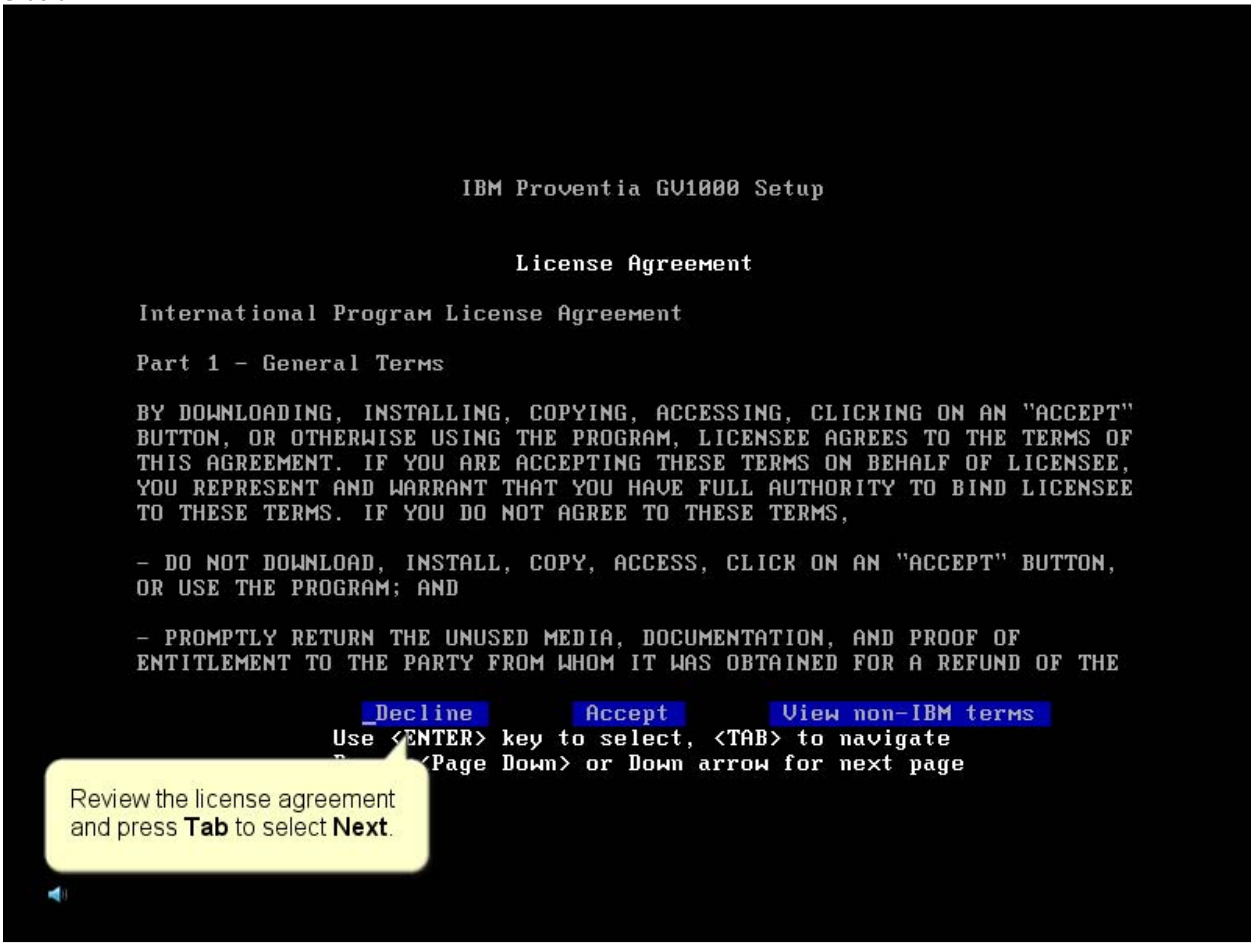
© 2011 IBM Corporation

Configuring the appliance

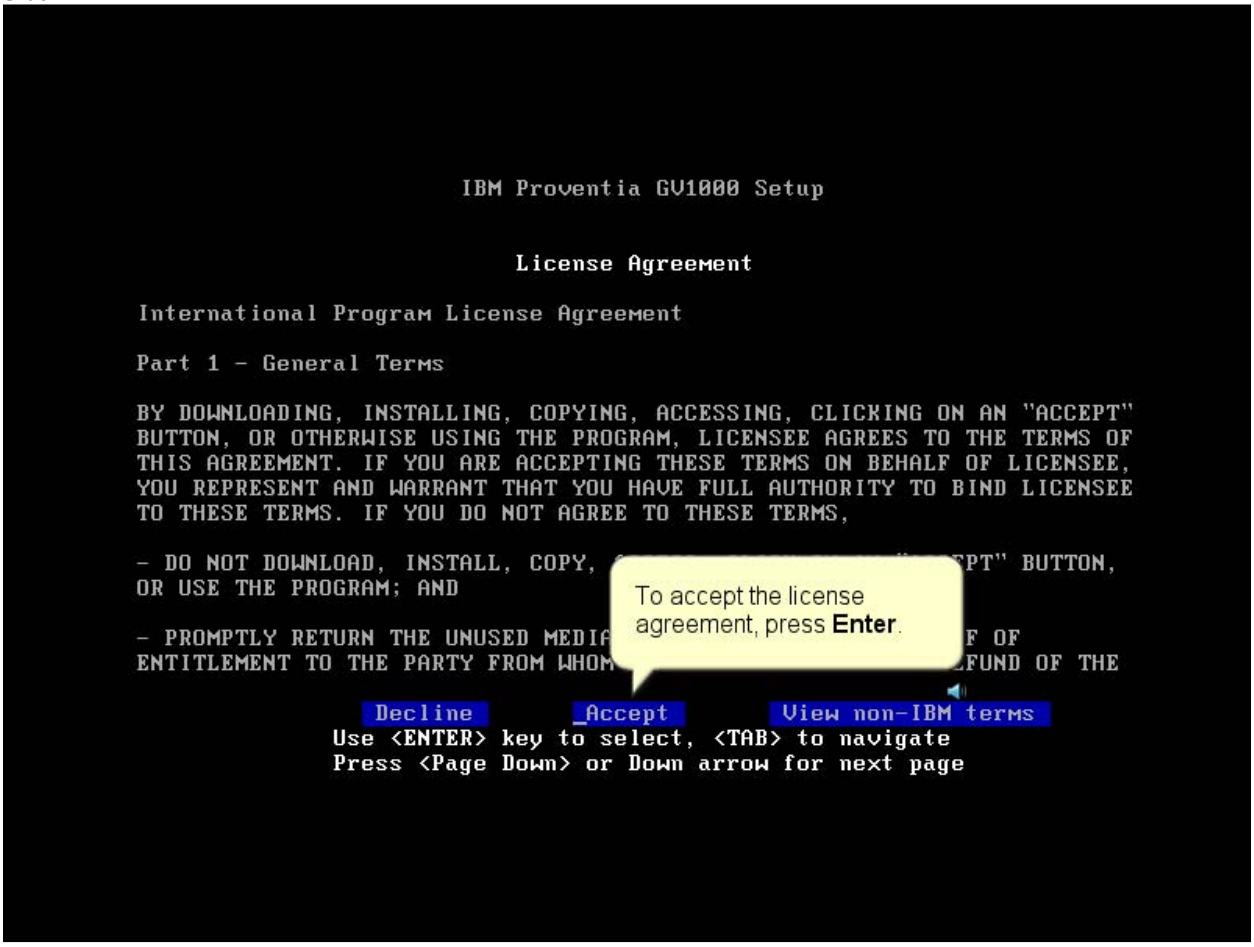
Slide 5



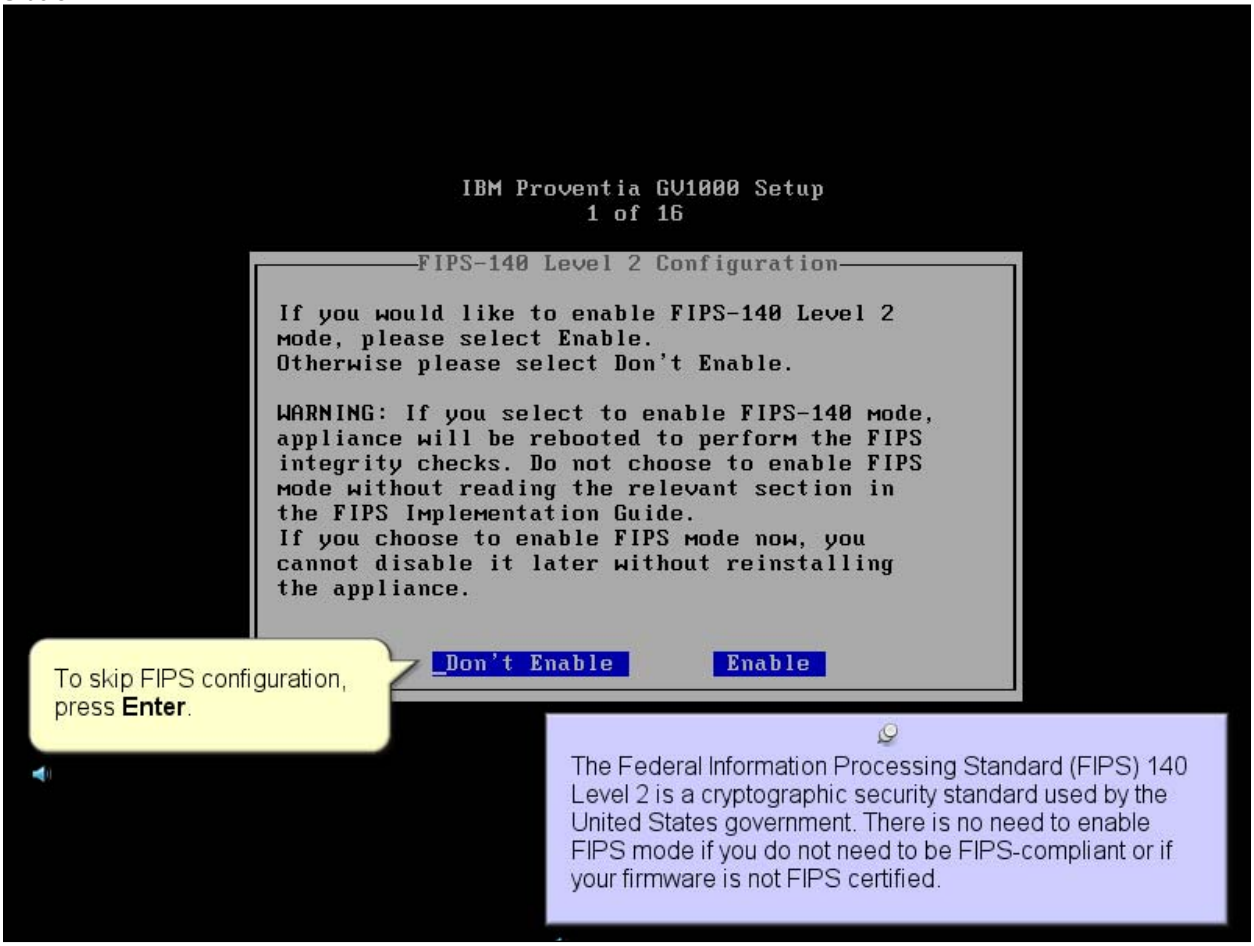
Slide 6


IBM Proventia GV1000 Setup
License Agreement
International Program License Agreement
Part 1 - General Terms
BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT" BUTTON, OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,
- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR USE THE PROGRAM; AND
- PROMPTLY RETURN THE UNUSED MEDIA, DOCUMENTATION, AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM IT WAS OBTAINED FOR A REFUND OF THE
_Decline
Accept
View non-IBM terms
Use <ENTER> key to select, <TAB> to navigate
<Page Down> or Down arrow for next page
Review the license agreement and press Tab to select Next.

Slide 7


IBM Proventia GV1000 Setup
License Agreement
International Program License Agreement
Part 1 - General Terms
BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT" BUTTON, OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,
- DO NOT DOWNLOAD, INSTALL, COPY,
OR USE THE PROGRAM; AND
- PROMPTLY RETURN THE UNUSED MEDIA
ENTITLEMENT TO THE PARTY FROM WHOM
To accept the license agreement, press Enter.
Decline
Accept
View non-IBM terms
Use <ENTER> key to select, <TAB> to navigate
Press <Page Down> or Down arrow for next page

Slide 8


IBM Proventia GV1000 Setup
1 of 16
FIPS-140 Level 2 Configuration
If you would like to enable FIPS-140 Level 2 mode, please select Enable.
Otherwise please select Don't Enable.
WARNING: If you select to enable FIPS-140 mode, appliance will be rebooted to perform the FIPS integrity checks. Do not choose to enable FIPS mode without reading the relevant section in the FIPS Implementation Guide.
If you choose to enable FIPS mode now, you cannot disable it later without reinstalling the appliance.
Don't Enable
Enable
To skip FIPS configuration, press Enter.
The Federal Information Processing Standard (FIPS) 140 Level 2 is a cryptographic security standard used by the United States government. There is no need to enable FIPS mode if you do not need to be FIPS-compliant or if your firmware is not FIPS certified.

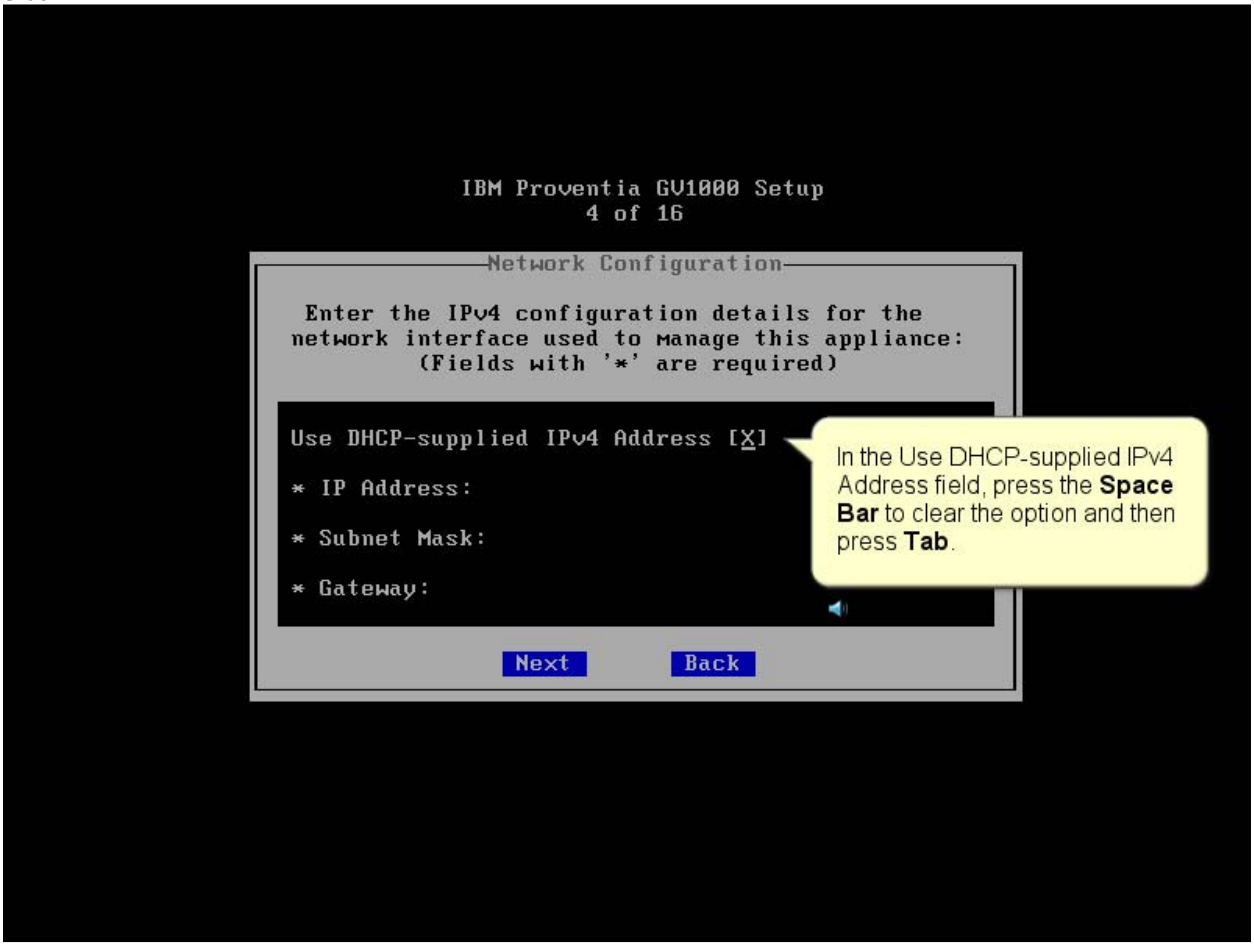
Slide 9

All passwords appear as asterisks, ***, in this utility. The default root password, admin, has been typed for you. A new password, tse123, has been typed and re-typed for you.
IBM Proventia GV1000 Setup
2 of 16
Change Password
Change password for user 'root':
Password must be at least 6 characters long
Old Password: ******
New Password: *******
Re-type Password: *******
Next
Back
Verify that Next is selected and press Enter.
Check <Caps Lock> key is OFF before entering passwords

