Application Notes for Configuring an IBM Proventia Network Intrusion Prevention System for Supporting an Avaya Telephony Infrastructure using Avaya Communication Manager in a Converged VoIP and Data Network - Issue 1.1

Abstract

These Application Notes describe the steps for configuring the IBM Proventia Network Intrusion Prevention System to support an Avaya IP Telephony infrastructure consisting of a Corporate Headquarters with three remote sites.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration of a Voice over IP (VoIP) solution using IBM Proventia GX5208 appliances and IBM Proventia Management SiteProtector SP1001 with an Avaya Telephony Infrastructure consisting of Avaya Communication Manager, Avaya SIP Enablement Services (SES), Avaya Modular Messaging, Avaya IA 770 INTUITY AUDIX and Avaya IP telephones. Compliance testing emphasis was placed on validating that Avaya VoIP telephony features worked properly under various security threats with the IBM Proventia Network Intrusion Prevention System in place.

The IBM Proventia Network Intrusion Prevention Security System is designed to identify VoIP traffic and analyze the payload for known or suspected attacks. It can alert administrators to attacks and anomalous traffic, or block it outright, even without a pattern matching signature update. The solution helps identify and protect VoIP services against known and unknown threats before they impact the network. The IBM Proventia Network Intrusion Prevention Security System provides the following security capabilities:

- Support for networking capabilities like Quality of Service (QoS), dynamic port assignment and Network Address Translation (NAT) traversal, without interfering with QoS deliverables.
- VoIP traffic auditing and attack protection using the IBM Proventia Intrusion Prevention System (IPS), with robust parsing and analysis of key VoIP protocols including Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), H.323, H.245, H.225, Q.931, T.120 and Skinny Client Control Protocol (SCCP).
- Protection from remote Transmission Control Protocol (TCP)/User Diagram Protocol (UDP)-based attacks, mis-configurations and vulnerabilities in the underlying operating systems such as Microsoft Windows, UNIX and Linux.
- Network-layer protection from distributed denial of service (DDoS) attacks, worm propagation and other attacks which exhaust network bandwidth.

1.1. Interoperability Compliance Testing

The interoperability compliance test covered feature functionality, serviceability, and performance testing. The emphasis in the compliance test was placed on validating that Avaya VoIP telephony features worked properly under various security threats with the IBM Proventia Network Intrusion Prevention System in place.

The telephony features verified to operate correctly included attended/unattended transfer, conference call participation, conference call add/drop, multiple call appearances, caller ID operation, call forwarding unconditional, call forwarding on busy, call park, call pick-up, bridged call appearances, voicemail using Avaya Modular Messaging and Avaya IA770 INTUITY AUDIX , Message Waiting Indicator (MWI), and hold and return from hold

Serviceability testing was conducted to verify the ability of the Avaya/IBM VoIP solution to recover from adverse conditions, such as power cycling network devices and disconnecting cables between the LAN interfaces. In all cases, the ability to recover after the network normalized from failures was verified.

1.2. Support

Technical Support for IBM ISS Products is Available 24/7/365.

Americas

- Customer Support Portal: https://www.iss.net/issEn/MYISS/login_help.jhtml
- Phone: 888-447-4861 (Toll free in U.S. or Canada) or 404-236-2700
- E-mail: support@iss.net
- Web: http://iss.net/support
- Customer Support Knowledgebase: http://www.iss.net/support/knowledgebase

2. Reference Configuration

The configuration in **Figure 1** shows a converged VoIP and data network with multiple remote sites. The extension numbers beginning with the number 5 are registered with Avaya Communication Manager in the Main Site and extension numbers beginning with the number 4 are registered with the Remote Site B Avaya Communication Manager. For compliance testing, a centralized corporate DHCP server was used. To better manage the different traffic types, the voice and data traffic were separated onto different VLANs.

2.1. Corporate Headquarters

The Corporate Headquarters consisted of one IBM Proventia GX5208, one IBM Proventia Management SiteProtector SP1001, one Brocade FastIron SuperX Switch, one Avaya Communication Manager running on an Avaya S8300 Server with an Avaya G450 Media Gateway, Avaya SIP Enablement Services (SES), Avaya Modular Messaging, Avaya IA 770 INTUITY AUDIX , one Avaya 2410 Digital Telephone, one Avaya 9630 IP Telephone running Avaya one-X Deskphone Edition on VLAN Voice1, one Avaya 9640 IP Telephone running Avaya one-X Deskphone SIP on VLAN Voice1 and one Corporate DHCP/File server. The Corporate Headquarters provided a DHCP/File server for assigning IP network parameters and to download settings to the Avaya IP telephones.

2.2. Remote Site A

Remote Site A consisted of one IBM Proventia GX5208, one Brocade FastIron GS Switch, one Avaya 9650 IP Telephone running Avaya one-X Deskphone Edition, one Avaya 9620 IP Telephone running Avaya one-X Deskphone SIP, and a PC on data network. The Avaya IP telephones register to headquarters Avaya Communication Manager.

2.3. Remote Site B

Remote Site B consisted of one IBM Proventia GX5208, one Brocade FastIron GS Switch, one Avaya Communication Manager running on an Avaya S8300 Server with an Avaya G700 Media Gateway, one Avaya 2410 Digital Telephone, one Avaya 9640G IP Telephone running Avaya one-X Deskphone Edition, one Avaya 9630 IP Telephone running Avaya one-X Deskphone Edition, and a PC on data network. The Avaya IP telephones register to the Remote Site B Avaya Communication Manager. An H.323 trunk was configured between the Avaya

Communication Manager systems at the Corporate Headquarters and Remote Site B to allow direct dialing between the sites.

2.4. Remote Site C

Remote Site C consisted of one IBM Proventia GX5208, one Brocade FastIron GS Switch, one Avaya G700 Media Gateway, and two Avaya 2410 Digital Telephones. The Remote Site C Avaya Media Gateway registers to the headquarters Avaya Communication Manager. While the Avaya 2410 Digital Telephones are directly connected to the Remote Site C Avaya Media gateway, they are administered on the headquarters Avaya Communication Manager.

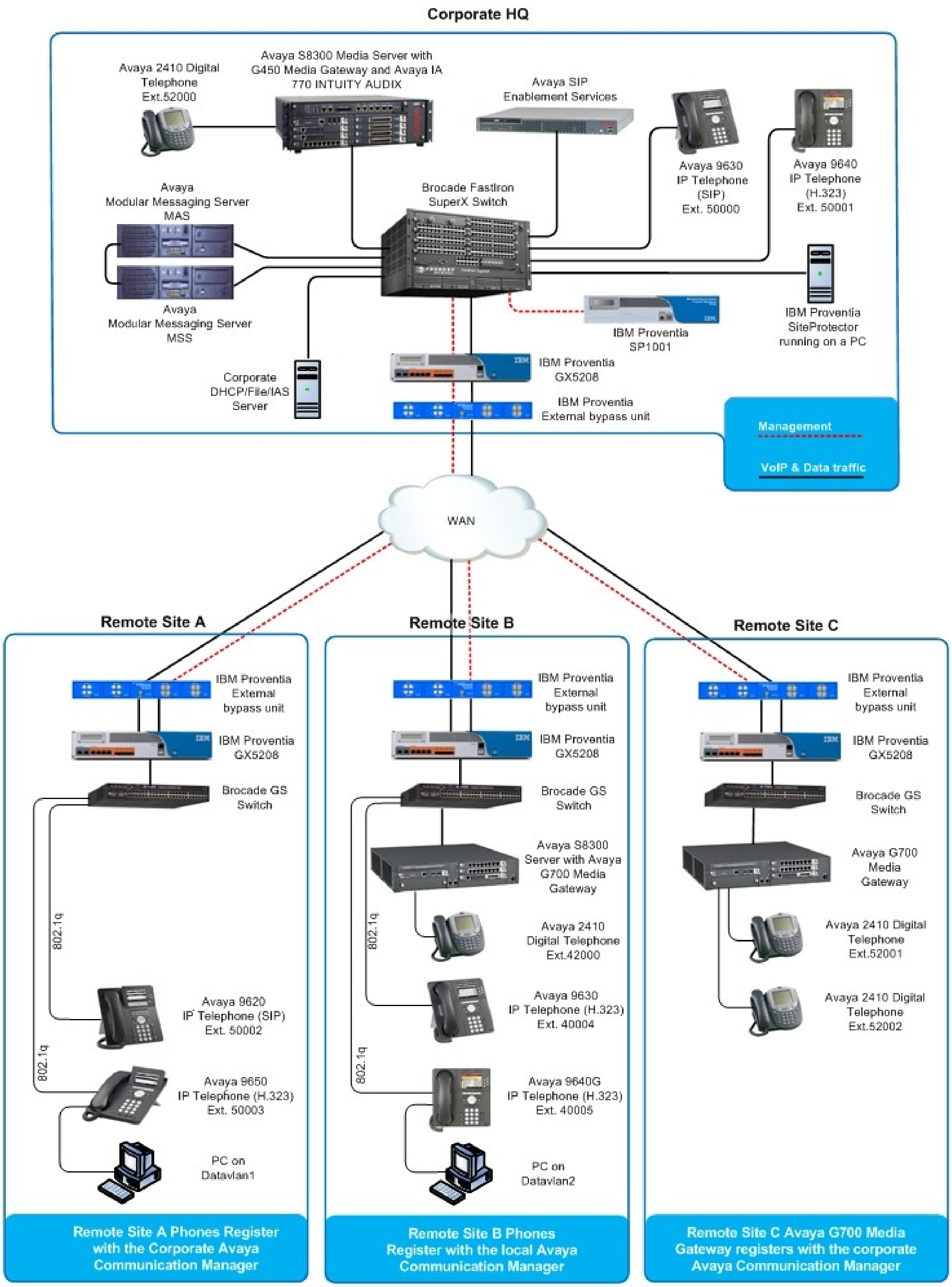

Corporate HQ
Avaya 2410 Digital Telephone Ext.52000
Avaya S8300 Media Server with G450 Media Gateway and Avaya IA 770 INTUITY AUDIX
Avaya SIP Enablement Services
Avaya 9630 IP Telephone (SIP) Ext. 50000
Avaya 9640 IP Telephone (H.323) Ext. 50001
Avaya Modular Messaging Server MAS
Brocade FastIron SuperX Switch
Avaya Modular Messaging Server MSS
IBM Proventia SP1001
IBM Proventia SiteProtector running on a PC
Corporate DHCP/File/IAS Server
IBM Proventia GX5208
IBM Proventia External bypass unit
Management
VoIP & Data traffic
WAN
Remote Site A
Remote Site B
Remote Site C
IBM Proventia External bypass unit
IBM Proventia GX5208
Brocade GS Switch
802.1q
Avaya 9620 IP Telephone (SIP) Ext. 50002
Avaya 9650 IP Telephone (H.323) Ext. 50003
PC on Datavlan1
Remote Site A Phones Register with the Corporate Avaya Communication Manager
IBM Proventia External bypass unit
IBM Proventia GX5208
Brocade GS Switch
Avaya S8300 Server with Avaya G700 Media Gateway
802.1q
Avaya 2410 Digital Telephone Ext.42000
Avaya 9630 IP Telephone (H.323) Ext. 40004
Avaya 9640G IP Telephone (H.323) Ext. 40005
PC on Datavlan2
Remote Site B Phones Register with the local Avaya Communication Manager
IBM Proventia External bypass unit
IBM Proventia GX5208
Brocade GS Switch
Avaya G700 Media Gateway
Avaya 2410 Digital Telephone Ext.52001
Avaya 2410 Digital Telephone Ext.52002
Remote Site C Avaya G700 Media Gateway registers with the corporate Avaya Communication Manager

Figure 1: Sample Network Configuration

3. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

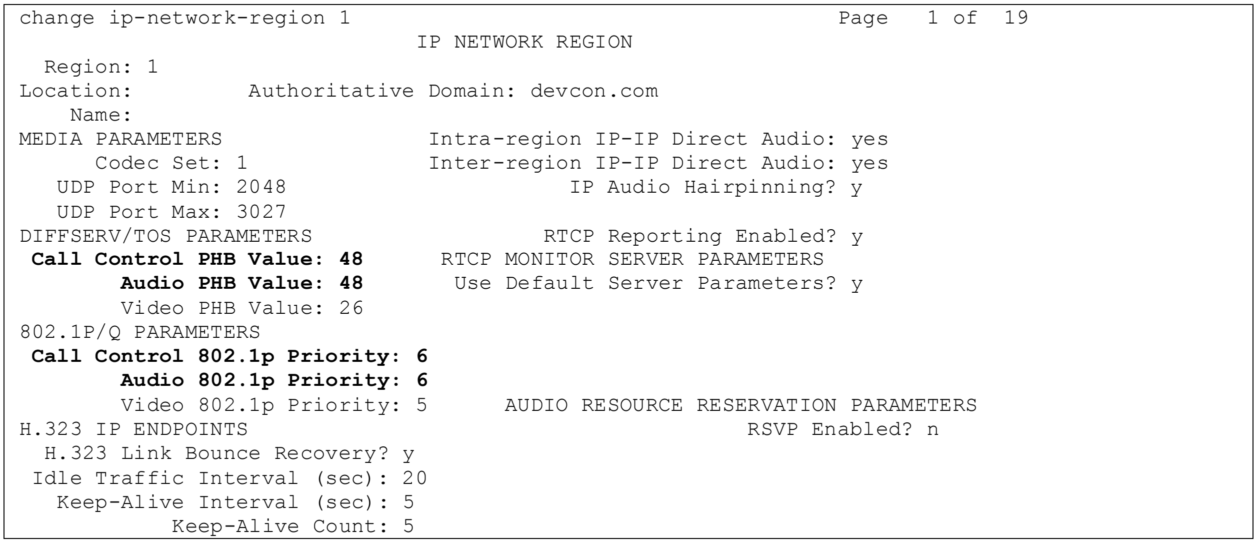
Equipment	Software/Firmware
Avaya PBX Products	
Avaya S8300 Server running Avaya Communication Manager	Avaya Communication Manager 5.1.2
Avaya G450 Media Gateway (Corporate Site) MGP MM712 DCP Media Module Avaya IA 770 INTUITY AUDIX	 28.22.0 HW9 5.1.2
Avaya G700 Media Gateway (Remote Site B) MGP MM712 DCP Media Module	 28.22.0 HW9
Avaya G700 Media Gateway (Remote Site C) MM712 DCP Media Module	 HW9
Avaya SIP Enablement Services (SES)	
Avaya SIP Enablement Services (SES) Server	5.1.2
Avaya Messaging (Voice Mail) Products	
Avaya Modular Messaging - Messaging Application Server (MAS)	4.0
Avaya Modular Messaging - Message Storage Server (MSS)	4.0
Avaya IA 770 INTUITY AUDIX	5.1
Avaya Telephony Sets	
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone Edition 3.0
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone SIP 2.0.0
Avaya 2410 Digital Telephone	5.0
IBM Intrusion Prevention System Products	
IBM Proventia GX5208	1.7(XPU 29.030)
IBM Proventia SP1001	1.7(XPU 29.030)
IBM External Bypass Unit	n/a
Brocade Products	
Brocade FastIron SuperX Switch	05.0.00T3e3
Brocade FastIron GS Switch with routing enabled	04.3.01T7e3
Brocade FastIron GS Switch	04.3.01T7e1
MS Products	
Microsoft Windows 2003 Server	File/DHCP Service

4. Configure Avaya Communication Manager

This section shows the steps used to configure Avaya Communication Manager. For detailed information on the installation, maintenance, and configuration of Avaya Communication Manager, refer to **[1]**.

Use the **change ip-network-region 1** command to change the DIFFSERV/TOS PARAMETERS and 802.1P/Q PARAMETERS settings configured in Avaya Communication Manager.

The Differentiated Services Code Point (DSCP) value of 48 will be used for both PHB values. DSCP 48 represents the traffic class of premium and the traffic type voice. Set the **Call Control PHB Value** to **48** and the **Audio PHB Value** to **48**. **Call Control 802.1p Priority** and **Audio 802.1p Priority** are set to **6**.



```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: devcon.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 3027
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 48      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 48       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                        RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5. Configure IBM Proventia Network IPS SP1001

The following steps detail the initial configuration of the IBM Proventia SP1001 via the front liquid crystal display (LCD).

Configure the IP Address, Subnet Mask, and Default Gateway for the IBM Proventia SP1001 using the front LCD display panel.

↵ = Enter ▲ = Up ▼ = Down ▶ = right ◀ = Down

Press ↵ on the LCD panel. The LCD displays a message asking to set up the network.

Highlight **OK**, and then press ↵.

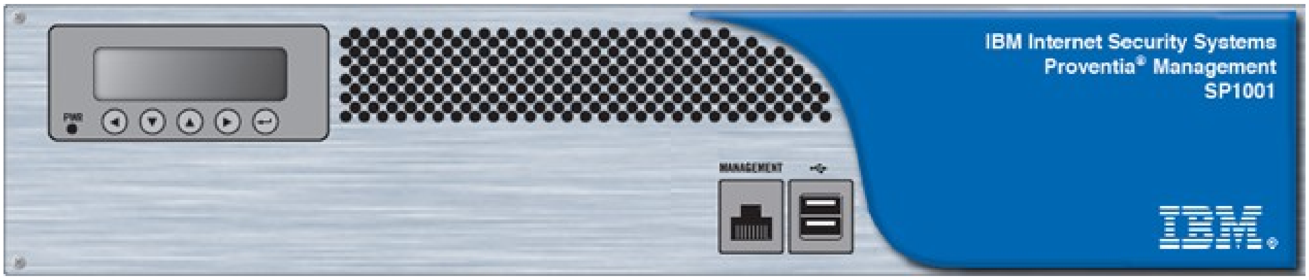
Press ↵ on the LCD panel to display the IP Address screen.

Press the ▲ and ▼ arrows to select a number, and then press the ▶ arrow to move to the next field, ◀ to move back.

When completing all of the fields, press ↵.

Select **OK** to move forward, and then press ↵ to confirm the selection.

Complete these steps again to provide the Subnet Mask and Default Gateway settings.
After entering all of the network information, a final conformation screen appears. Select **OK** to save all network information and enable the Management port, or select **Cancel** to return to the IBM Proventia SP1001 screen without saving any information.
After confirming the settings, the appliance generates a temporary, case-sensitive password.
Record this password, it must be used to log on to the appliance.



6. Configure the IBM Proventia Network IPS GX5208

6.1. Configure the IBM Proventia Network IPS GX5208

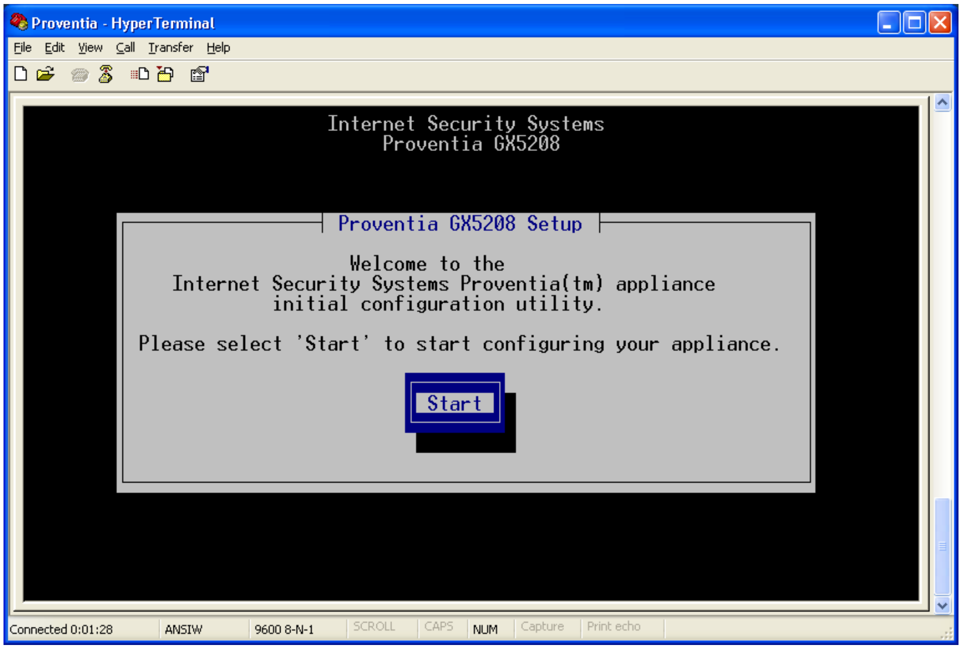
The following steps detail the initial configuration of the IBM Proventia GX5208 Appliance via the command line interface over a console connection. This process should be uses for all of the IBM Proventia Network IPS GX5208's in this test bed. Change the names and IP addresses according

Connect a computer (such as a laptop) to the serial port on the appliance using the serial cable provided. Using a program such as HyperTerminal, create a connection to the appliance with the following settings:

Bits per second	**"9600"**
Data Bits	**"8"**
Parity	**"None"**
Stop bits	**"1"**
Flow control	**"None"**

- Set up Terminal Emulation = VT-100
- Press the power button to start the appliance. The appliance displays the login prompt: <appliance name> login:
- Type admin, and then press ENTER.
- Type the admin password, and then press ENTER. (Obtain the default admin password from [7]).

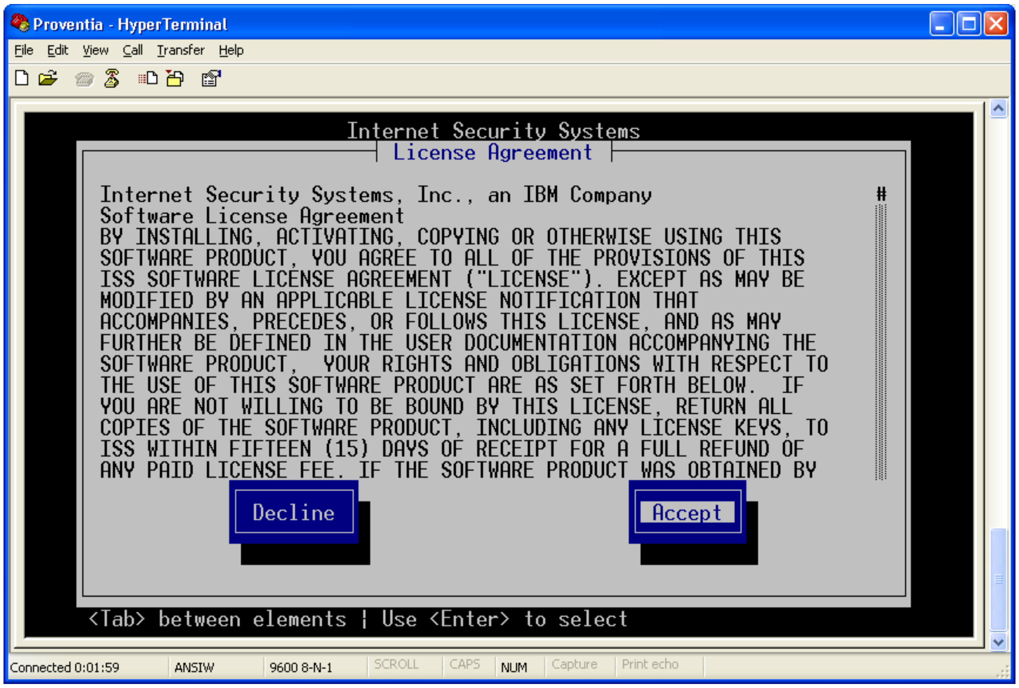
An introductory screen appears. Press **Start**, the **License Agreement** will appear.



```
                    Internet Security Systems
                       Proventia GX5208

              Proventia GX5208 Setup

                       Welcome to the
        Internet Security Systems Proventia(tm) appliance
                initial configuration utility.

      Please select 'Start' to start configuring your appliance.