Slide 10

The default admin password, admin, has been typed for you. A new password, tse123, has been typed and re-typed for you.
IBM Proventia GV1000 Setup
3 of 16
Change Password
Change password for user 'admin':
Password must be at least 6 characters long
Old Password: ******
New Password: *******
Re-type Password: *******
Next
Back
Verify that Next is selected and press Enter.
Check <Caps Lock> key is OFF before entering passwords

Slide 11

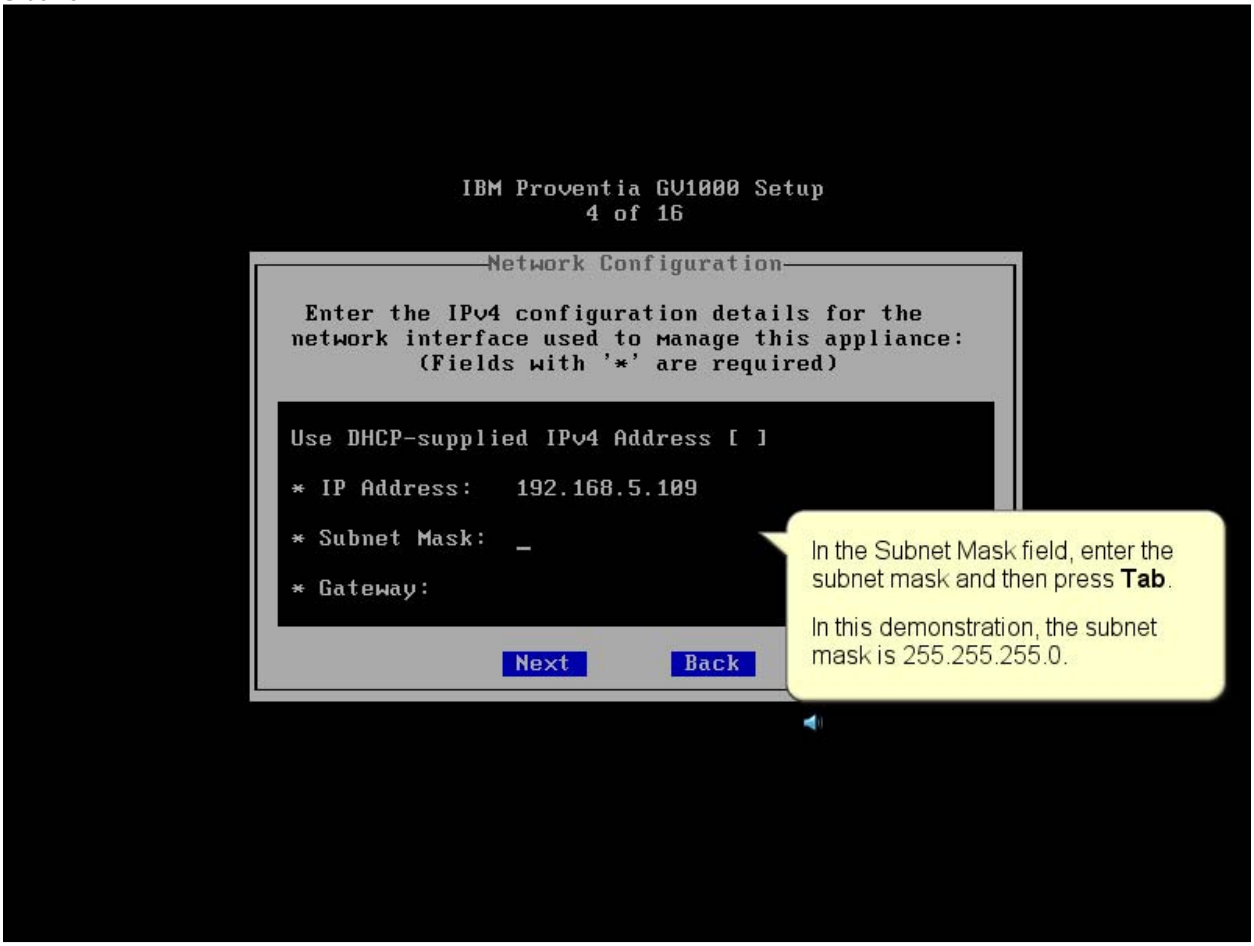

IBM Proventia GV1000 Setup
4 of 16
Network Configuration
Enter the IPv4 configuration details for the network interface used to manage this appliance:
(Fields with '*' are required)
Use DHCP-supplied IPv4 Address [X]
* IP Address:
* Subnet Mask:
* Gateway:
Next
Back
In the Use DHCP-supplied IPv4 Address field, press the **Space Bar** to clear the option and then press **Tab**.

Slide 12

IBM Proventia GV1000 Setup
4 of 16
Network Configuration
Enter the IPv4 configuration details for the network interface used to manage this appliance:
(Fields with '*' are required)
Use DHCP-supplied IPv4 Address [ ]
* IP Address:
* Subnet Mask:
* Gateway:
Next
Back
In the IP Address field, enter the IP address of the appliance and then press **Tab**.
In this demonstration, the appliance IP address is 192.168.5.109.

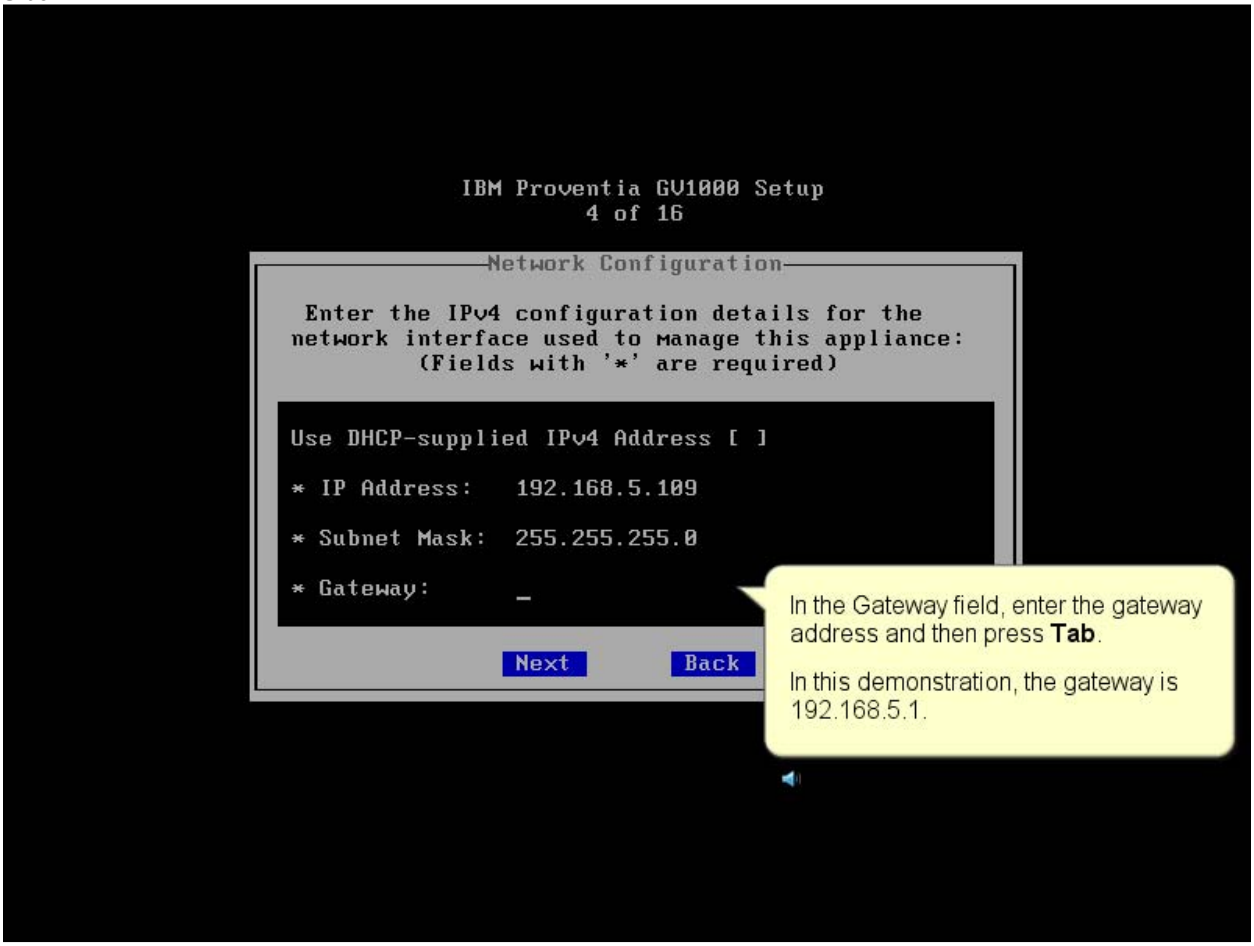
Configuring the appliance

Slide 13



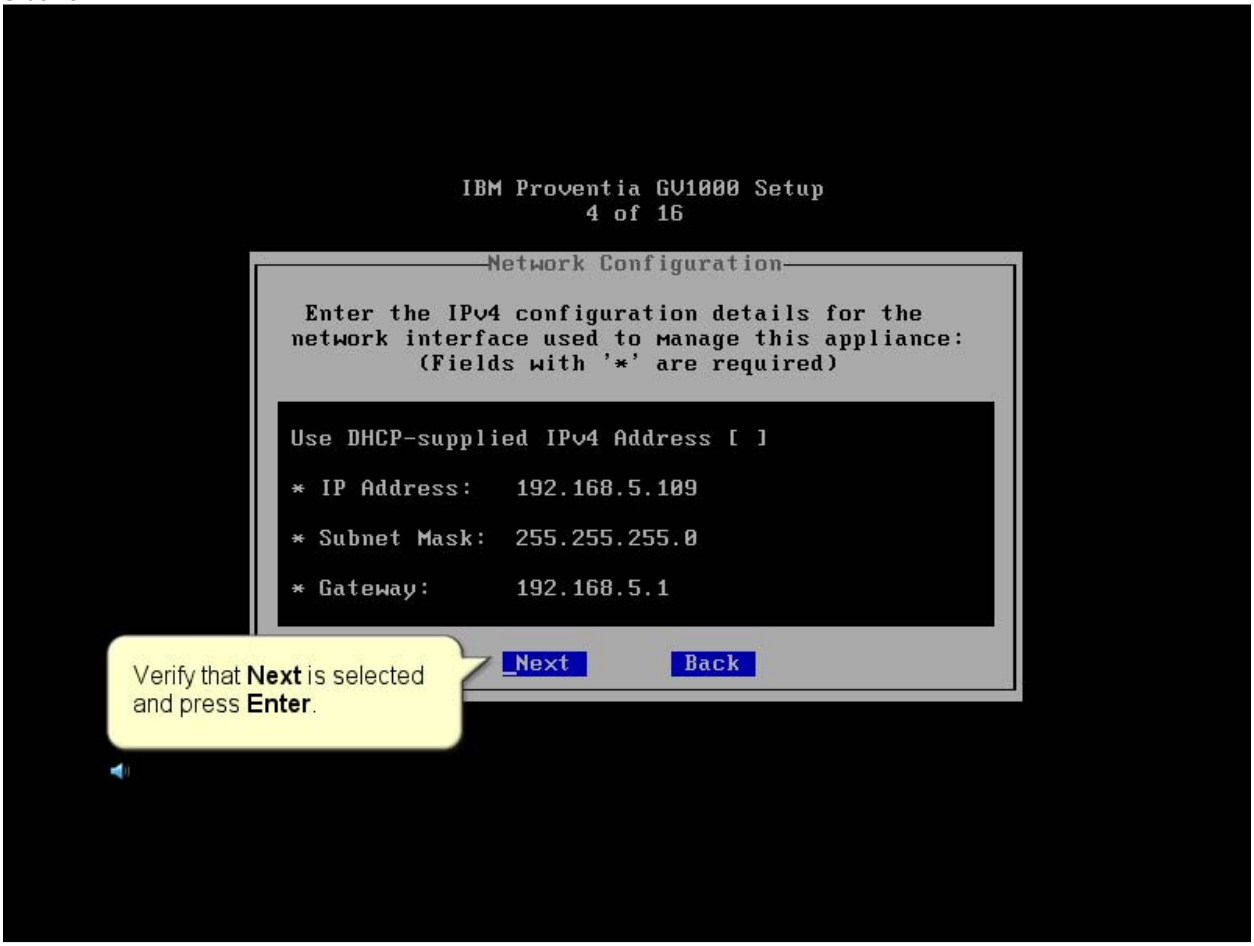
Configuring the appliance

Slide 14

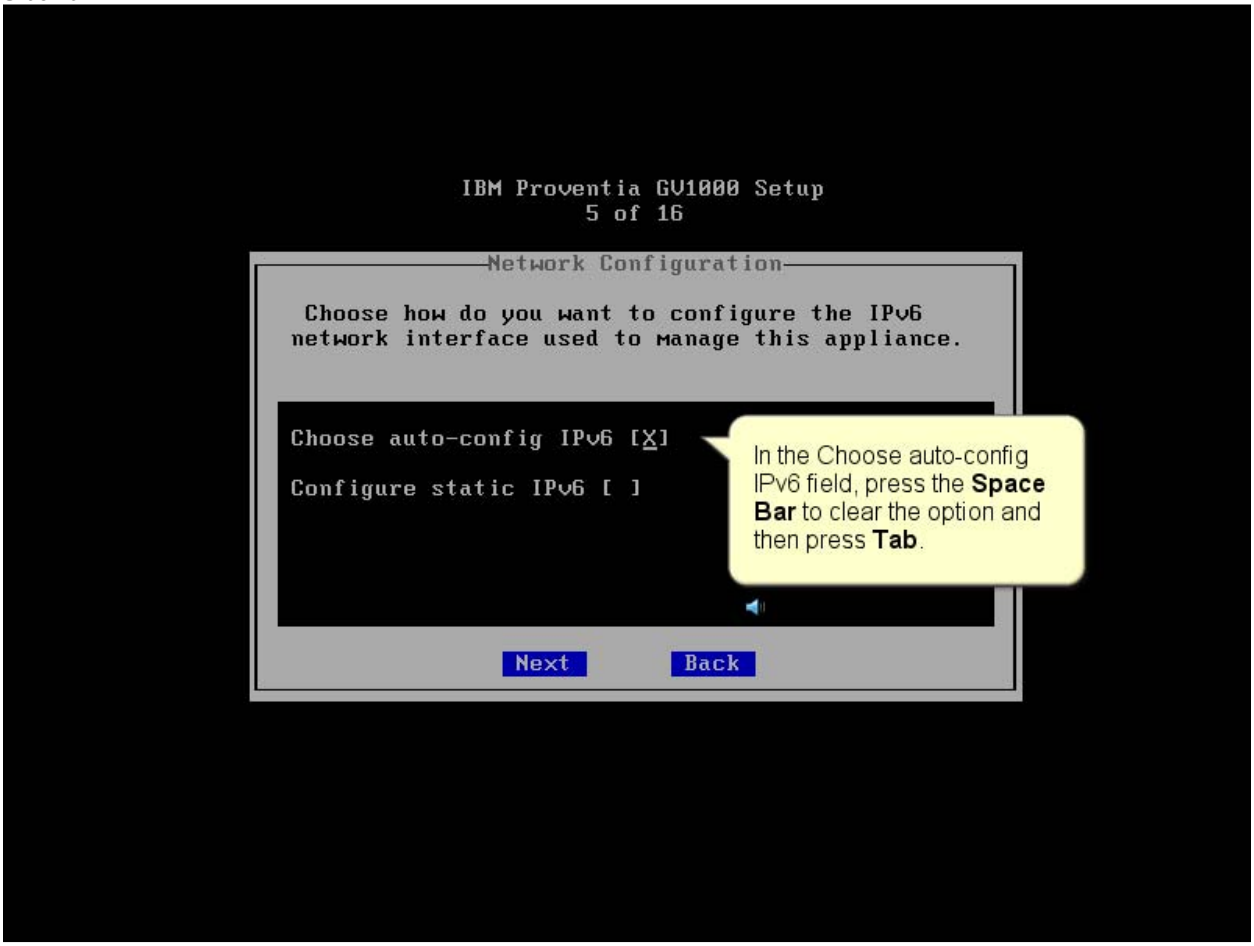


Configuring the appliance

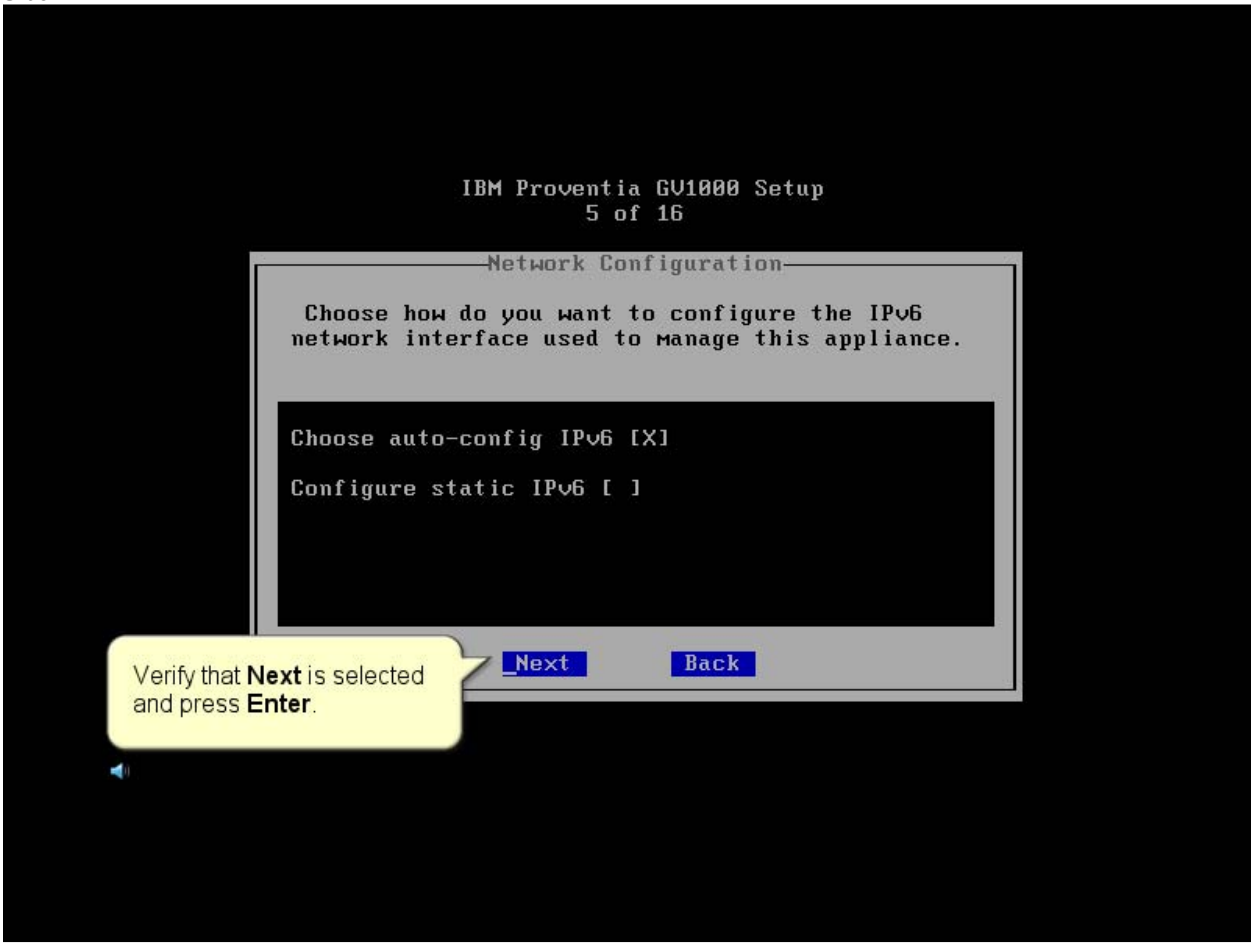
Slide 15



Slide 16

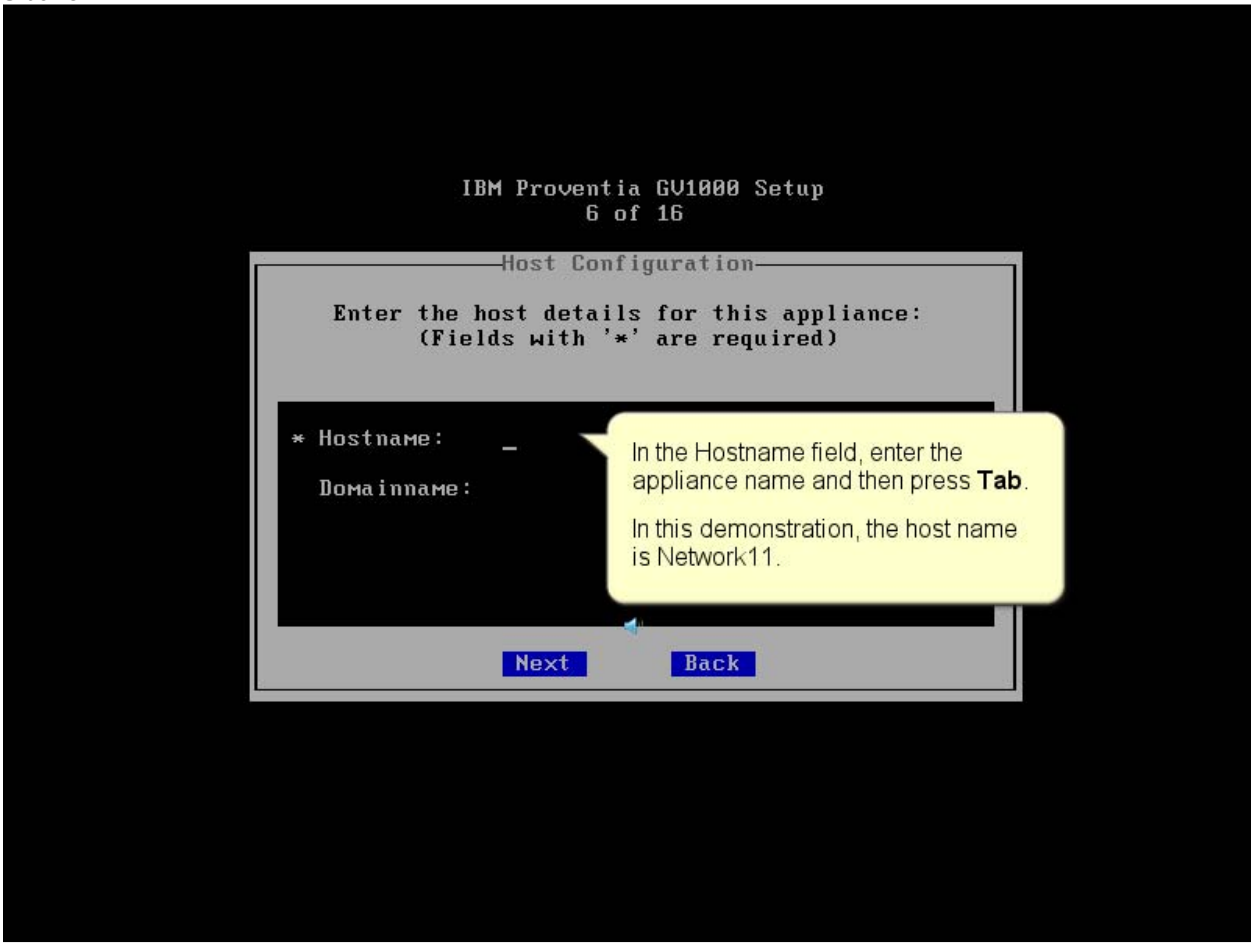

IBM Proventia GV1000 Setup
5 of 16
Network Configuration
Choose how do you want to configure the IPv6 network interface used to manage this appliance.
Choose auto-config IPv6 [X]
Configure static IPv6 [ ]
In the Choose auto-config IPv6 field, press the Space Bar to clear the option and then press Tab.
Next
Back

Slide 17


IBM Proventia GV1000 Setup
5 of 16
Network Configuration
Choose how do you want to configure the IPv6 network interface used to manage this appliance.
Choose auto-config IPv6 [X]
Configure static IPv6 [ ]
Next
Back
Verify that Next is selected and press Enter.

Configuring the appliance

Slide 18

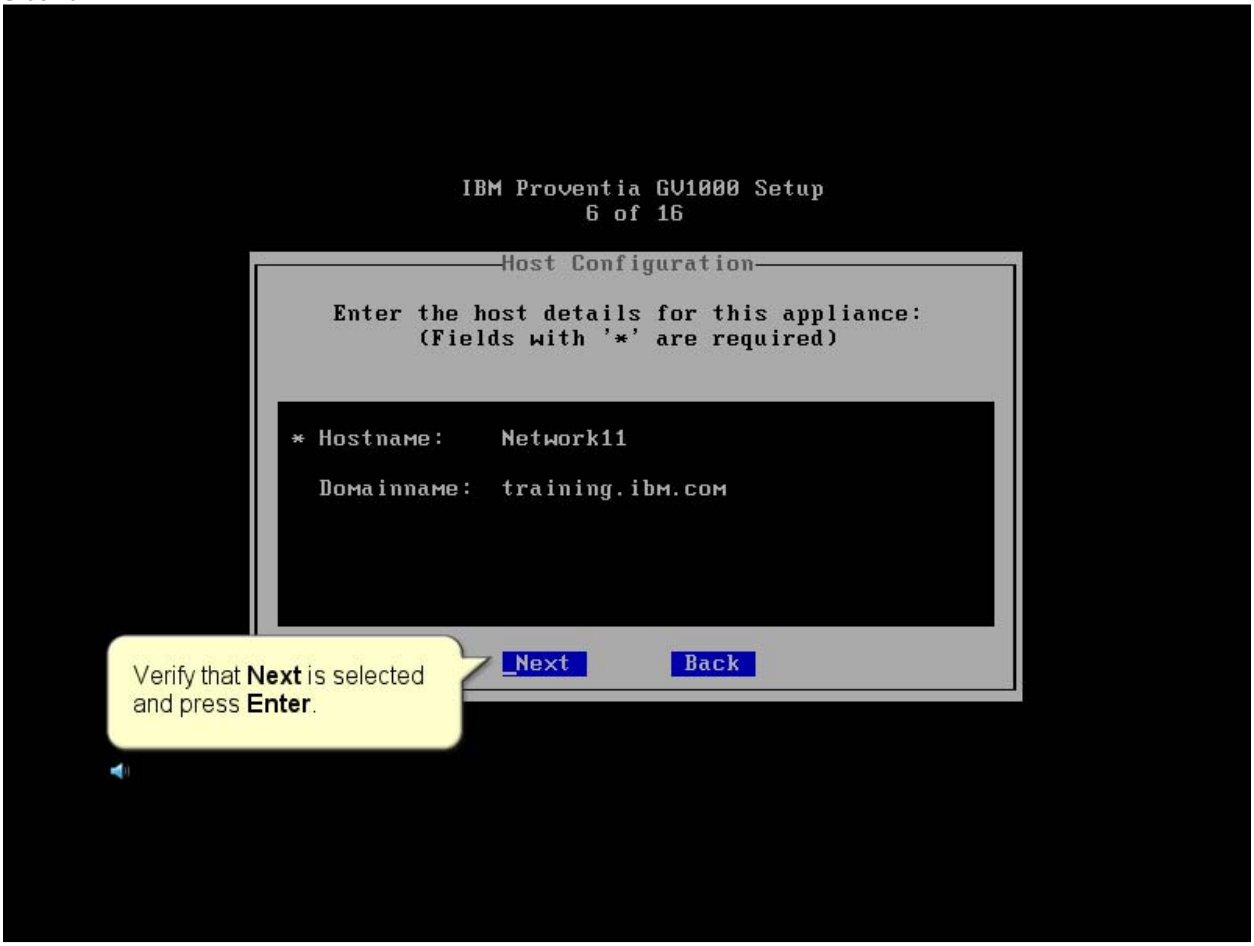


Slide 19

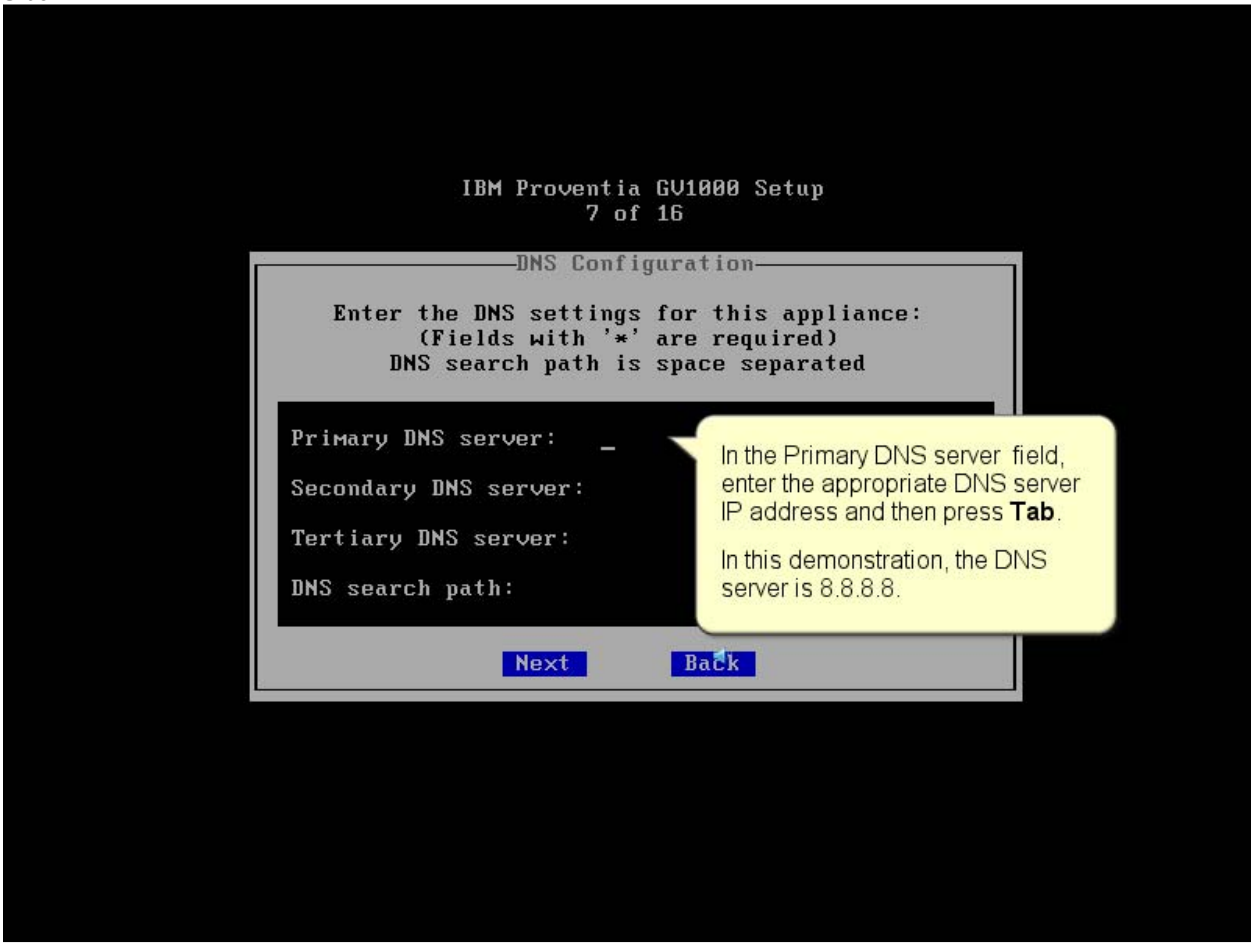
IBM Proventia GV1000 Setup
6 of 16
Host Configuration
Enter the host details for this appliance:
(Fields with '*' are required)
* Hostname: Network11
Domainname:
In the Domainname field, enter the domain name and then press Tab.
In this demonstration, the domain is training.ibm.com.
Next
Back