                            Start
```

6.2. Accept License Agreement

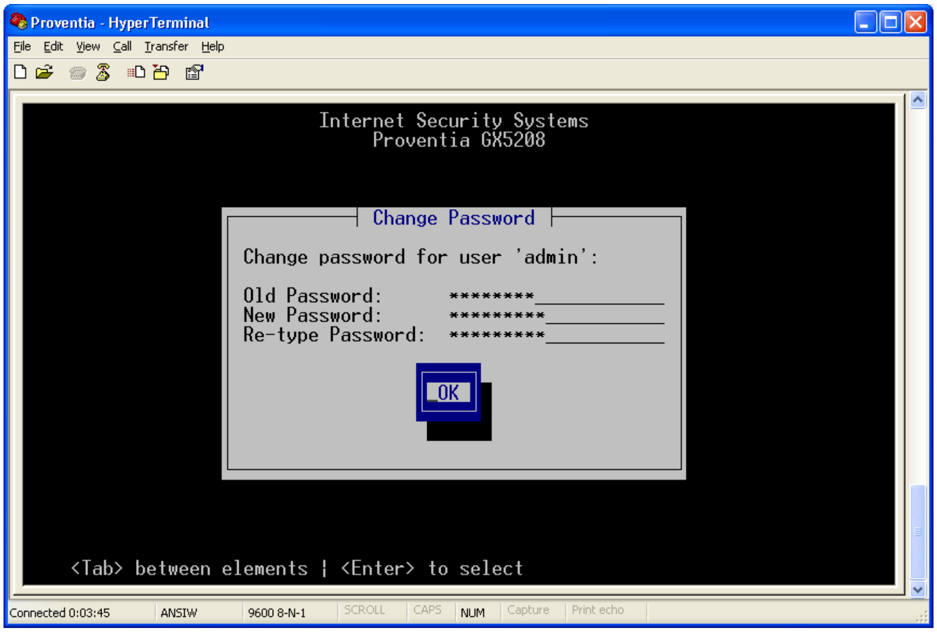
Accept License Agreement, press **Accept** to continue.



```
Internet Security Systems
License Agreement

Internet Security Systems, Inc., an IBM Company
Software License Agreement
BY INSTALLING, ACTIVATING, COPYING OR OTHERWISE USING THIS
SOFTWARE PRODUCT, YOU AGREE TO ALL OF THE PROVISIONS OF THIS
ISS SOFTWARE LICENSE AGREEMENT ("LICENSE"). EXCEPT AS MAY BE
MODIFIED BY AN APPLICABLE LICENSE NOTIFICATION THAT
ACCOMPANIES, PRECEDES, OR FOLLOWS THIS LICENSE, AND AS MAY
FURTHER BE DEFINED IN THE USER DOCUMENTATION ACCOMPANYING THE
SOFTWARE PRODUCT,  YOUR RIGHTS AND OBLIGATIONS WITH RESPECT TO
THE USE OF THIS SOFTWARE PRODUCT ARE AS SET FORTH BELOW.  IF
YOU ARE NOT WILLING TO BE BOUND BY THIS LICENSE, RETURN ALL
COPIES OF THE SOFTWARE PRODUCT, INCLUDING ANY LICENSE KEYS, TO
ISS WITHIN FIFTEEN (15) DAYS OF RECEIPT FOR A FULL REFUND OF
ANY PAID LICENSE FEE. IF THE SOFTWARE PRODUCT WAS OBTAINED BY

        Decline                          Accept

<Tab> between elements | Use <Enter> to select
```

6.3.Change default passwords on the GX5208

Change default passwords, press **OK** to continue

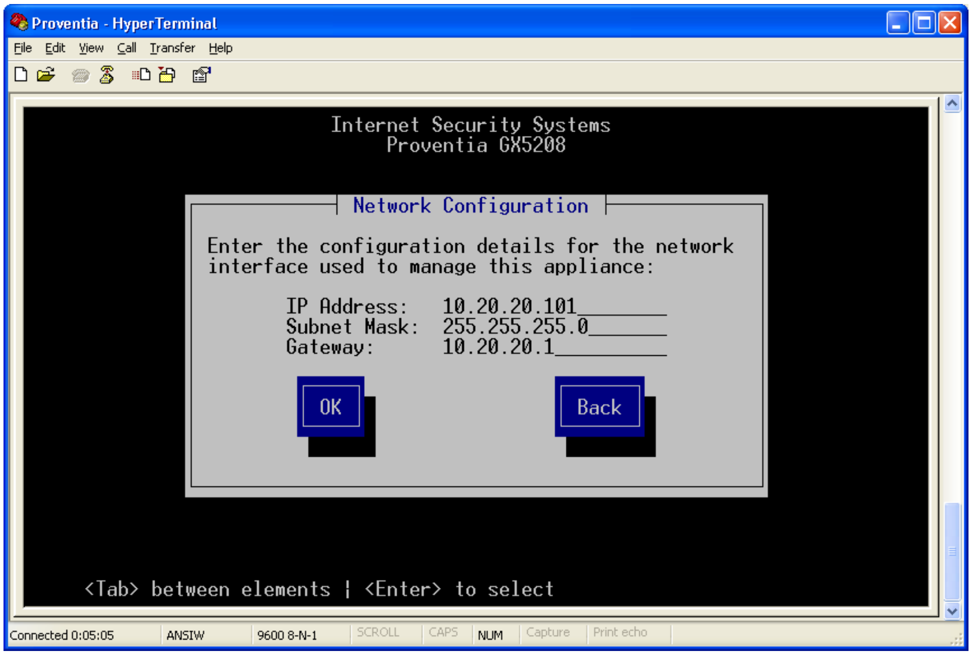


```
Internet Security Systems
  Proventia GX5208

Change Password

Change password for user 'admin':

Old Password:        ********_________
New Password:        *********________
Re-type Password:    *********________

OK

<Tab> between elements | <Enter> to select
```

6.4.Configure the Management IP address

The IP address assigned to the GX5208 must be routable so it can reach the SP1001

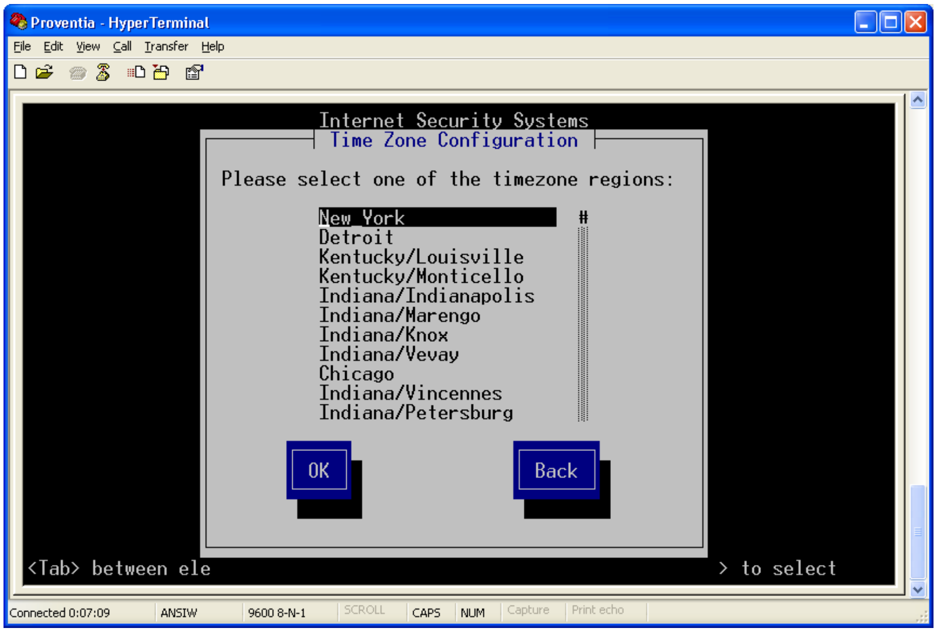
Configure the Management **IP Address, Subnet Mask** and **Gateway,** press **OK** to continue.



```
Internet Security Systems
  Proventia GX5208

Network Configuration

Enter the configuration details for the network
interface used to manage this appliance:

IP Address:    10.20.20.101_______
Subnet Mask:   255.255.255.0______
Gateway:       10.20.20.1_________

OK                    Back

<Tab> between elements | <Enter> to select
```

6.5.Set Timezone

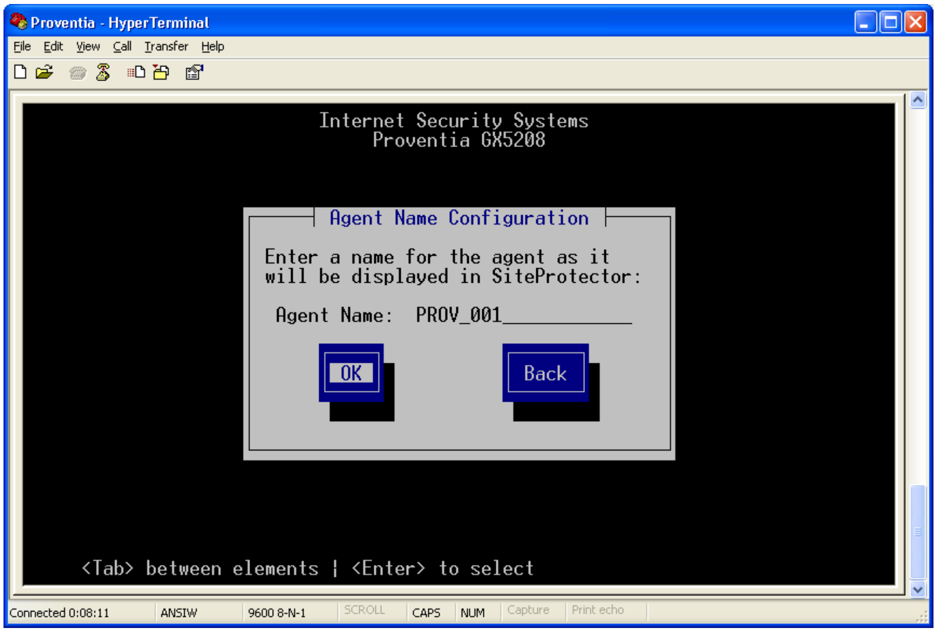
Set **timezone**, press **OK** to continue



```
                 Internet Security Systems
                  Time Zone Configuration

 Please select one of the timezone regions:

          New York                    #
          Detroit
          Kentucky/Louisville
          Kentucky/Monticello
          Indiana/Indianapolis
          Indiana/Marengo
          Indiana/Knox
          Indiana/Vevay
          Chicago
          Indiana/Vincennes
          Indiana/Petersburg

              OK              Back

<Tab> between ele                              > to select
```

6.6.Accept License Agreement

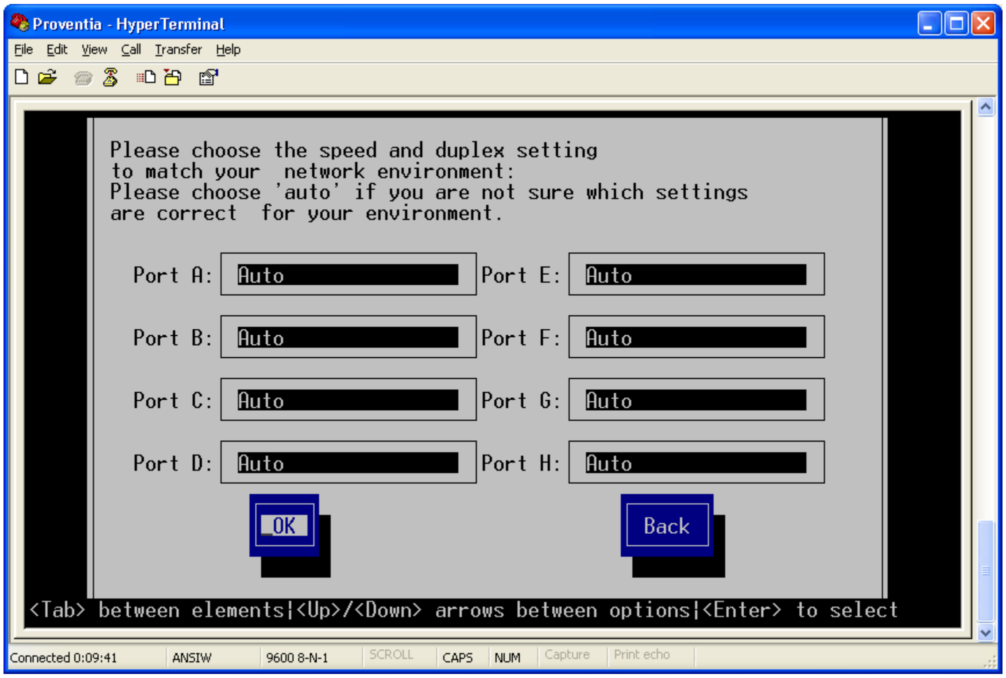
Enter unique **Agent Name** for the Proventia as it will appear in SiteProtector Management, Press **OK** to continue