Configuring the appliance

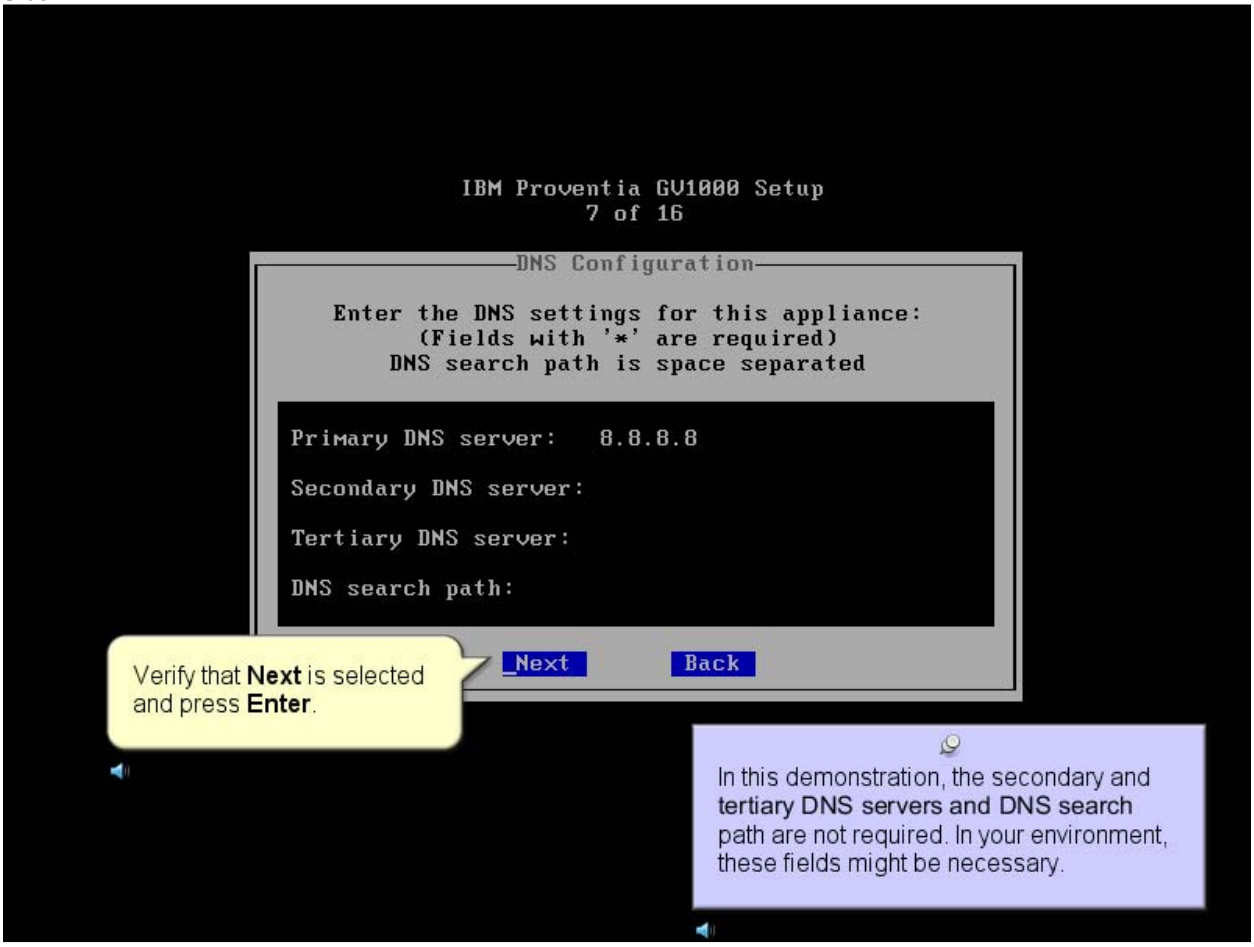
Slide 20



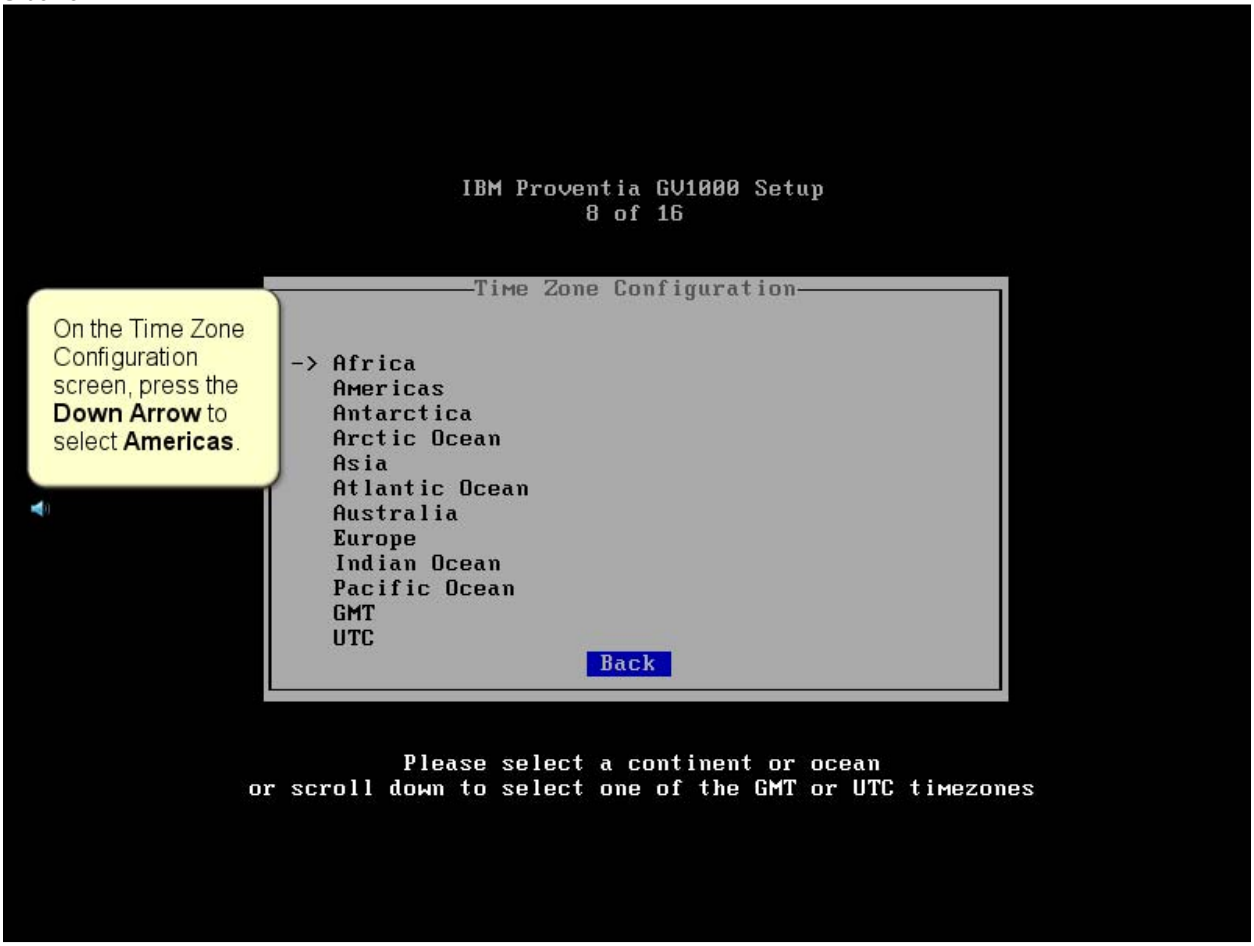
Slide 21


IBM Proventia GV1000 Setup
7 of 16
DNS Configuration
Enter the DNS settings for this appliance:
(Fields with '*' are required)
DNS search path is space separated
Primary DNS server:
Secondary DNS server:
Tertiary DNS server:
DNS search path:
Next
Back
In the Primary DNS server field, enter the appropriate DNS server IP address and then press Tab.
In this demonstration, the DNS server is 8.8.8.8.

Slide 22


IBM Proventia GV1000 Setup
7 of 16
DNS Configuration
Enter the DNS settings for this appliance:
(Fields with '*' are required)
DNS search path is space separated
Primary DNS server: 8.8.8.8
Secondary DNS server:
Tertiary DNS server:
DNS search path:
Next
Back
Verify that Next is selected and press Enter.
In this demonstration, the secondary and tertiary DNS servers and DNS search path are not required. In your environment, these fields might be necessary.

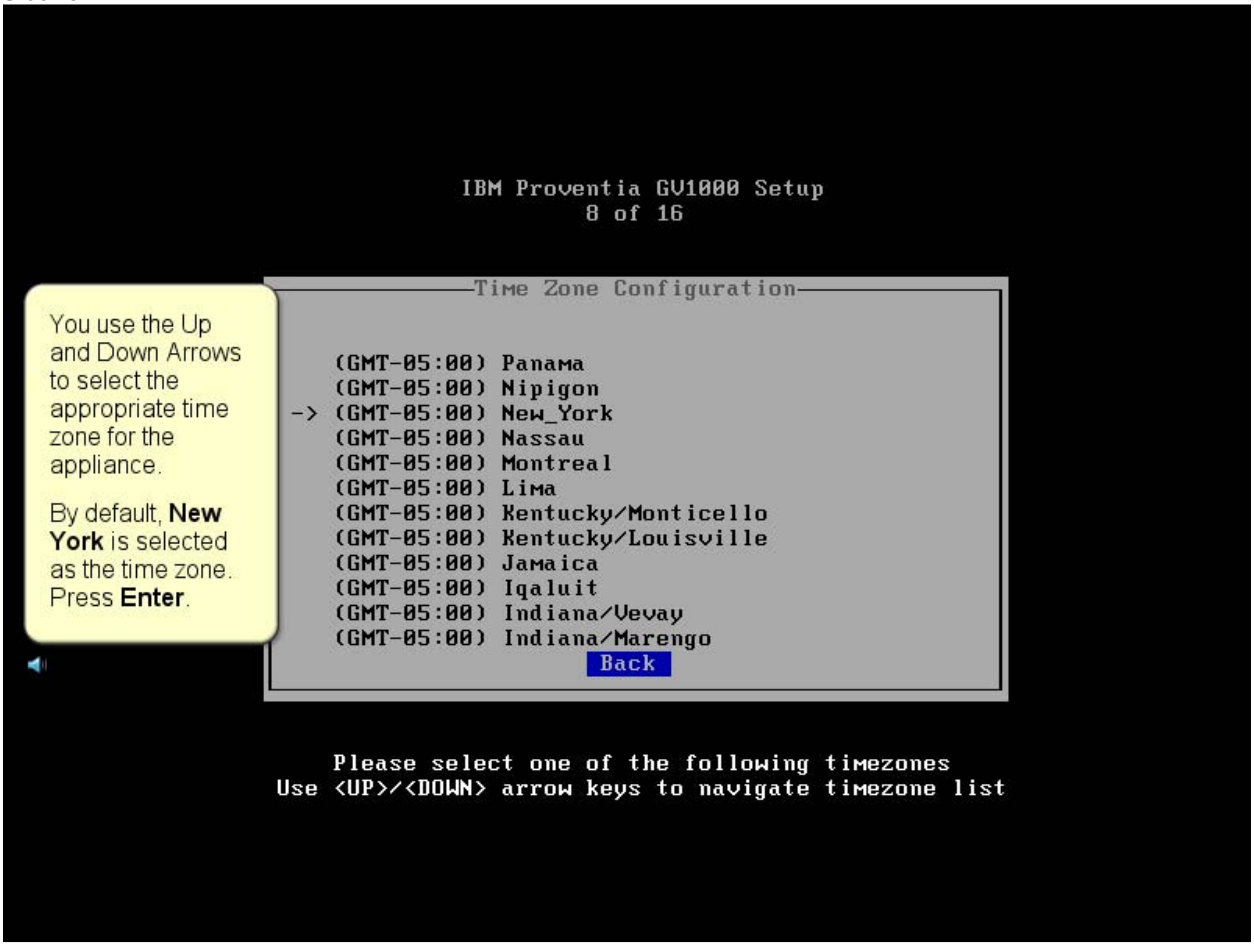
Slide 23


IBM Proventia GV1000 Setup
8 of 16
Time Zone Configuration
-> Africa
Americas
Antarctica
Arctic Ocean
Asia
Atlantic Ocean
Australia
Europe
Indian Ocean
Pacific Ocean
GMT
UTC
Back
Please select a continent or ocean
or scroll down to select one of the GMT or UTC timezones
On the Time Zone Configuration screen, press the **Down Arrow** to select **Americas**.

Slide 24

IBM Proventia GV1000 Setup
8 of 16
Time Zone Configuration
Africa
-> Americas
Antarctica
Arctic Ocean
Asia
Atlantic Ocean
Australia
Europe
Indian Ocean
Pacific Ocean
GMT
UTC
Back
Please select a continent or ocean
or scroll down to select one of the GMT or UTC timezones
Verify that the arrow points to Americas and press **Enter**.

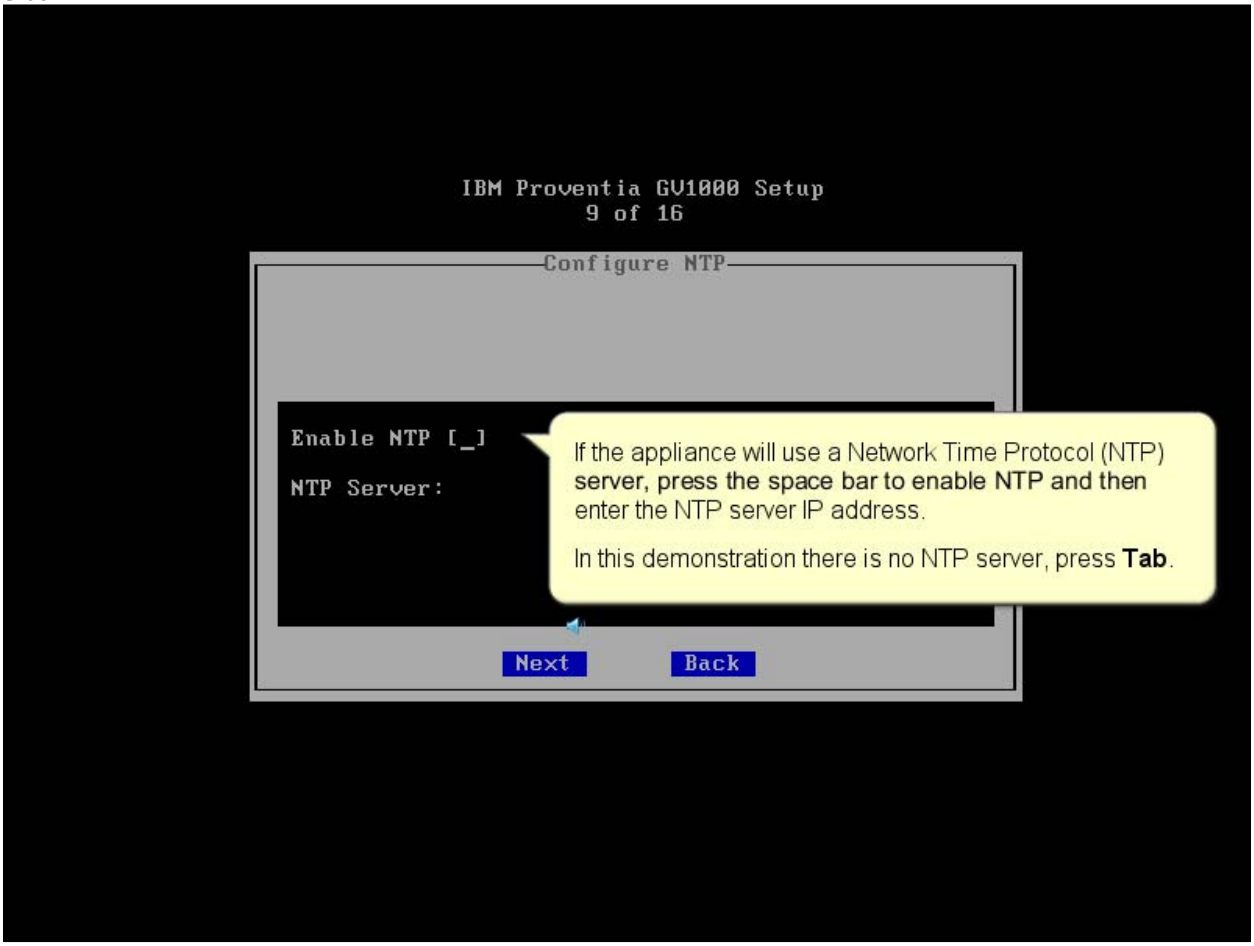
Slide 25


IBM Proventia GV1000 Setup
8 of 16
Time Zone Configuration
(GMT-05:00) Panama
(GMT-05:00) Nipigon
-> (GMT-05:00) New_York
(GMT-05:00) Nassau
(GMT-05:00) Montreal
(GMT-05:00) Lima
(GMT-05:00) Kentucky/Monticello
(GMT-05:00) Kentucky/Louisville
(GMT-05:00) Jamaica
(GMT-05:00) Iqaluit
(GMT-05:00) Indiana/Vevay
(GMT-05:00) Indiana/Marengo
Back
You use the Up and Down Arrows to select the appropriate time zone for the appliance.
By default, New York is selected as the time zone. Press Enter.
Please select one of the following timezones
Use <UP>/<DOWN> arrow keys to navigate timezone list