```
                 Internet Security Systems
                     Proventia GX5208

                   Agent Name Configuration

               Enter a name for the agent as it
               will be displayed in SiteProtector:

                Agent Name:  PROV_001___________

                    OK            Back

     <Tab> between elements | <Enter> to select
```

6.7.Speed and Duplex settings

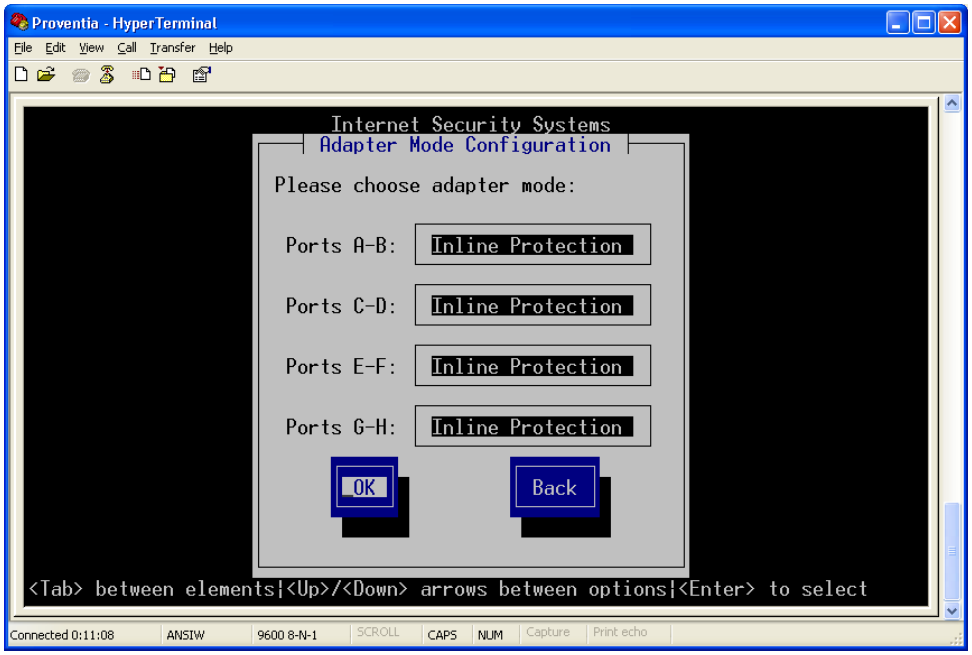
Choose **speed** and **duplex** settings for interfaces, Press **OK** to continue



```
Please choose the speed and duplex setting
 to match your  network environment:
Please choose 'auto' if you are not sure which settings
are correct  for your environment.

  Port A: Auto                Port E: Auto

  Port B: Auto                Port F: Auto

  Port C: Auto                Port G: Auto

  Port D: Auto                Port H: Auto

          OK                          Back

<Tab> between elements|<Up>/<Down> arrows between options|<Enter> to select
```

6.8. Adapter Mode Configuration

Choose **Inline Protection** for the **Ports**, Press **OK** to continue



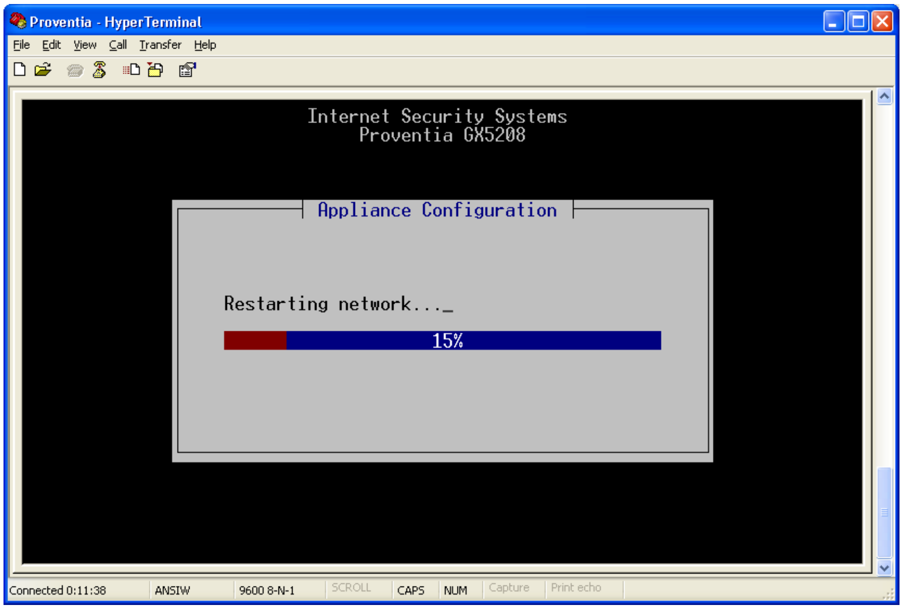
Proventia - HyperTerminal
File Edit View Call Transfer Help

```
Internet Security Systems
Adapter Mode Configuration

Please choose adapter mode:

Ports A-B:  Inline Protection
Ports C-D:  Inline Protection
Ports E-F:  Inline Protection
Ports G-H:  Inline Protection

   OK          Back

<Tab> between elements|<Up>/<Down> arrows between options|<Enter> to select
```

Connected 0:11:08 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

6.9. Re-start Appliance

Once appliance is configured it will re-start.



Proventia - HyperTerminal
File Edit View Call Transfer Help

```
Internet Security Systems
   Proventia GX5208

Appliance Configuration

Restarting network..._
15%
```

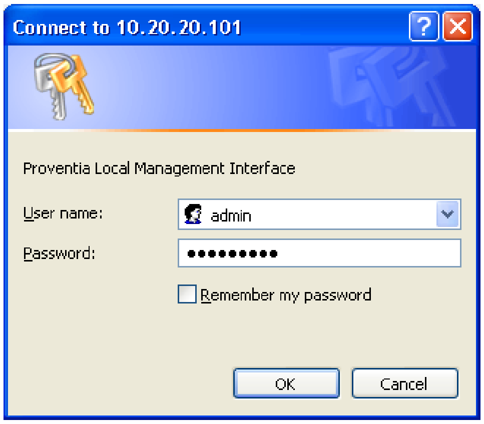
Connected 0:11:38 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

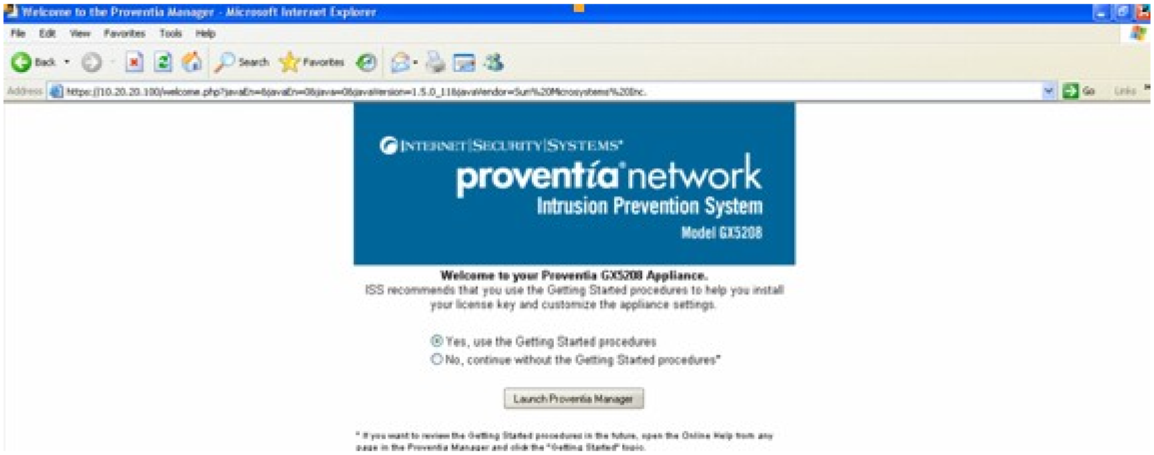
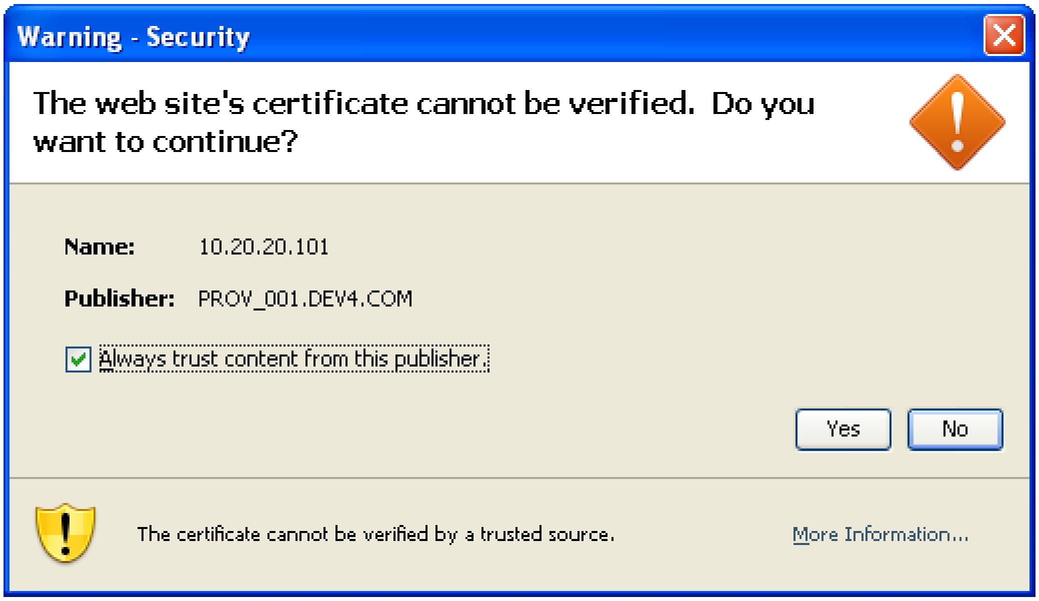
7. Configure the IBM Proventia Network IPS GX5208 Manager

Proventia Manager is the Web-based management interface for the appliance. Use Proventia Manager to monitor the appliance status, configure and manage settings, and review and manage appliance activities.

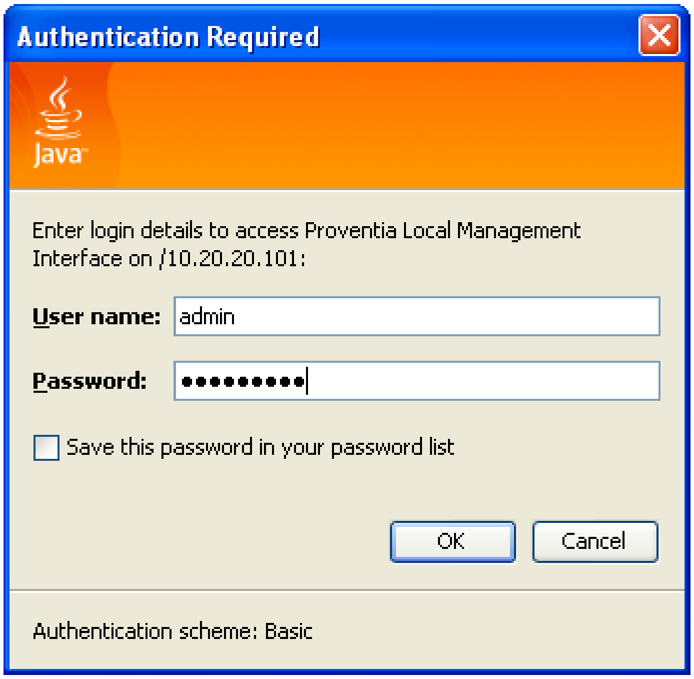
- Start Internet Explorer 6.0 or 7.0.
- Type https://XXX.XXX.XXX.XXX (where XXX.XXX.XXX.XXX is the IP address for this appliance).
- Log in using the user name "admin" and the Proventia Manager password created in section 6.3.
- If necessary, install the Java Runtime Environment (JRE).

7.1. Login to the Proventia Manager

Step	Description
1.	enter "admin" and the Proventia Manager password created in section 6.3  Connect to 10.20.20.101 Proventia Local Management Interface User name: admin Password: •••••••••• □ Remember my password

Step	Description
2.	The Welcome screen appears, select the following: • Select **Yes, use the Getting Started Procedures** • Click **Launch Proventia Manager** to continue  Welcome to your Proventia GX5208 Appliance. ISS recommends that you use the Getting Started procedures to help you install your license key and customize the appliance settings. ● Yes, use the Getting Started procedures ○ No, continue without the Getting Started procedures* * If you want to review the Getting Started procedures in the future, open the Online Help from any page in the Proventia Manager and click the "Getting Started" topic.
3.	The Warning – Security box appears , check the **Always trust content from this publisher** checkbox**,** select **Yes** to continue  The web site's certificate cannot be verified. Do you want to continue? Name: 10.20.20.101 Publisher: PROV_001.DEV4.COM ☑ Always trust content from this publisher. The certificate cannot be verified by a trusted source.

4. The **Authentication Required** box appears, enter “**admin**” and the Proventia Manager password created in section 6.3, select **OK** to continue.



Authentication Required

Enter login details to access Proventia Local Management Interface on /10.20.20.101:

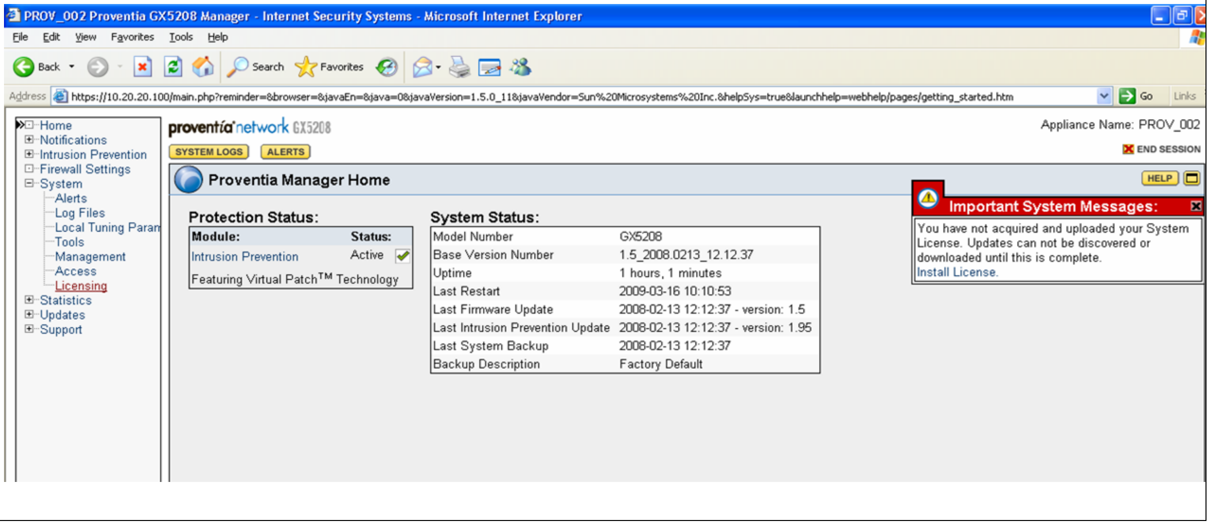
User name: admin

Password: ●●●●●●●●●

□ Save this password in your password list

Authentication scheme: Basic

5. The Main Proventia GX5208 web page will appear. The following steps refer to the Configuration Tree, which is in the left pane of the window.



PROV_002 Proventia GX5208 Manager - Internet Security Systems - Microsoft Internet Explorer

Address https://10.20.20.100/main.php?reminder=&browser=&javaEn=&java=0&javaVersion=1.5.0_11&javaVendor=Sun%20Microsystems%20Inc.&helpSys=true&launchhelp=webhelp/pages/getting_started.htm

Appliance Name: PROV_002

Proventia Manager Home

Protection Status:

Module:	Status:
Intrusion Prevention	Active ✓
Featuring Virtual Patch™ Technology	

System Status:

Model Number	GX5208
Base Version Number	1.5_2008.0213_12.12.37
Uptime	1 hours, 1 minutes
Last Restart	2009-03-16 10:10:53
Last Firmware Update	2008-02-13 12:12:37 - version: 1.5
Last Intrusion Prevention Update	2008-02-13 12:12:37 - version: 1.95
Last System Backup	2008-02-13 12:12:37
Backup Description	Factory Default

Important System Messages:

You have not acquired and uploaded your System License. Updates can not be discovered or downloaded until this is complete.
Install License.

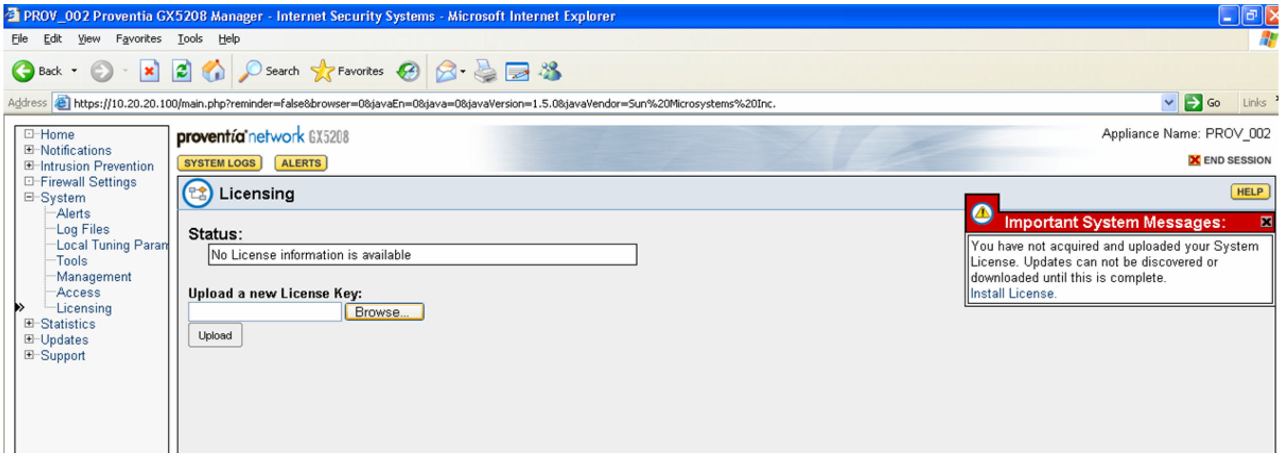
7.2. Install the Product License

Proventia Network IPS requires a properly configured license file in order to run at full capability. You must save the license file to the appropriate location so the Proventia Manager software can locate and acknowledge it.

Install the product license for the IBM Proventia Network IPS GX5208

- Register your customer license at https://www1.iss.net/wos
- You should receive login credentials. Login and download license.
- Download the license from the ISS Registration Center (note where it is downloaded).

From the Configuration Tree, click **System → Licensing**. Click the **Browse** button under **Upload a new License Key:**, Locate the license file that was downloaded, select **OK** (not shown) then click the **Upload** button.



PROV_002 Proventia GX5208 Manager - Internet Security Systems - Microsoft Internet Explorer

Address https://10.20.20.100/main.php?reminder=false&browser=0&javaEn=0&java=0&javaVersion=1.5.0&javaVendor=Sun%20Microsystems%20Inc.

Appliance Name: PROV_002

Licensing

Status:

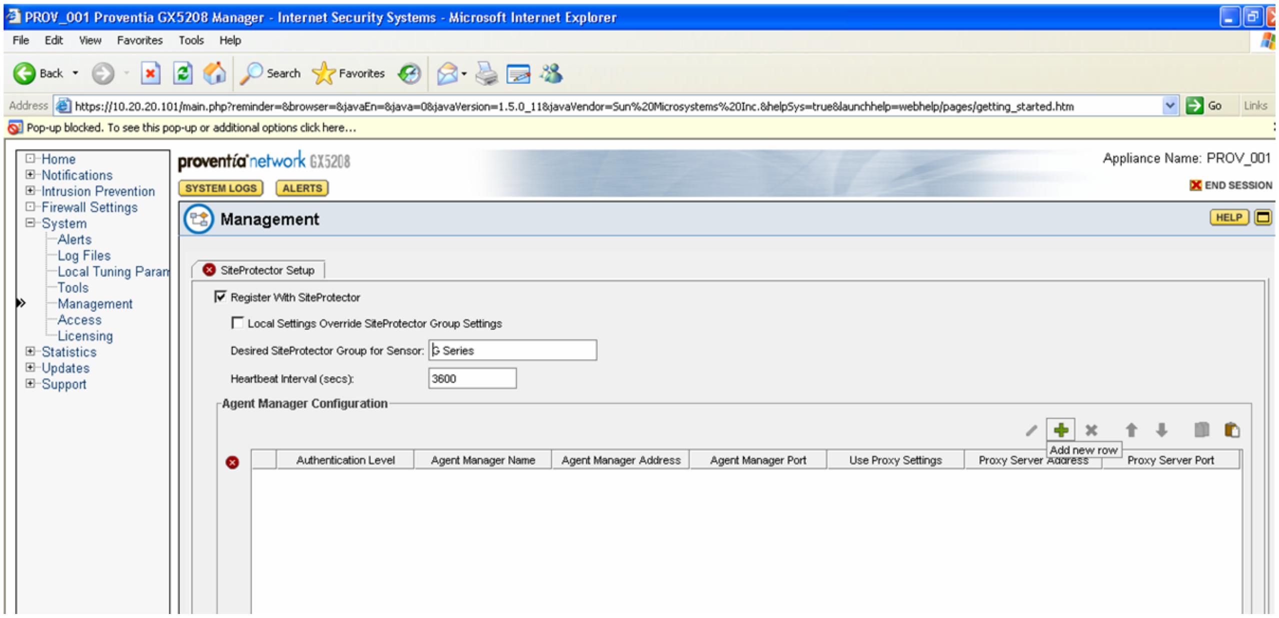
No License information is available

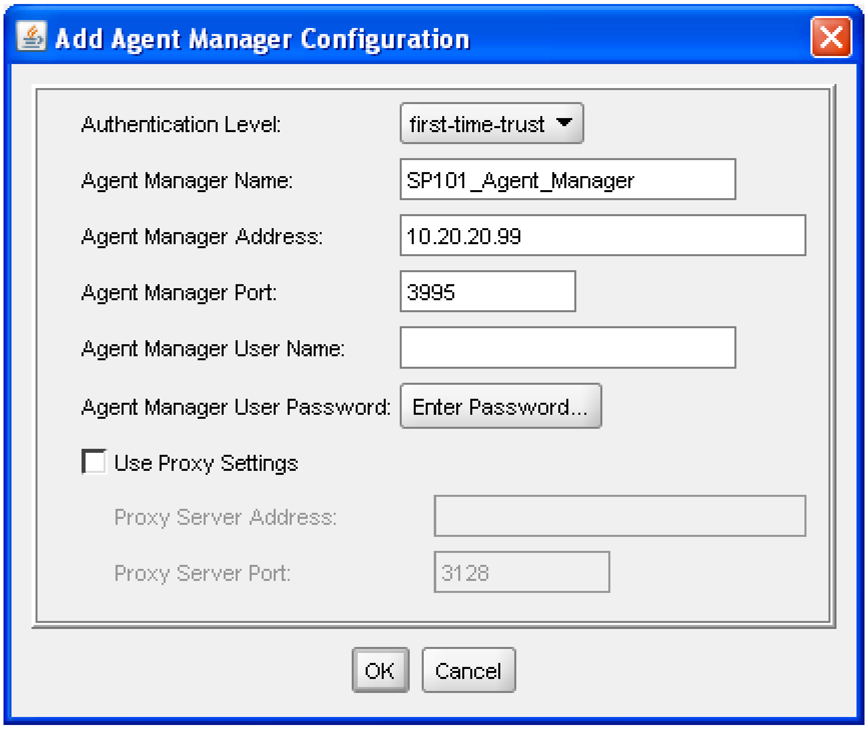
Upload a new License Key:

Important System Messages:

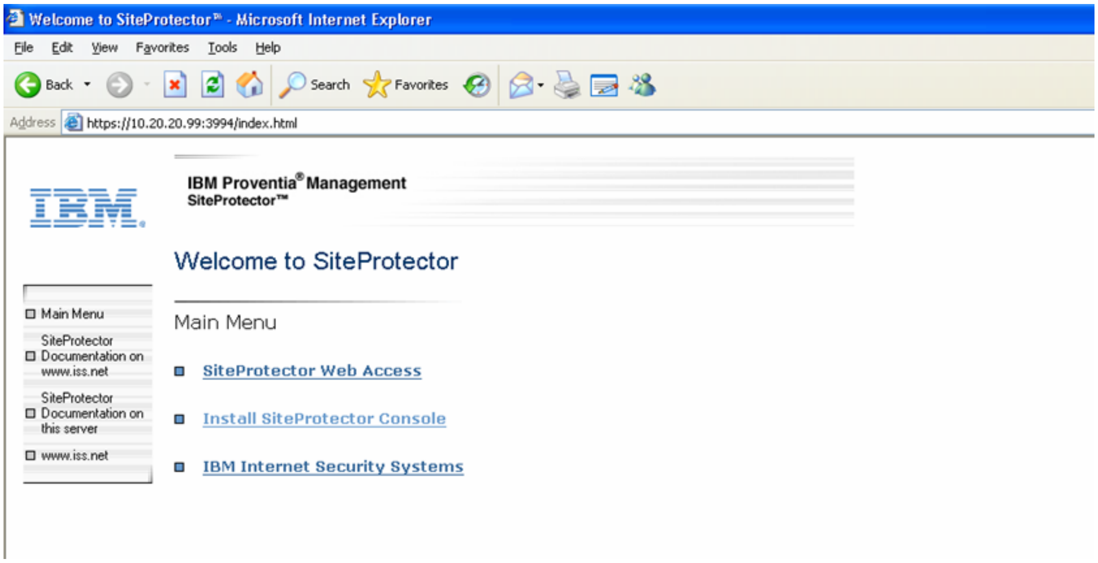
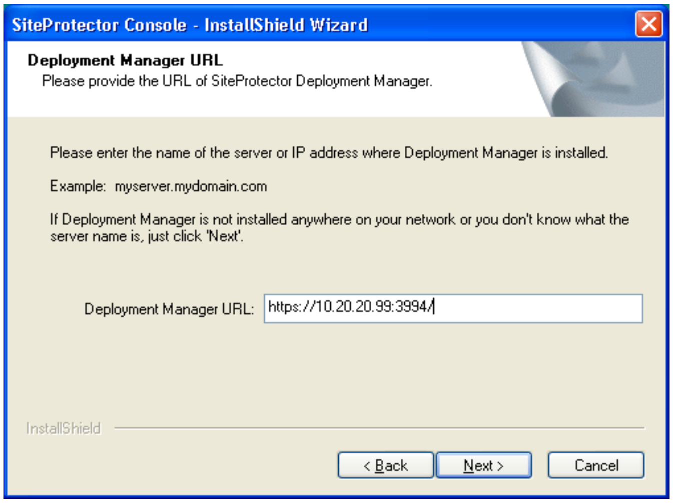
You have not acquired and uploaded your System License. Updates can not be discovered or downloaded until this is complete.