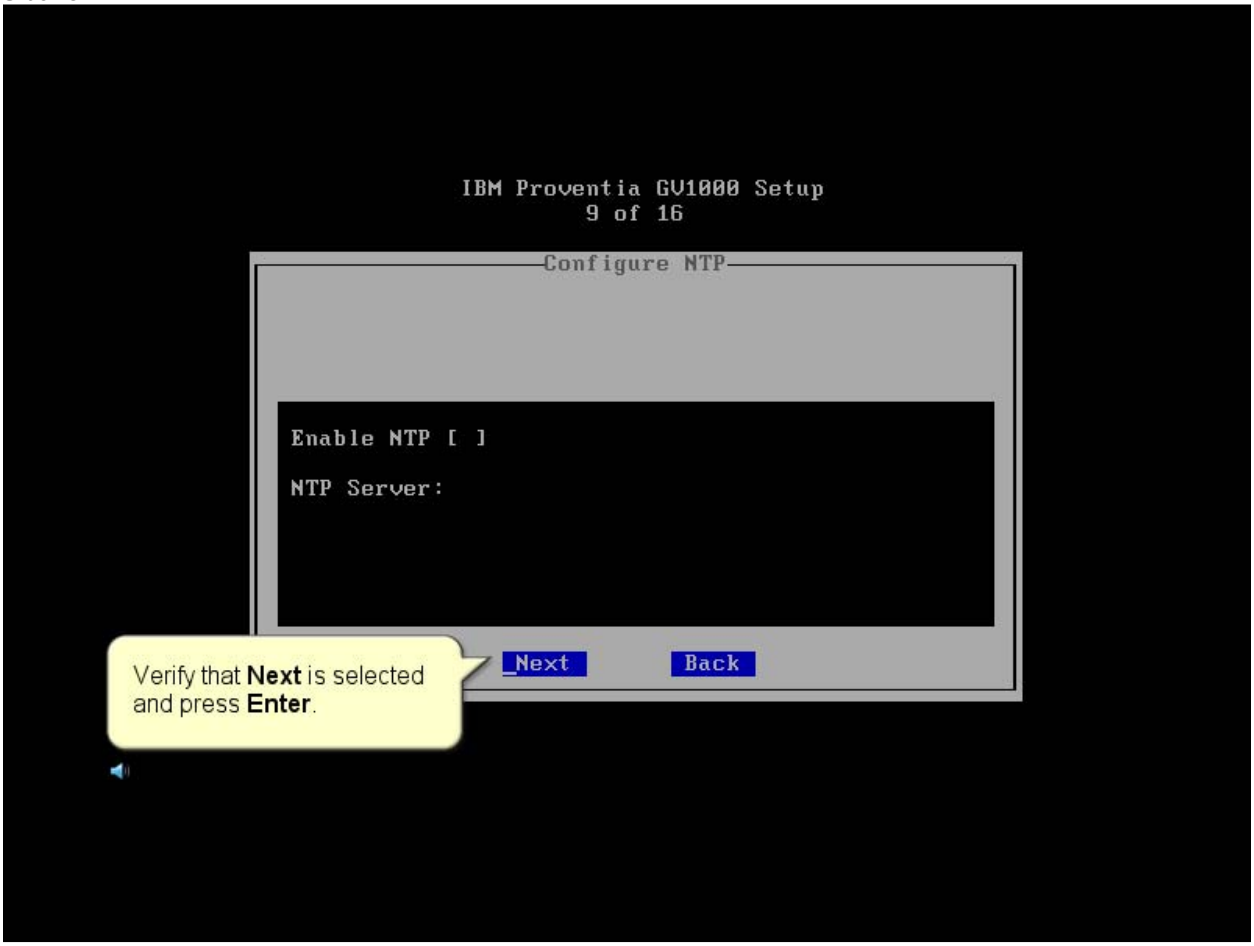
Slide 26

IBM Proventia GV1000 Setup
8 of 16
Time Zone Confirmation
The time zone will be set to
(GMT-05:00) America/New_York.
_OK
Cancel
The utility confirms the time zone. To select the time zone, press **Enter**.
If the time zone is incorrect, press **Tab** to select the **Cancel** button.

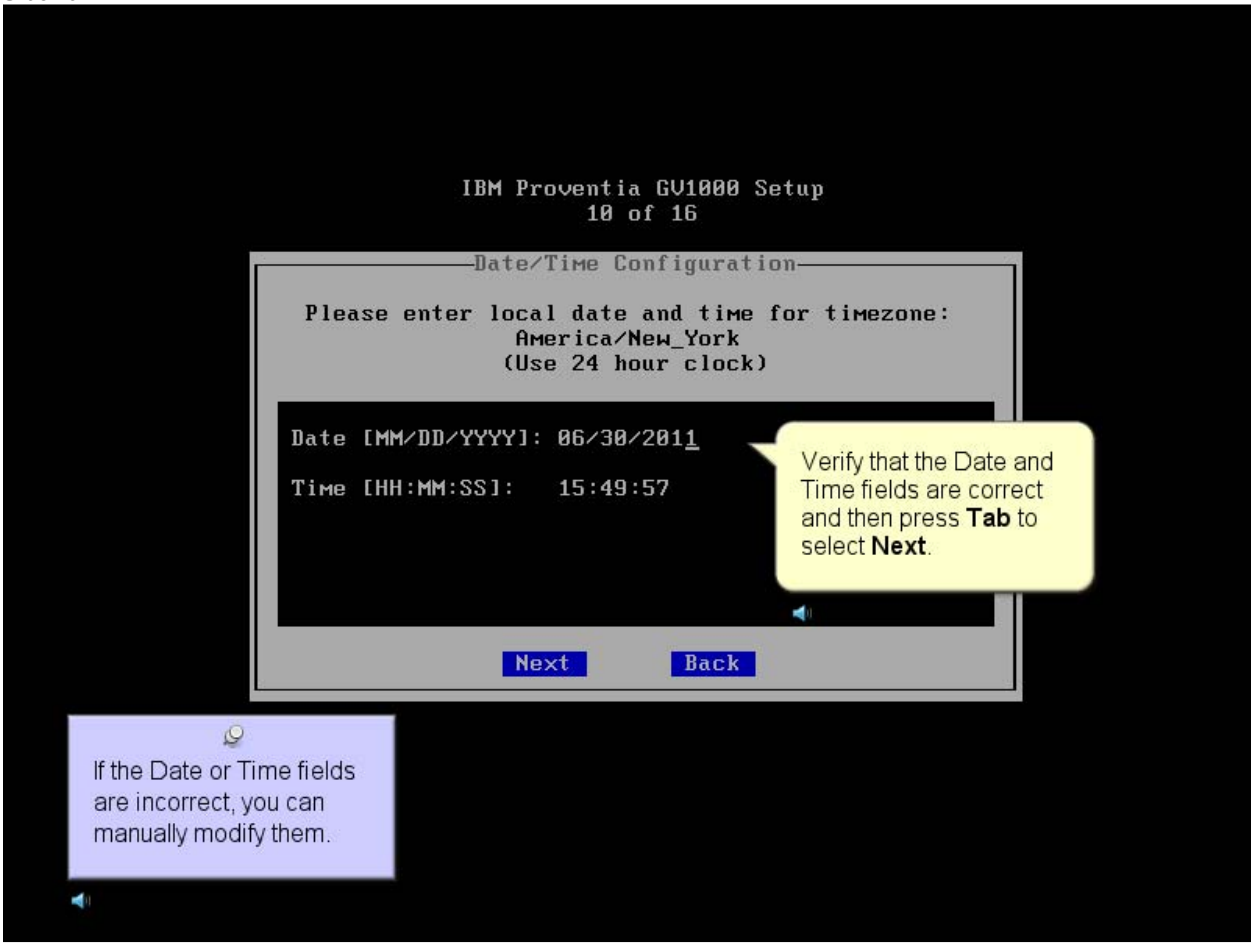
Slide 27


IBM Proventia GV1000 Setup
9 of 16
Configure NTP
Enable NTP [_]
NTP Server:
If the appliance will use a Network Time Protocol (NTP) server, press the space bar to enable NTP and then enter the NTP server IP address.
In this demonstration there is no NTP server, press Tab.
Next
Back

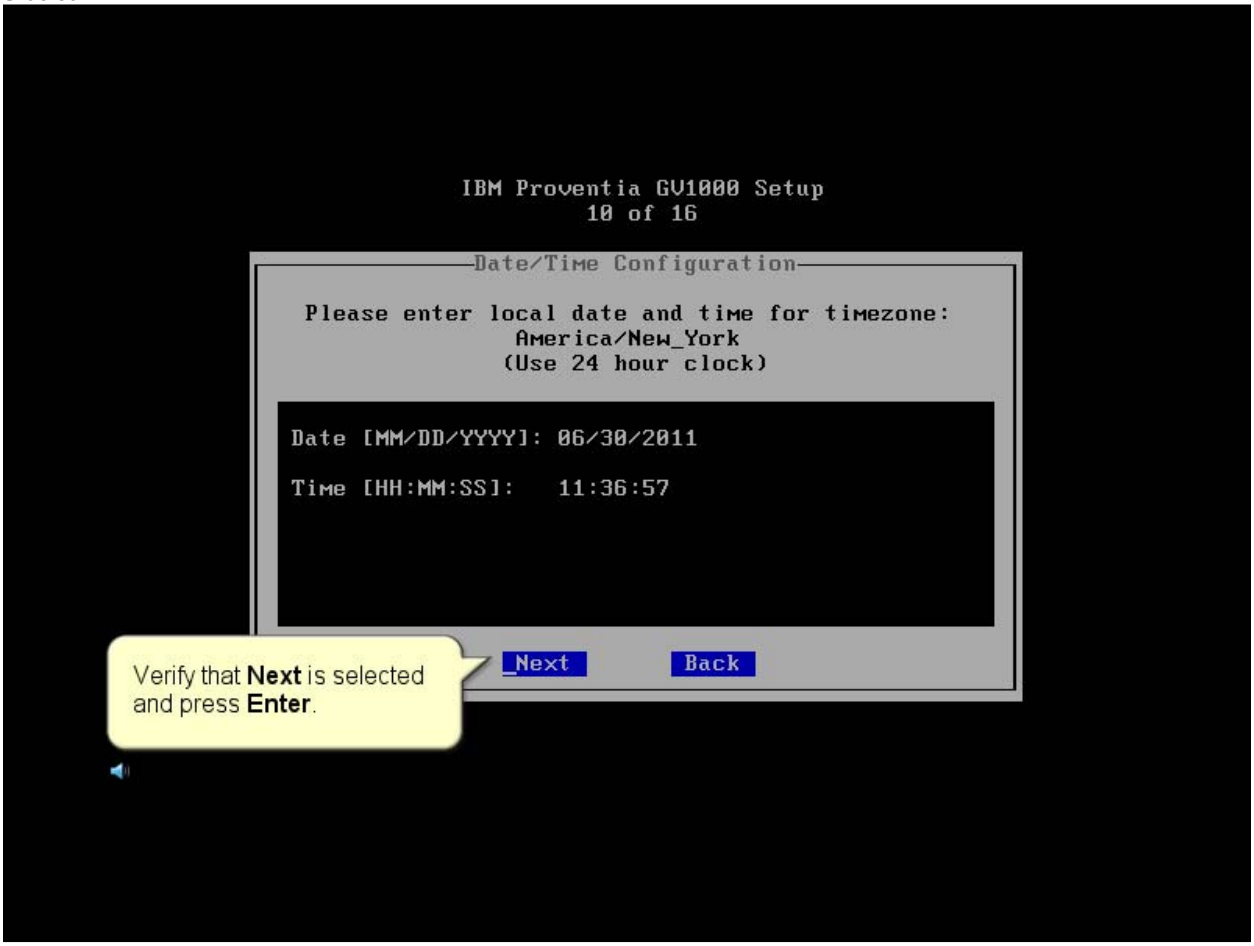
Slide 28


IBM Proventia GV1000 Setup
9 of 16
Configure NTP
Enable NTP [ ]
NTP Server:
Next
Back
Verify that **Next** is selected and press **Enter**.

Slide 29


IBM Proventia GV1000 Setup
10 of 16
Date/Time Configuration
Please enter local date and time for timezone:
America/New_York
(Use 24 hour clock)
Date [MM/DD/YYYY]: 06/30/2011
Time [HH:MM:SS]: 15:49:57
Next
Back
Verify that the Date and Time fields are correct and then press Tab to select Next.
If the Date or Time fields are incorrect, you can manually modify them.

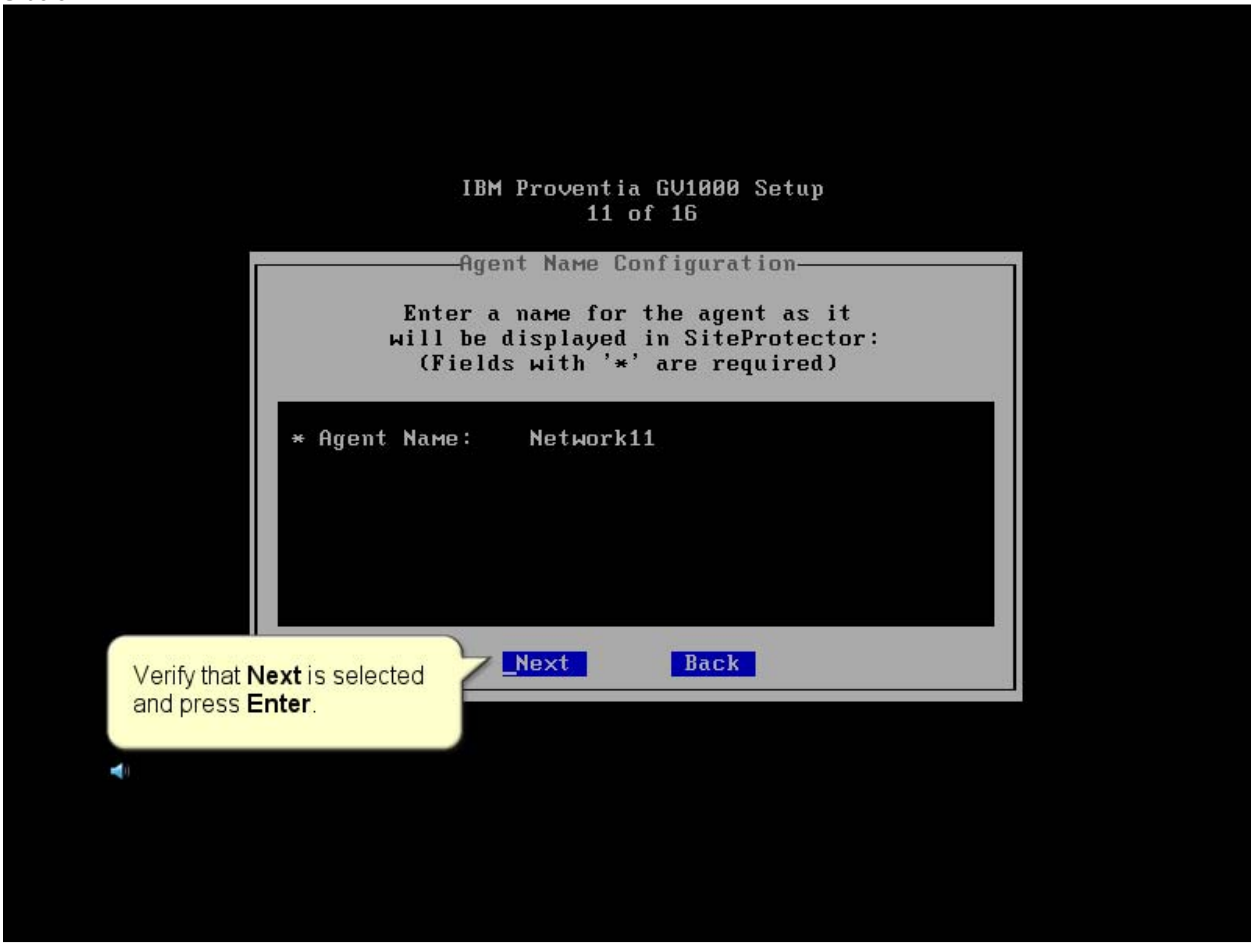
Slide 30


IBM Proventia GV1000 Setup
10 of 16
Date/Time Configuration
Please enter local date and time for timezone:
America/New_York
(Use 24 hour clock)
Date [MM/DD/YYYY]: 06/30/2011
Time [HH:MM:SS]: 11:36:57
Next
Back
Verify that Next is selected and press Enter.