Install License.

7.3. Register Proventia IPS with SiteProtector

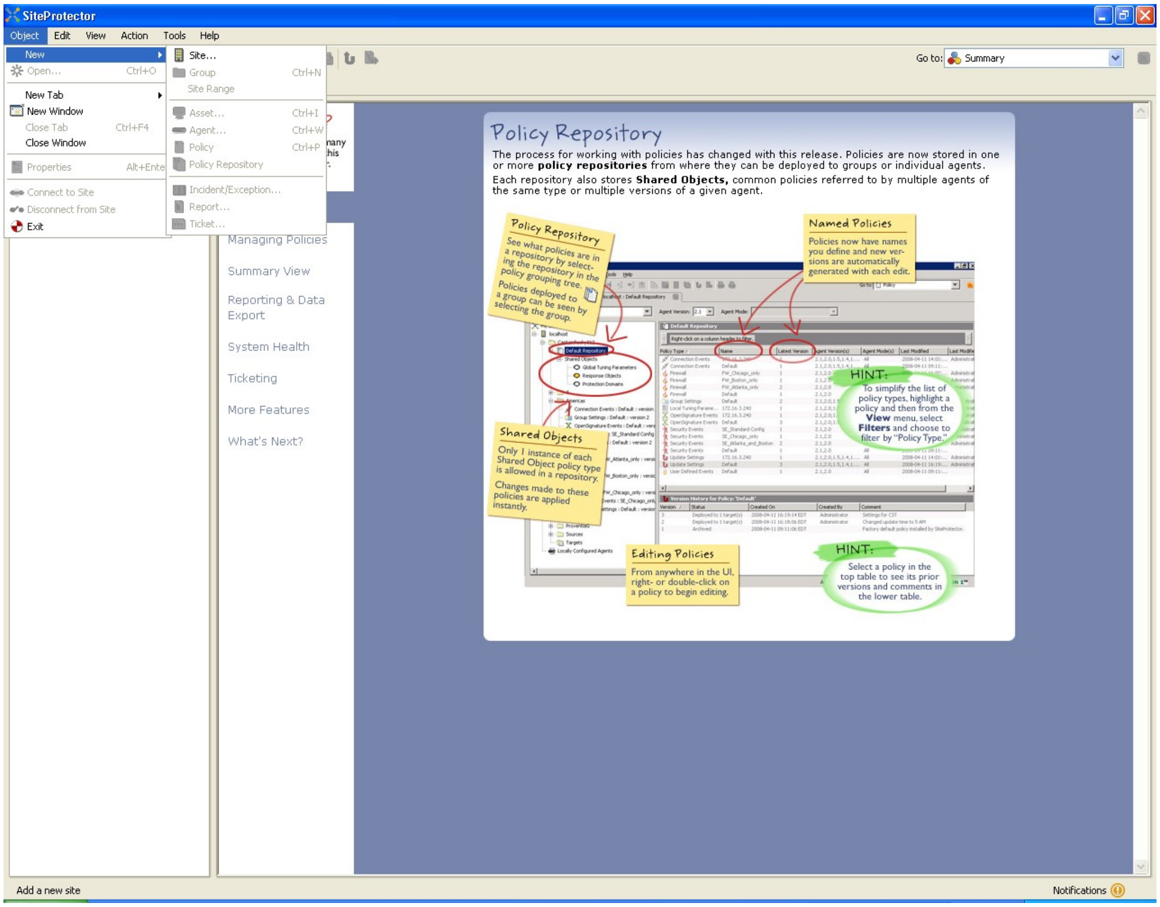
Step	Description
1.	Register the Proventia GX Series IPS Appliance for SiteProtector Management. From the Configuration Tree, click **System → Management.** In the **SiteProtector Setup** tab in the main display area**,** check the checkbox next to **Register With SiteProtector.** Enter information for the following options: - **Desired SiteProtector Group for Sensor**: ***G-Series*** - **Heartbeat Interval (secs): *3600*** Click the + icon to continue.  PROV_001 Proventia GX5208 Manager - Internet Security Systems - Microsoft Internet Explorer Address https://10.20.20.101/main.php?reminder=&browser=&javaEn=&java=0&javaVersion=1.5.0_11&javaVendor=Sun%20Microsystems%20Inc.&helpSys=true&launchhelp=webhelp/pages/getting_started.htm Pop-up blocked. To see this pop-up or additional options click here... Appliance Name: PROV_001 Management SiteProtector Setup ☑ Register With SiteProtector □ Local Settings Override SiteProtector Group Settings Desired SiteProtector Group for Sensor: G Series Heartbeat Interval (secs): 3600 Agent Manager Configuration Authentication Level | Agent Manager Name | Agent Manager Address | Agent Manager Port | Use Proxy Settings | Proxy Server Address | Proxy Server Port File Edit View Favorites Tools Help Back Search Favorites Go Links Home Notifications Intrusion Prevention Firewall Settings System Alerts Log Files Local Tuning Paran Tools Management Access Licensing Statistics Updates Support proventia network GX5208 SYSTEM LOGS ALERTS END SESSION HELP Add new row

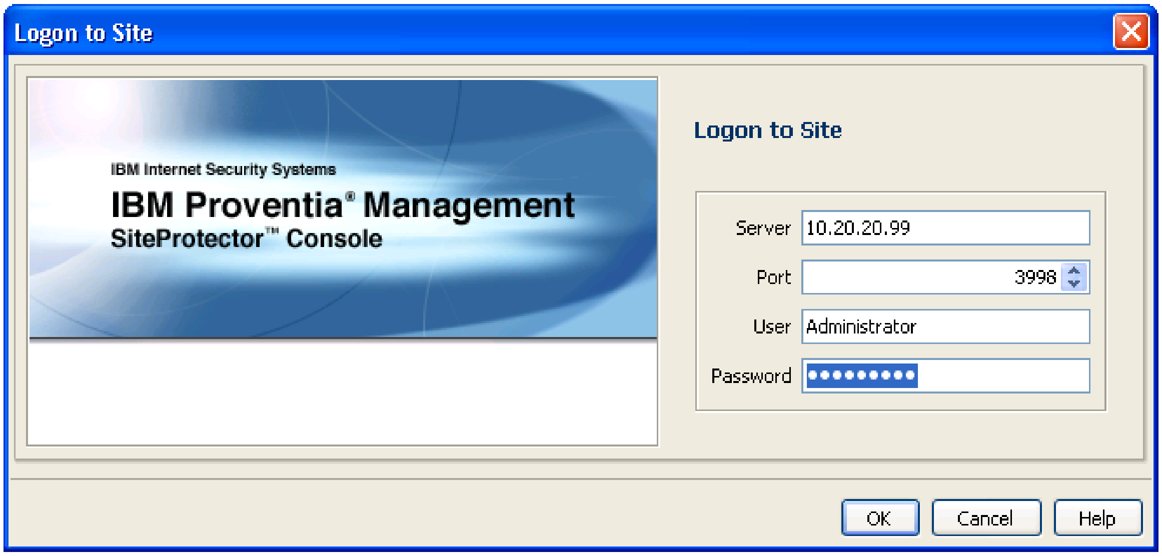
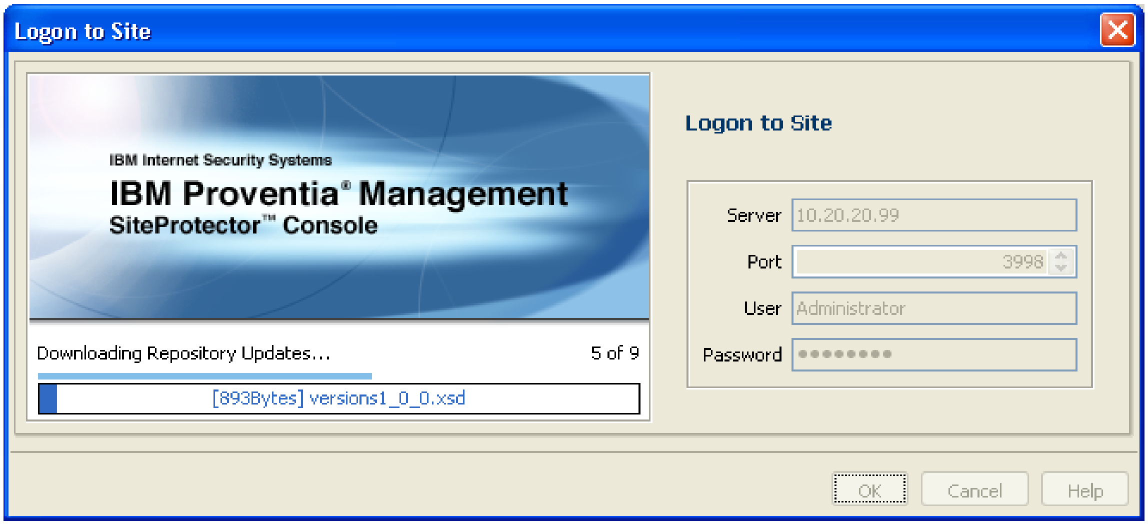
Step	Description
2.	The **Add Agent Manager Configuration** screen appears. Enter the following information: - **Agent Manager Name:** ***SP101_Agent_Manager*** - **Agent Manager Address:** ***10.20.20.99*** Select **OK** to continue  Add Agent Manager Configuration Authentication Level: first-time-trust Agent Manager Name: SP101_Agent_Manager Agent Manager Address: 10.20.20.99 Agent Manager Port: 3995 Agent Manager User Name: Agent Manager User Password: Enter Password... ☐ Use Proxy Settings Proxy Server Address: Proxy Server Port: 3128

7.4. Install SiteProtector Console

Step	Description
1.	From the PC being used to run SiteProtector, go to: https://10.20.20.99:3994 (the IP assigned to the SiteProtector) Under **Main Menu,** select **Install SiteProtector Console**.  Welcome to SiteProtector™ - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Address https://10.20.20.99:3994/index.html IBM IBM Proventia® Management SiteProtector™ Welcome to SiteProtector Main Menu SiteProtector Documentation on www.iss.net SiteProtector Documentation on this server www.iss.net Main Menu SiteProtector Web Access Install SiteProtector Console IBM Internet Security Systems
2.	Click through the installation screens (not shown). At the **Deployment Manager URL screen**, enter ***https://10.20.20.99:3994/*** in the **Deployment Manager URL** field. Select **Next** to continue.  **Deployment Manager URL** Please provide the URL of SiteProtector Deployment Manager. Please enter the name of the server or IP address where Deployment Manager is installed. Example: myserver.mydomain.com If Deployment Manager is not installed anywhere on your network or you don't know what the server name is, just click 'Next'. Deployment Manager URL: https://10.20.20.99:3994/
3.	The **InstallShield Wizard Complete** screen appears (Not Shown). Select **Finish** to continue.

7.5. Create a new site (reference the SiteProtector Server Address or Hostname).

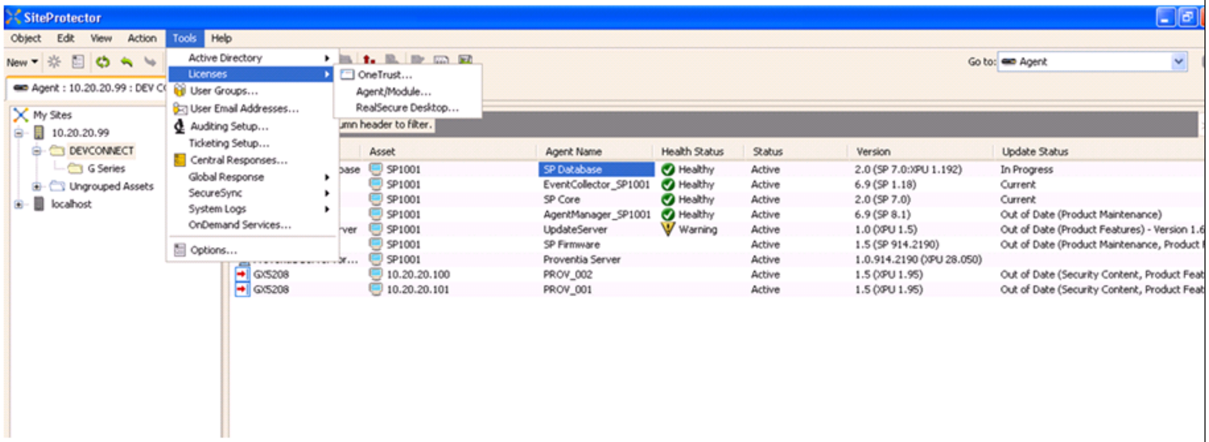
Step	Description
4.	To launch SiteProtector, from the PC, select **Start → Programs → ISS → SiteProtector → Console**. From the top menu bar on **SiteProtector** select **Object → New → Site**. Note: DEVCONNECT was used as the site name for testing.  Policy Repository The process for working with policies has changed with this release. Policies are now stored in one or more **policy repositories** from where they can be deployed to groups or individual agents. Each repository also stores **Shared Objects,** common policies referred to by multiple agents of the same type or multiple versions of a given agent. Policy Repository: See what policies are in a repository by selecting the repository in the policy grouping tree. Policies deployed to a group can be seen by selecting the group. Named Policies: Policies now have names you define and new versions are automatically generated with each edit. Shared Objects: Only 1 instance of each Shared Object policy type is allowed in a repository. Changes made to these policies are applied instantly. Editing Policies: From anywhere in the UI, right- or double-click on a policy to begin editing. HINT: To simplify the list of policy types, highlight a policy and then from the **View** menu, select **Filters** and choose to filter by "Policy Type." HINT: Select a policy in the top table to see its prior versions and comments in the lower table. SiteProtector Object Edit View Action Tools Help New Open... Ctrl+O New Tab New Window Close Tab Ctrl+F4 Close Window Properties Alt+Ente Connect to Site Disconnect from Site Exit Site... Group Ctrl+N Site Range Asset... Ctrl+I Agent... Ctrl+W Policy Ctrl+P Policy Repository Incident/Exception... Report... Ticket... Go to: Summary Managing Policies Summary View Reporting & Data Export System Health Ticketing More Features What's Next? Add a new site Notifications