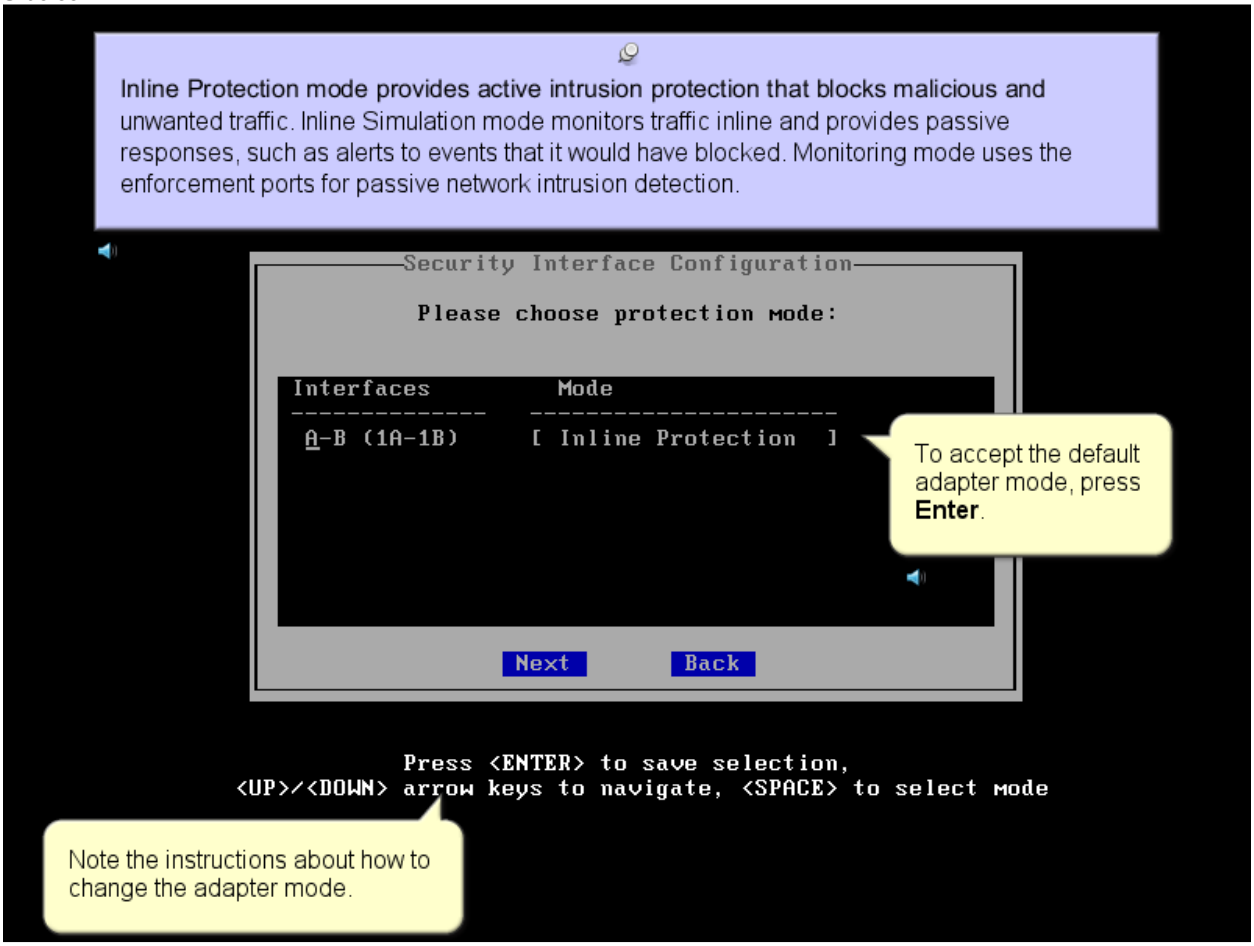
Slide 31

IBM Proventia GV1000 Setup
11 of 16
Agent Name Configuration
Enter a name for the agent as it will be displayed in SiteProtector: (Fields with '*' are required)
* Agent Name: Network11_
To accept the default agent name, press Tab.
The Agent Name is the name that appears for the appliance in the SiteProtector Console. The agent name should correspond to a meaningful classification such as the appliance's geographic location, business unit, or building address.
Next
Back

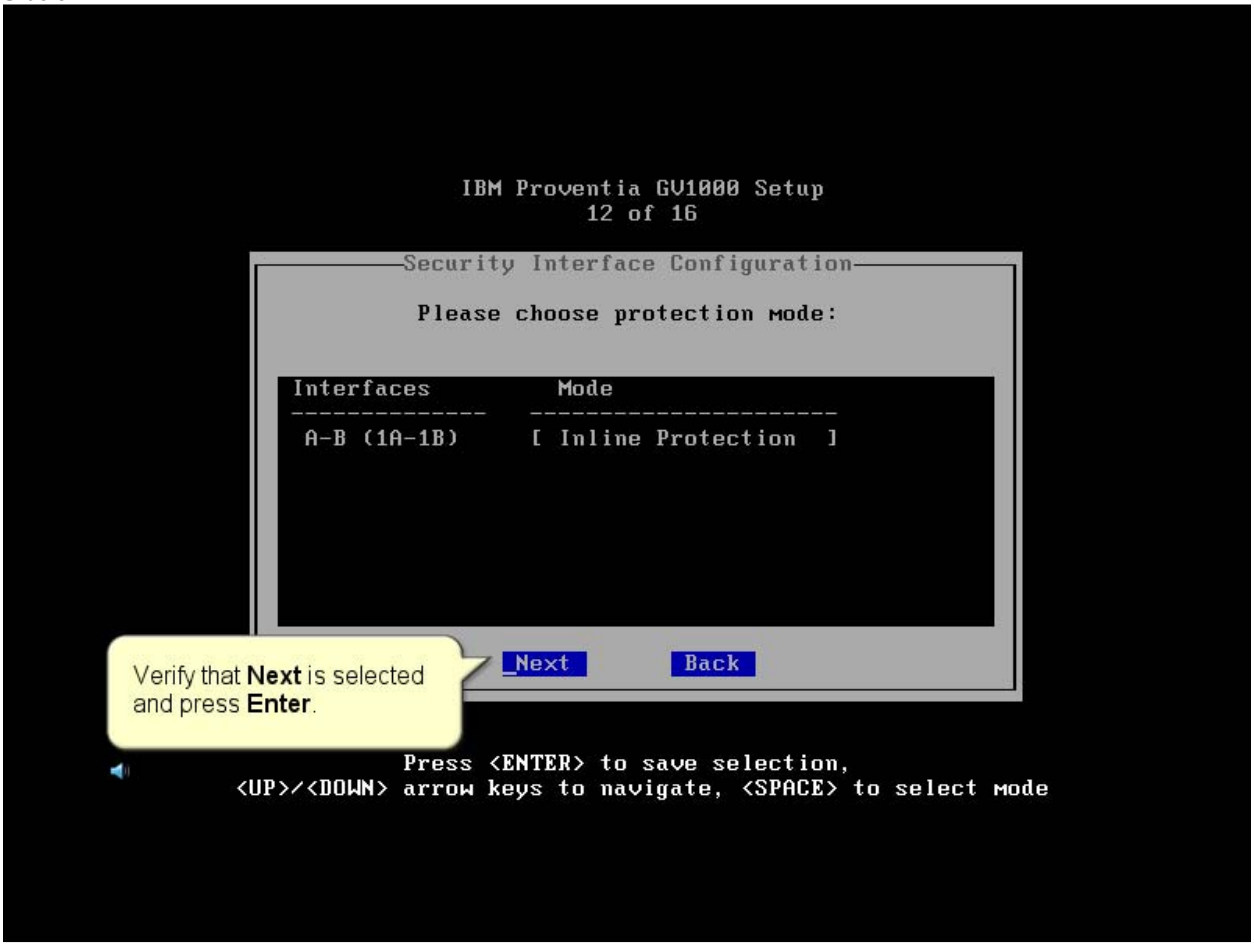
Slide 32


IBM Proventia GV1000 Setup
11 of 16
Agent Name Configuration
Enter a name for the agent as it
will be displayed in SiteProtector:
(Fields with '*' are required)
* Agent Name: Network11
Next
Back
Verify that Next is selected and press Enter.

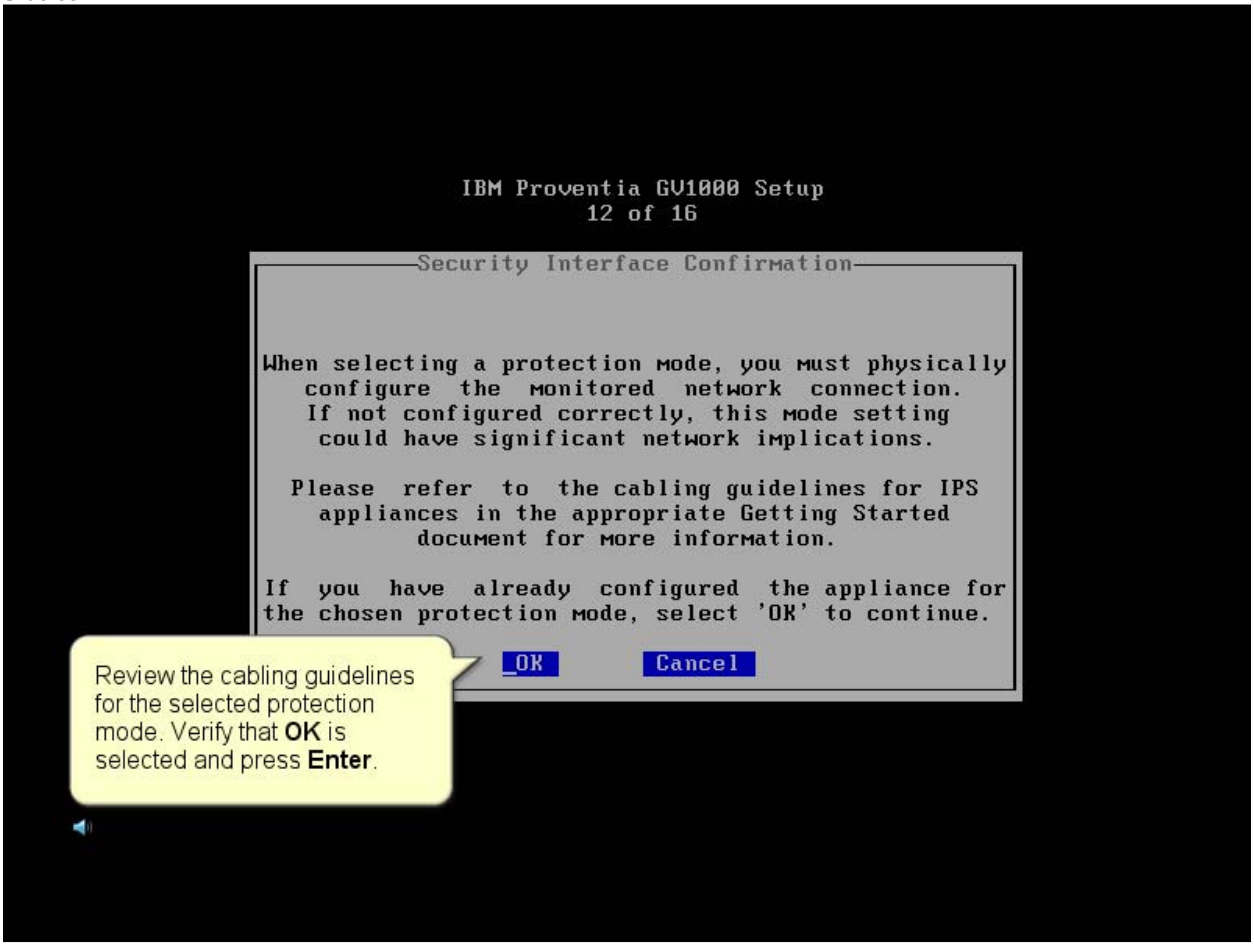
Slide 33


Inline Protection mode provides active intrusion protection that blocks malicious and unwanted traffic. Inline Simulation mode monitors traffic inline and provides passive responses, such as alerts to events that it would have blocked. Monitoring mode uses the enforcement ports for passive network intrusion detection.
Security Interface Configuration
Please choose protection mode:
Interfaces
Mode
A-B (1A-1B)
[Inline Protection]
To accept the default adapter mode, press Enter.
Next
Back
Press <ENTER> to save selection,
<UP>/<DOWN> arrow keys to navigate, <SPACE> to select mode
Note the instructions about how to change the adapter mode.

Slide 34

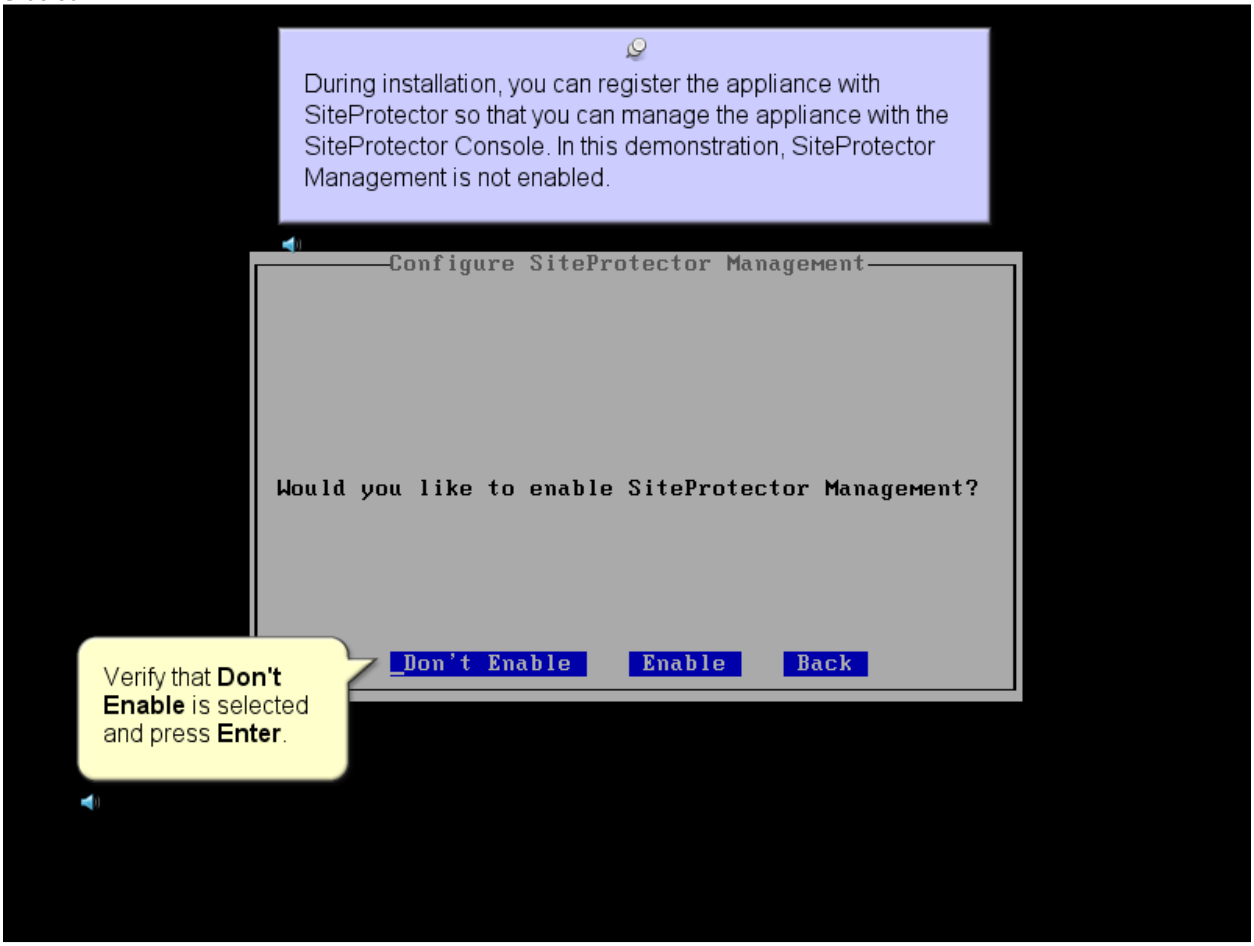

IBM Proventia GV1000 Setup
12 of 16
Security Interface Configuration
Please choose protection mode:
Interfaces
Mode
A-B (1A-1B)
[Inline Protection]
Next
Back
Verify that Next is selected and press Enter.
Press <ENTER> to save selection,
<UP>/<DOWN> arrow keys to navigate, <SPACE> to select mode