Step	Description
5.	The **Logon to Site** screen will appear, Enter the following: - **Server – 10.20.20.99** - **Port – 3998** - **User – Administrator** - **Password –** Use the password created in section 6.3 Press **OK** to continue.  Logon to Site IBM Internet Security Systems IBM Proventia® Management SiteProtector™ Console Logon to Site Server 10.20.20.99 Port 3998 User Administrator Password ●●●●●●●●●
6.	Wait for the SiteProtector to complete synchronizing and downloading the repository updates. Press **OK** to continue.  Logon to Site IBM Internet Security Systems IBM Proventia® Management SiteProtector™ Console Downloading Repository Updates... 5 of 9 [893Bytes] versions1_0_0.xsd Logon to Site Server 10.20.20.99 Port 3998 User Administrator Password ●●●●●●●●

7.6. Install All Applicable licensing.

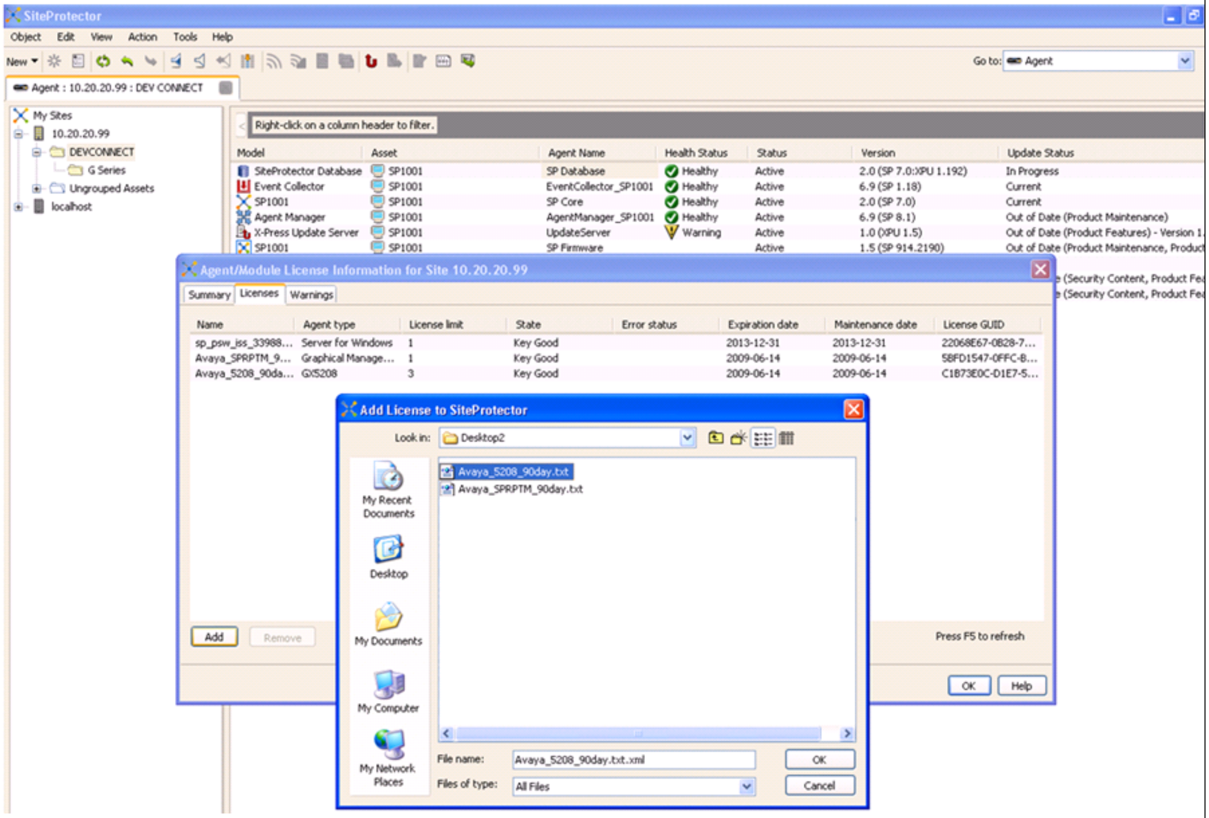
Obtain all licenses and registration instructions form an IBM Proventia fulfillment representative or visit https://www1.iss.net/wos. Refer to **section 1.2** for support information.

1. From the top menu bar on **SiteProtector** select **Tools → Licenses → Add License**



	Asset	Agent Name	Health Status	Status	Version	Update Status
base	SP1001	SP Database	Healthy	Active	2.0 (SP 7.0:XPU 1.192)	In Progress
	SP1001	EventCollector_SP1001	Healthy	Active	6.9 (SP 1.18)	Current
	SP1001	SP Core	Healthy	Active	2.0 (SP 7.0)	Current
	SP1001	AgentManager_SP1001	Healthy	Active	6.9 (SP 8.1)	Out of Date (Product Maintenance)
rver	SP1001	UpdateServer	Warning	Active	1.0 (XPU 1.5)	Out of Date (Product Features) - Version 1.6
	SP1001	SP Firmware		Active	1.5 (SP 914.2190)	Out of Date (Product Maintenance, Product F
r...	SP1001	Proventia Server		Active	1.0.914.2190 (XPU 28.050)	
GX5208	10.20.20.100	PROV_002		Active	1.5 (XPU 1.95)	Out of Date (Security Content, Product Feat
GX5208	10.20.20.101	PROV_001		Active	1.5 (XPU 1.95)	Out of Date (Security Content, Product Feat

2. The **Agent/Module License Information** box will appear. Select the **License** tab, click the **Import** tab, (not shown), find the License file obtained from the IBM Proventia Representative, click **OK** to continue.



Model	Asset	Agent Name	Health Status	Status	Version	Update Status
SiteProtector Database	SP1001	SP Database	Healthy	Active	2.0 (SP 7.0:XPU 1.192)	In Progress
Event Collector	SP1001	EventCollector_SP1001	Healthy	Active	6.9 (SP 1.18)	Current
SP1001	SP1001	SP Core	Healthy	Active	2.0 (SP 7.0)	Current
Agent Manager	SP1001	AgentManager_SP1001	Healthy	Active	6.9 (SP 8.1)	Out of Date (Product Maintenance)
X-Press Update Server	SP1001	UpdateServer	Warning	Active	1.0 (XPU 1.5)	Out of Date (Product Features) - Version 1.
SP1001	SP1001	SP Firmware		Active	1.5 (SP 914.2190)	Out of Date (Product Maintenance, Product
						e (Security Content, Product Fe
						e (Security Content, Product Fe

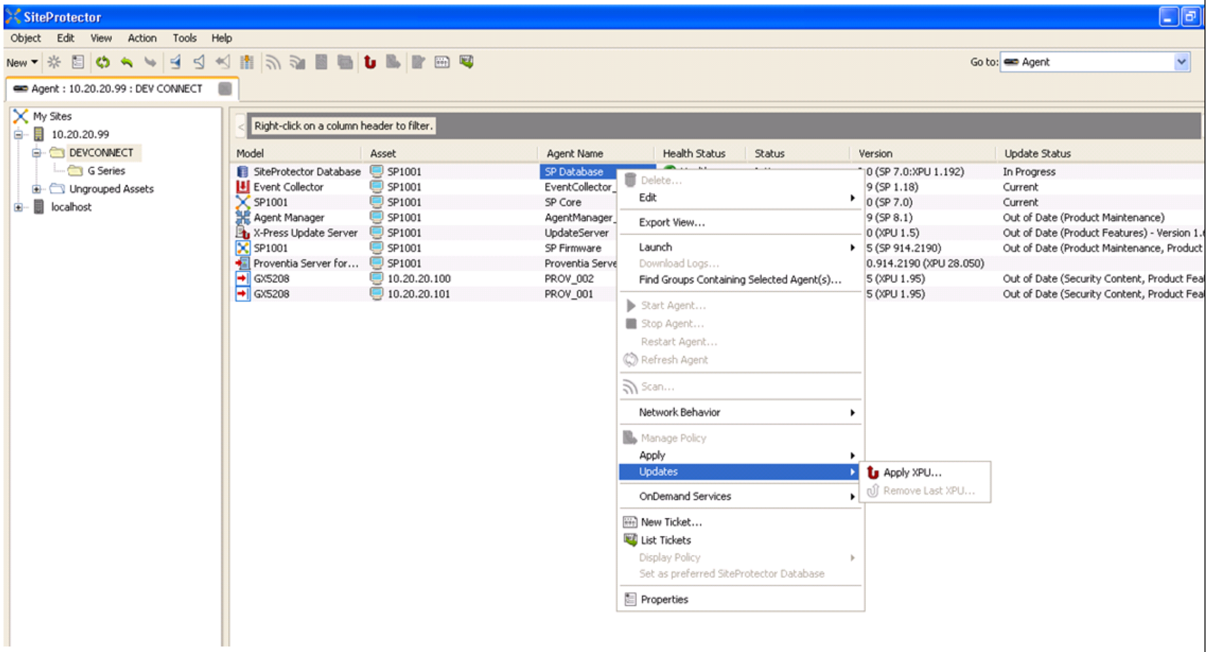
Name	Agent type	License limit	State	Error status	Expiration date	Maintenance date	License GUID
sp_psw_iss_33988...	Server for Windows	1	Key Good		2013-12-31	2013-12-31	22068E67-0B28-7...
Avaya_SPRPTM_9...	Graphical Manage...	1	Key Good		2009-06-14	2009-06-14	5BFD1547-0FFC-B...
Avaya_5208_90da...	GX5208	3	Key Good		2009-06-14	2009-06-14	C1B73E0C-D1E7-5...

File name: Avaya_5208_90day.txt.xml

Files of type: All Files

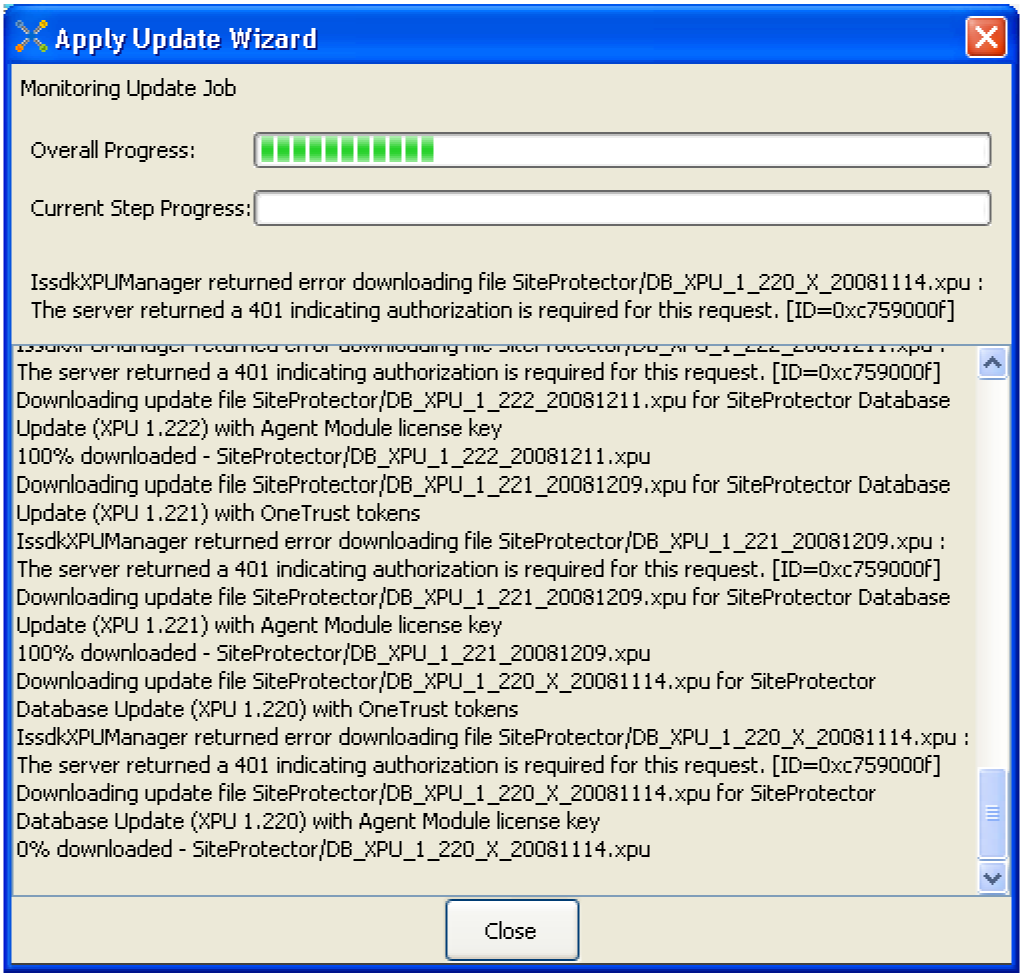
7.7. Applying Initial Updates

1. From the left navigation tree of the SiteProtector window, select **DEVCONNET**, right click on the **Agent Name** that is **Out of Date**, click on **Updates** → Apply **XPU**.



Model	Asset	Agent Name	Health Status	Status	Version	Update Status
SiteProtector Database	SP1001	SP Database			0 (SP 7.0:XPU 1.192)	In Progress
Event Collector	SP1001	EventCollector_			9 (SP 1.18)	Current
SP1001	SP1001	SP Core			0 (SP 7.0)	Current
Agent Manager	SP1001	AgentManager_			9 (SP 8.1)	Out of Date (Product Maintenance)
X-Press Update Server	SP1001	UpdateServer			0 (XPU 1.5)	Out of Date (Product Features) - Version 1.
SP1001	SP1001	SP Firmware			5 (SP 914.2190)	Out of Date (Product Maintenance, Product
Proventia Server for...	SP1001	Proventia Serve			0.914.2190 (XPU 28.050)	
GX5208	10.20.20.100	PROV_002			5 (XPU 1.95)	Out of Date (Security Content, Product Fea
GX5208	10.20.20.101	PROV_001			5 (XPU 1.95)	Out of Date (Security Content, Product Fea

2. The **Apply Updates Wizard** will appear and will start applying all necessary updates:



Monitoring Update Job

Overall Progress:

Current Step Progress:

IssdkXPUManager returned error downloading file SiteProtector/DB_XPU_1_220_X_20081114.xpu : The server returned a 401 indicating authorization is required for this request. [ID=0xc759000f]