Slide 35

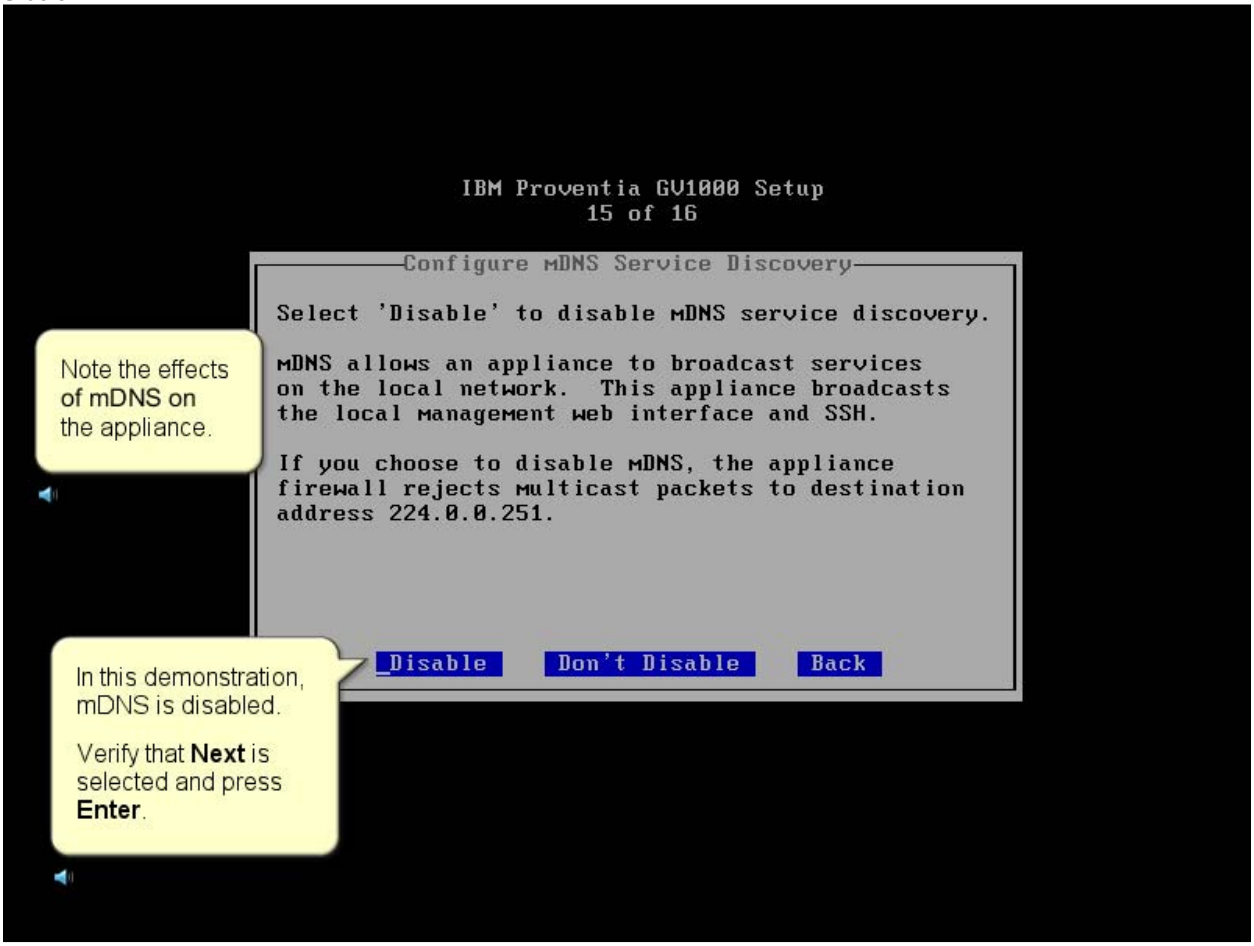

IBM Proventia GV1000 Setup
12 of 16
Security Interface Confirmation
When selecting a protection mode, you must physically configure the monitored network connection. If not configured correctly, this mode setting could have significant network implications.
Please refer to the cabling guidelines for IPS appliances in the appropriate Getting Started document for more information.
If you have already configured the appliance for the chosen protection mode, select 'OK' to continue.
OK
Cancel
Review the cabling guidelines for the selected protection mode. Verify that **OK** is selected and press **Enter**.

Configuring the appliance

Slide 36



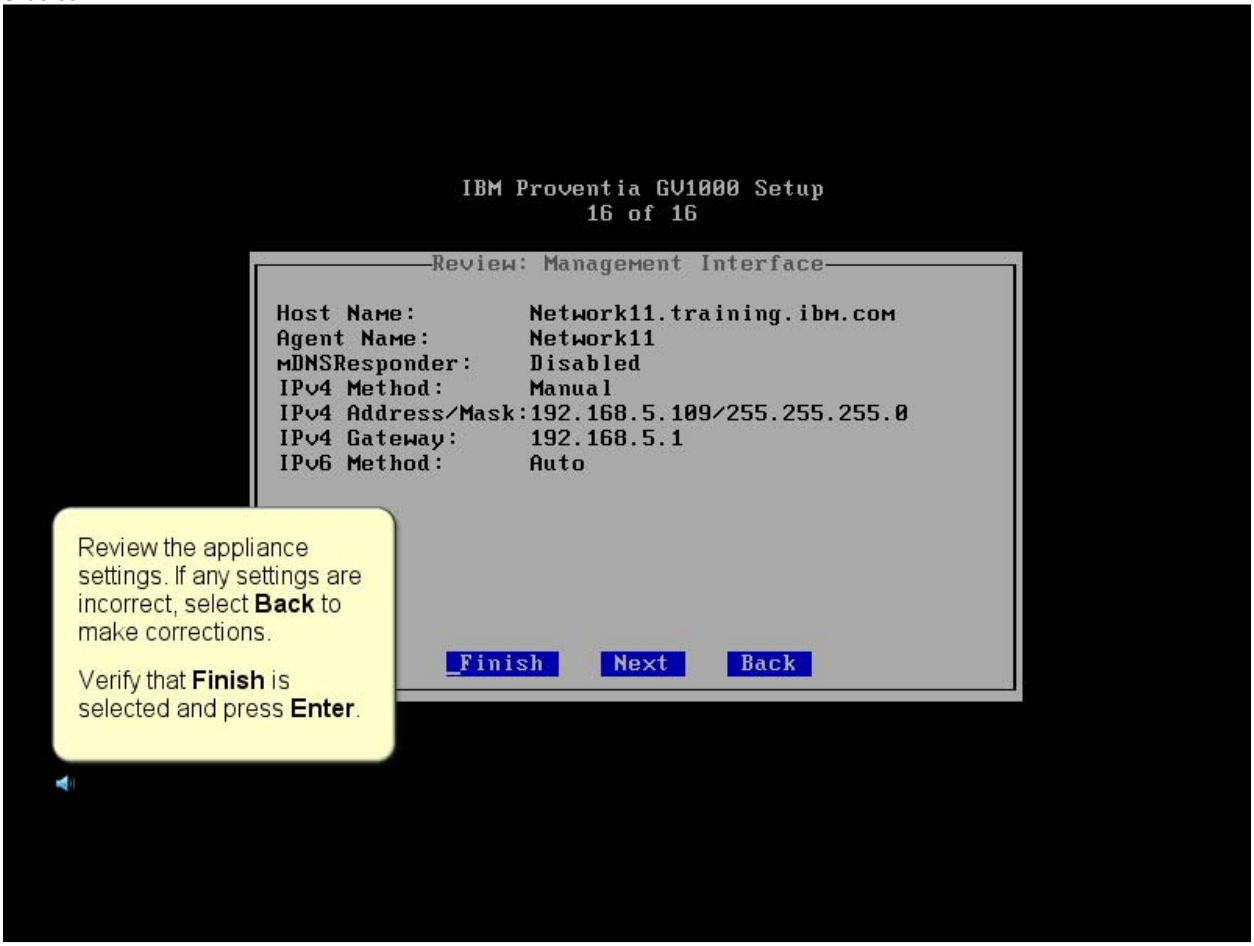
Slide 37


IBM Proventia GV1000 Setup
15 of 16
Configure mDNS Service Discovery
Select 'Disable' to disable mDNS service discovery.
mDNS allows an appliance to broadcast services on the local network. This appliance broadcasts the local management web interface and SSH.
If you choose to disable mDNS, the appliance firewall rejects multicast packets to destination address 224.0.0.251.
_Disable
Don't Disable
Back
Note the effects of mDNS on the appliance.
In this demonstration, mDNS is disabled.
Verify that Next is selected and press Enter.

Slide 38

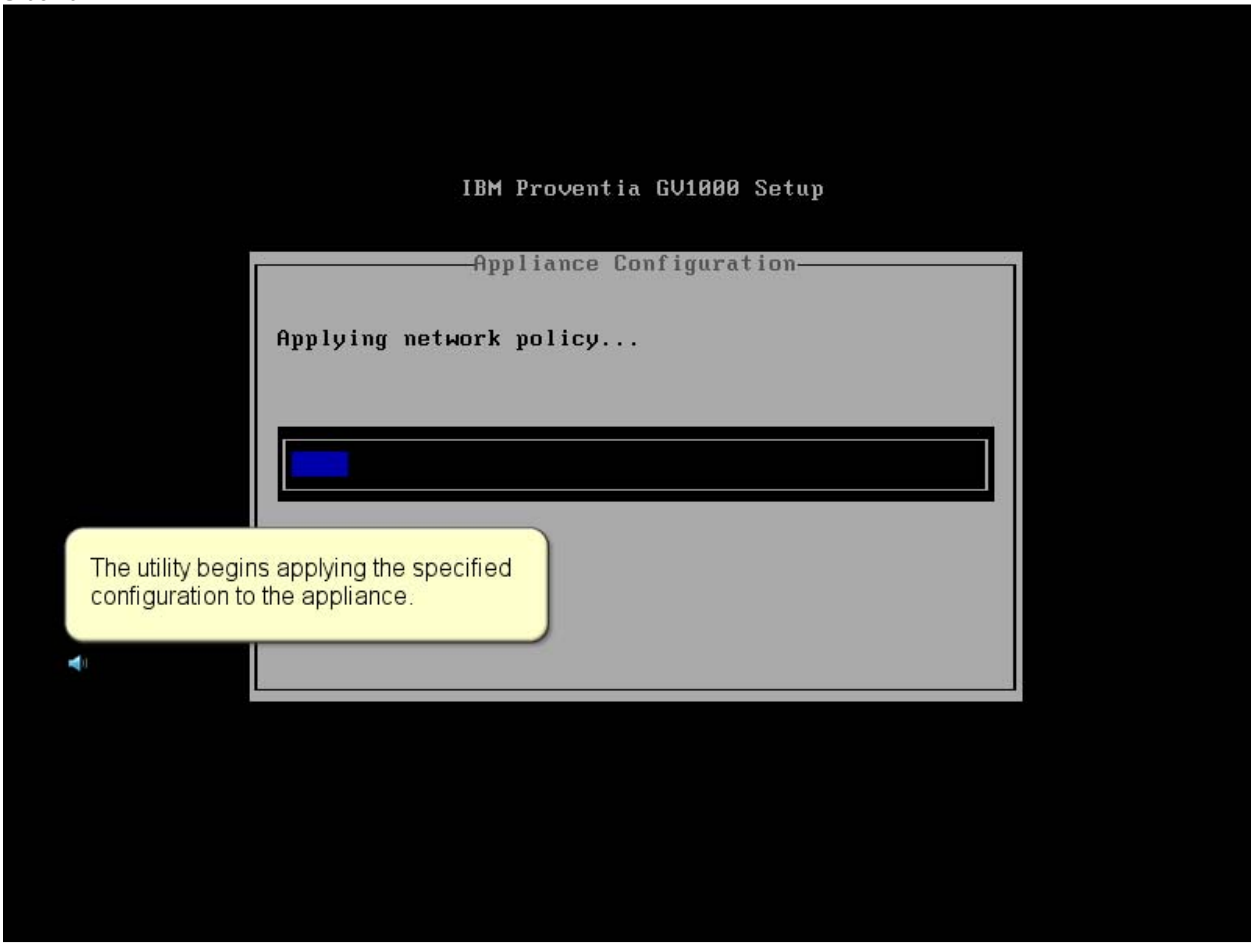
IBM Proventia GV1000 Setup
16 of 16
Review Settings
On the next screens you can review your settings before they are applied.
You can review all settings or press the <Finish> key on any screen to skip the rest of the review and apply your changes.
Note: If you are configuring the appliance via SSH terminal you may lose your connection when the network settings are applied.
You can manually re-connect to the appliance with a new SSH session.
OK
Back
To review the appliance settings, verify that OK is selected and press Enter.

Slide 39


IBM Proventia GV1000 Setup
16 of 16
Review: Management Interface
Host Name: Network11.training.ibm.com
Agent Name: Network11
mDNSResponder: Disabled
IPv4 Method: Manual
IPv4 Address/Mask: 192.168.5.109/255.255.255.0
IPv4 Gateway: 192.168.5.1
IPv6 Method: Auto
Finish
Next
Back
Review the appliance settings. If any settings are incorrect, select Back to make corrections.
Verify that Finish is selected and press Enter.

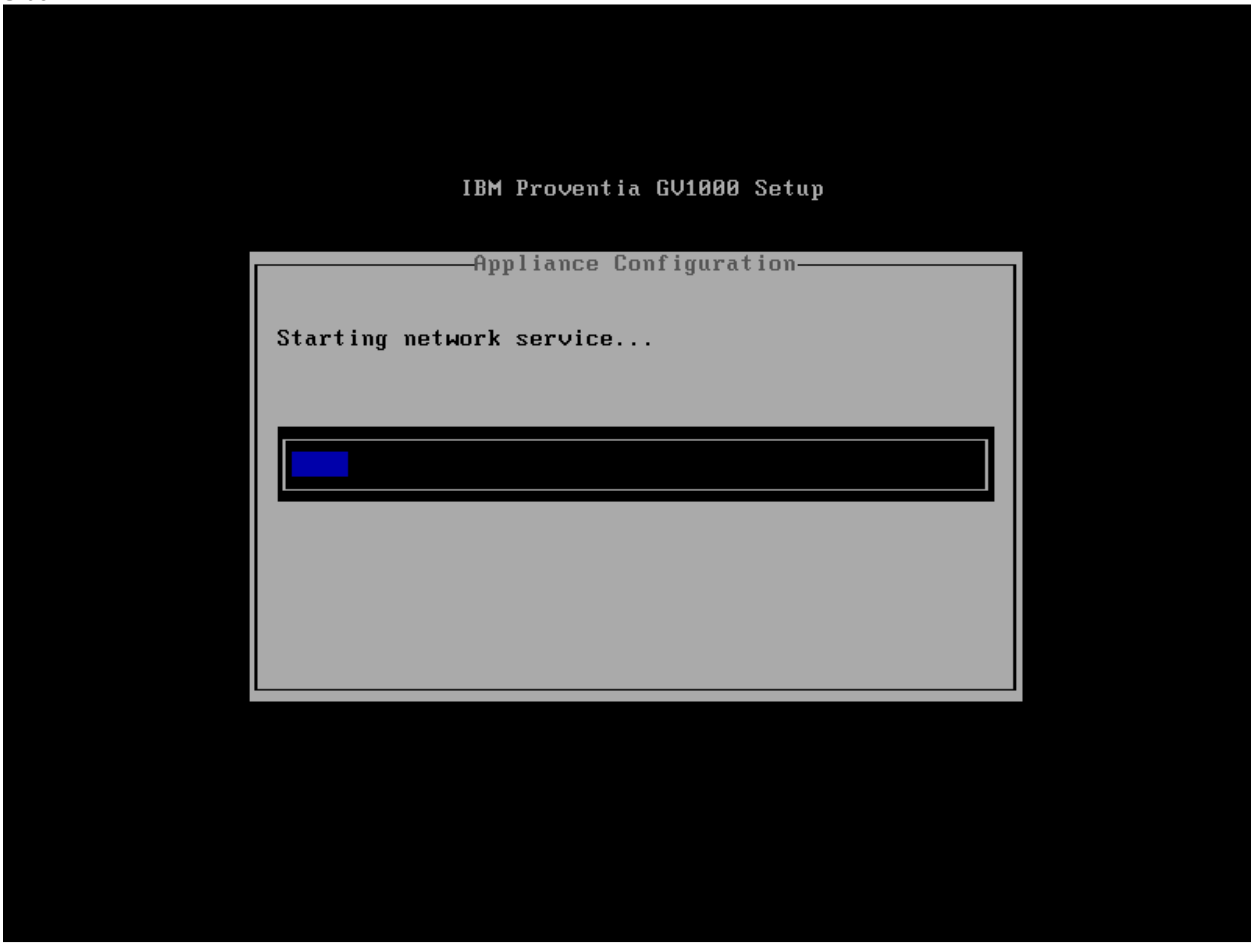
Configuring the appliance

Slide 40



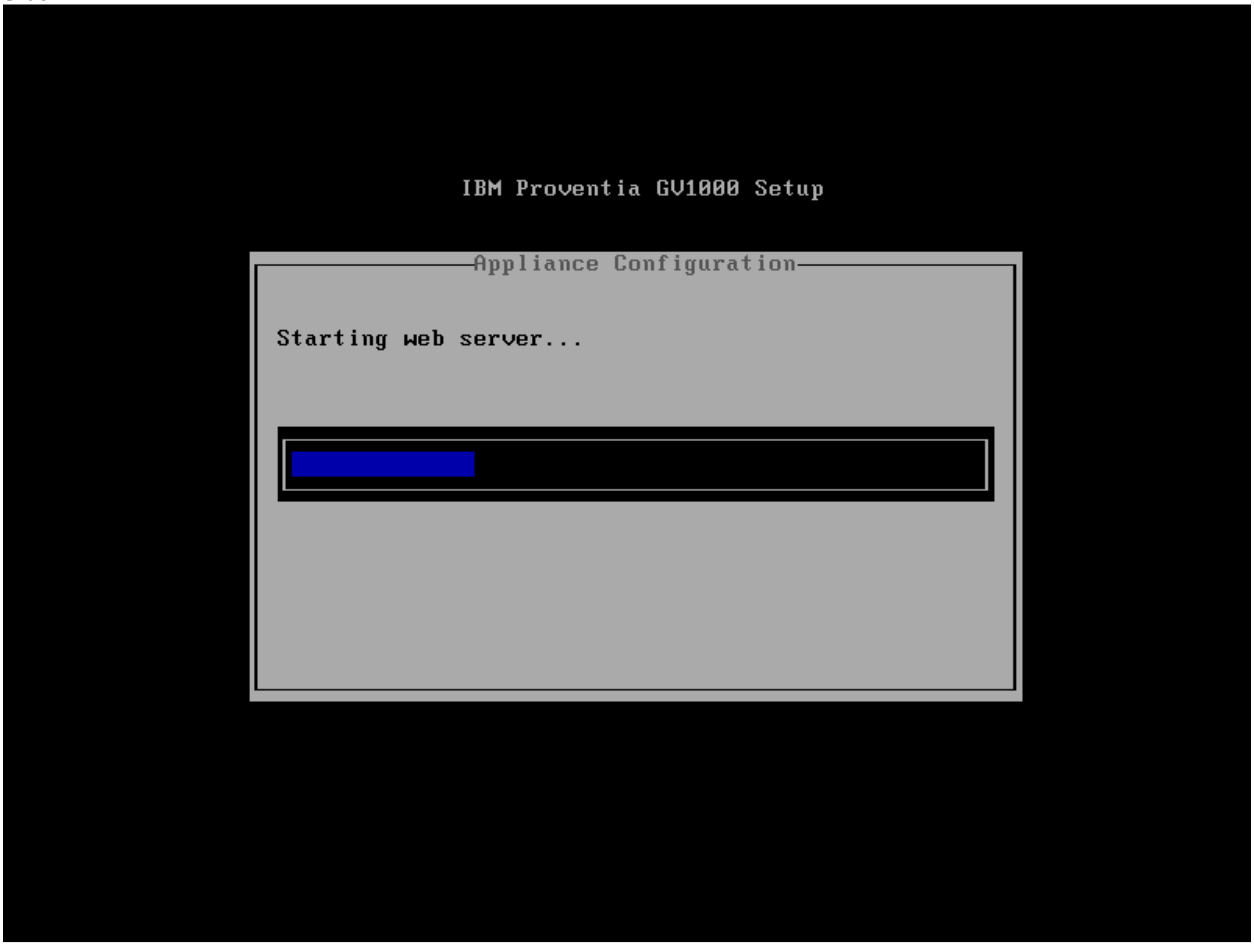
Configuring the appliance

Slide 41



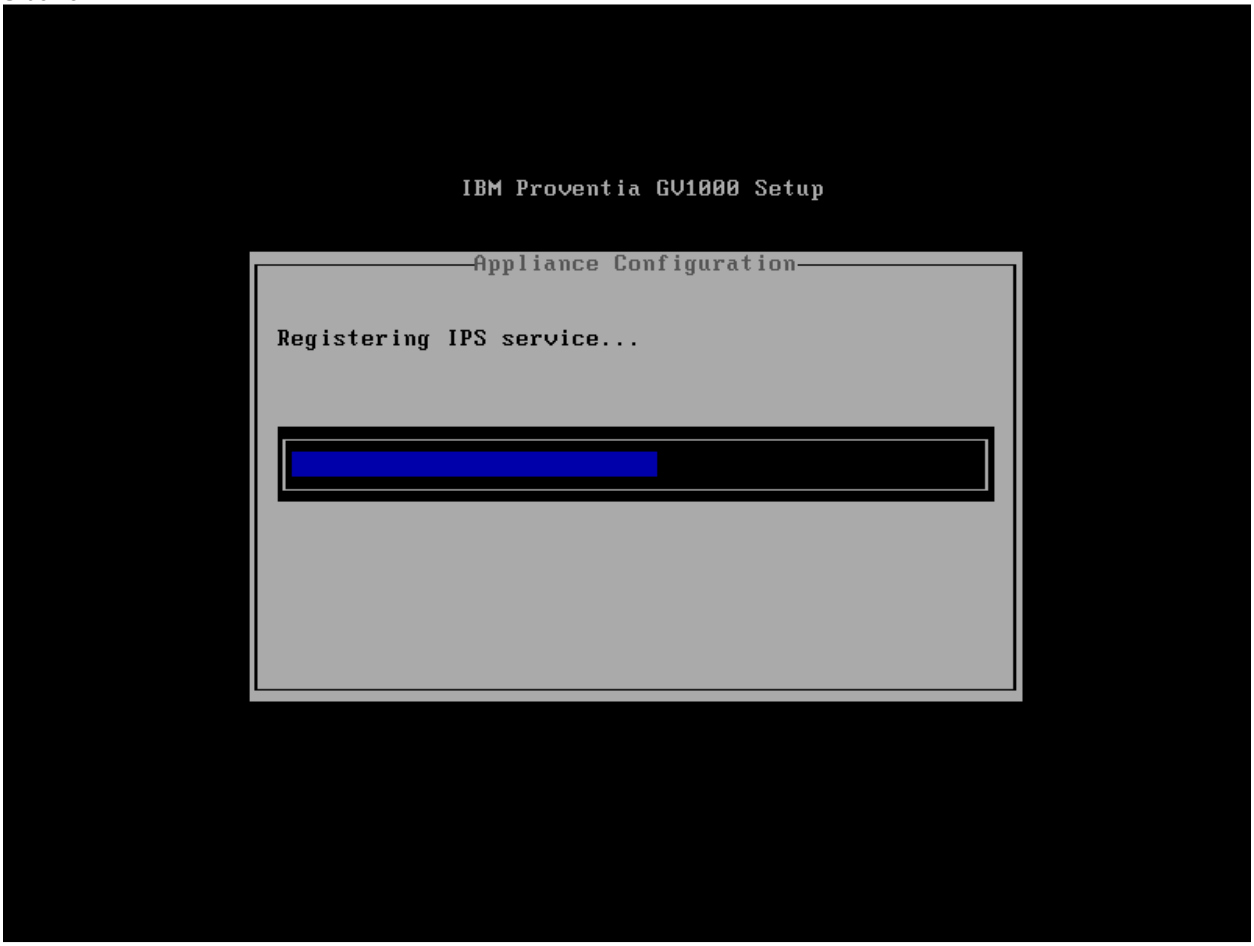
Configuring the appliance

Slide 42

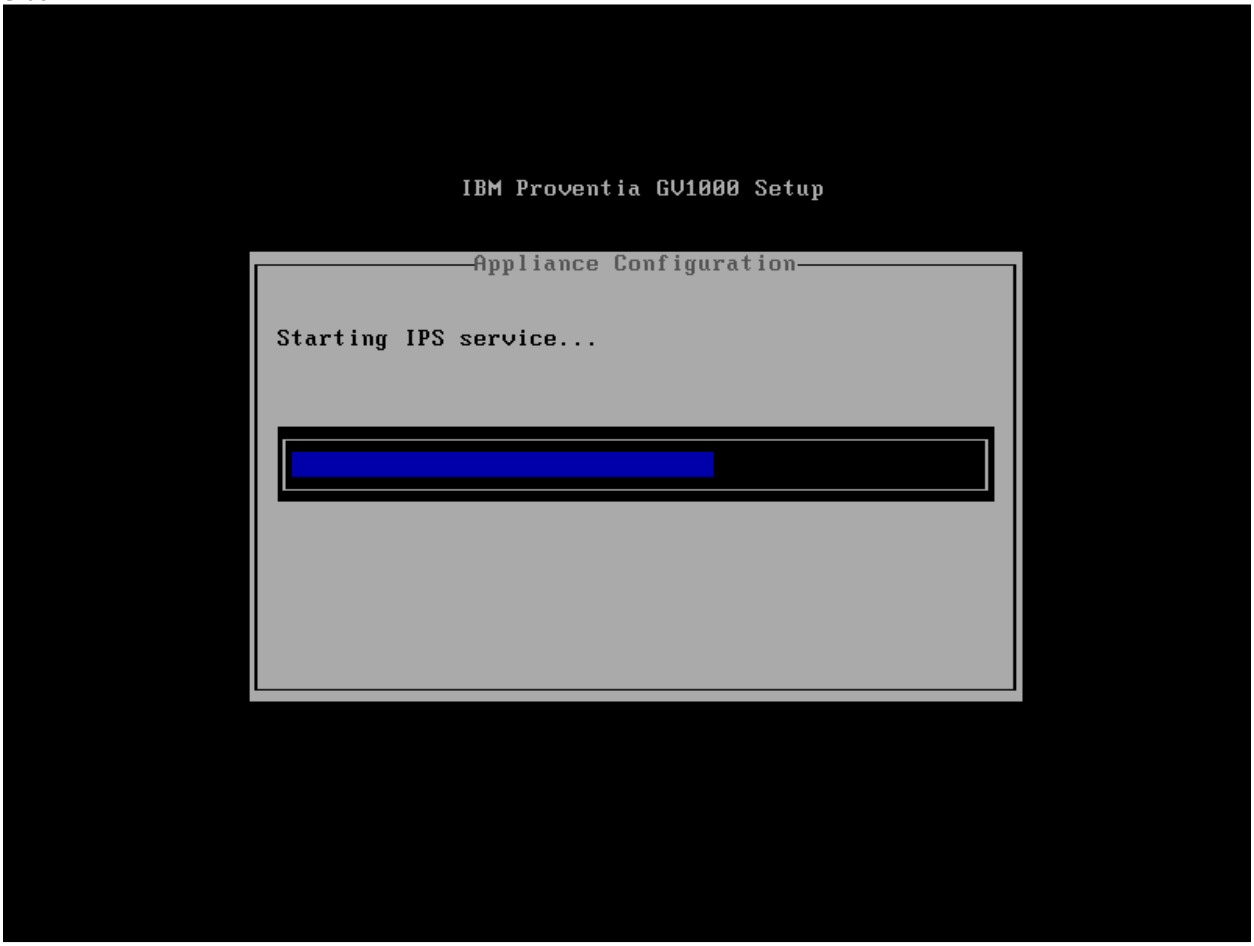


Configuring the appliance

Slide 43

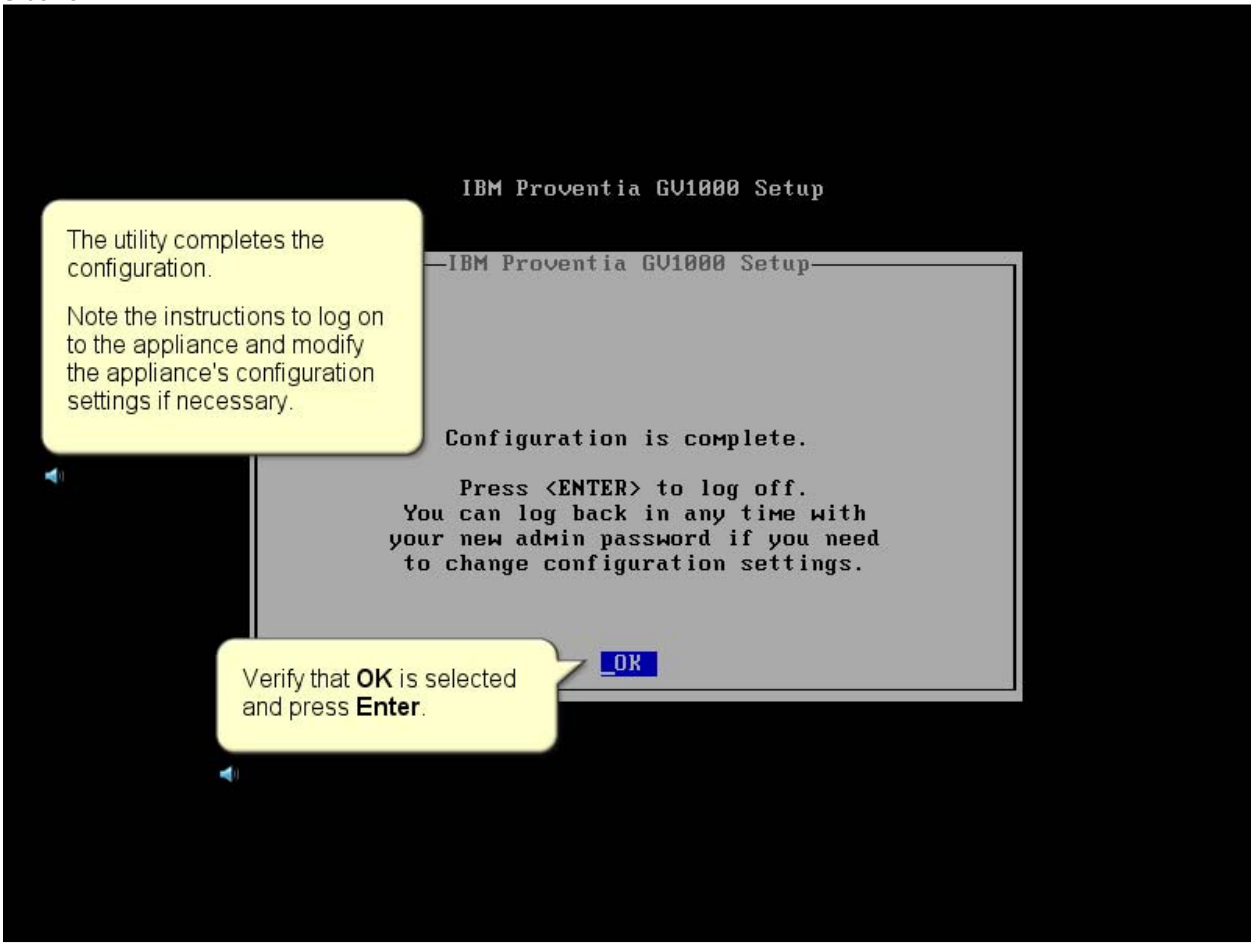


Slide 44


IBM Proventia GV1000 Setup
Appliance Configuration
Starting IPS service...

Configuring the appliance

Slide 45



Slide 46

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" 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.