```
IssdkXPUManager returned error downloading file SiteProtector/DB_XPU_1_222_20081211.xpu :
The server returned a 401 indicating authorization is required for this request. [ID=0xc759000f]
Downloading update file SiteProtector/DB_XPU_1_222_20081211.xpu for SiteProtector Database
Update (XPU 1.222) with Agent Module license key
100% downloaded - SiteProtector/DB_XPU_1_222_20081211.xpu
Downloading update file SiteProtector/DB_XPU_1_221_20081209.xpu for SiteProtector Database
Update (XPU 1.221) with OneTrust tokens
IssdkXPUManager returned error downloading file SiteProtector/DB_XPU_1_221_20081209.xpu :
The server returned a 401 indicating authorization is required for this request. [ID=0xc759000f]
Downloading update file SiteProtector/DB_XPU_1_221_20081209.xpu for SiteProtector Database
Update (XPU 1.221) with Agent Module license key
100% downloaded - SiteProtector/DB_XPU_1_221_20081209.xpu
Downloading update file SiteProtector/DB_XPU_1_220_X_20081114.xpu for SiteProtector
Database Update (XPU 1.220) with OneTrust tokens
IssdkXPUManager returned error downloading file SiteProtector/DB_XPU_1_220_X_20081114.xpu :
The server returned a 401 indicating authorization is required for this request. [ID=0xc759000f]
Downloading update file SiteProtector/DB_XPU_1_220_X_20081114.xpu for SiteProtector
Database Update (XPU 1.220) with Agent Module license key
0% downloaded - SiteProtector/DB_XPU_1_220_X_20081114.xpu
```

7.8. Tuning and Customization

To maximize the resources available and mimic the "real world" deployment, IBM ISS recommends evaluating tuning and customization of the Proventia GX appliance through the Proventia Management SiteProtector.

7.8.1. Recommended Policies

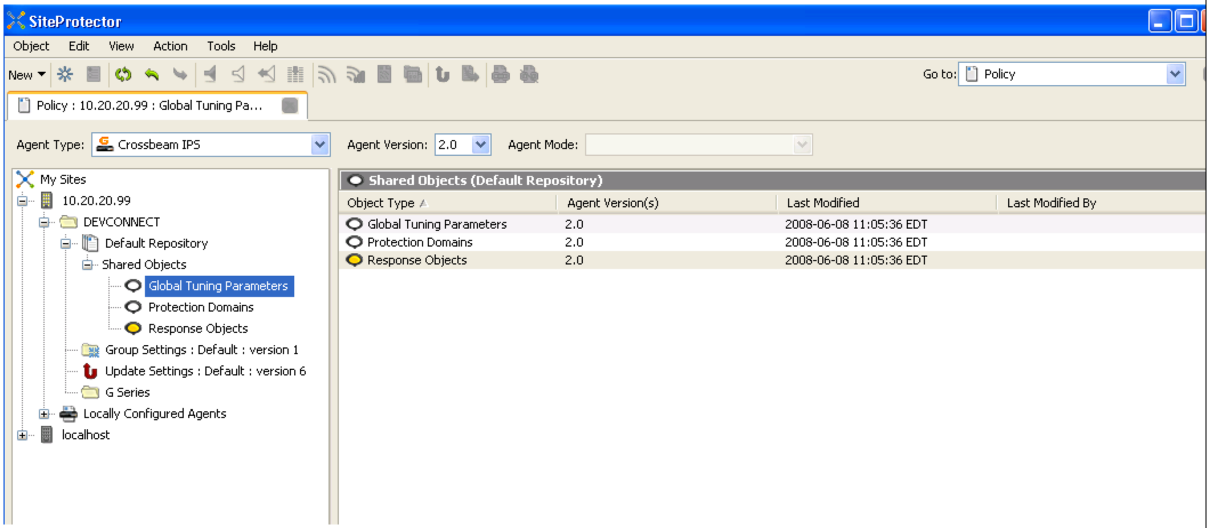
The IPS must be offered as a pre-configured appliance and operate effectively using an "out-of-the-box" configuration and must adequately protect its environment with minimal tuning. The default blocking policy should protect against known hybrid threats and future worm propagations without requiring advanced knowledge of configuration options.

Default policies are comprised of all X-Force recommended responses for each type of attack, which requires minimal configuration or expertise from the user. Additional tuning can be done in the “in-line simulation” mode, which allows for response visibility without blocking network traffic.

7.8.2. Install the Trust X-Force Policy

The Trust X-Force Policy was used for compliance testing.

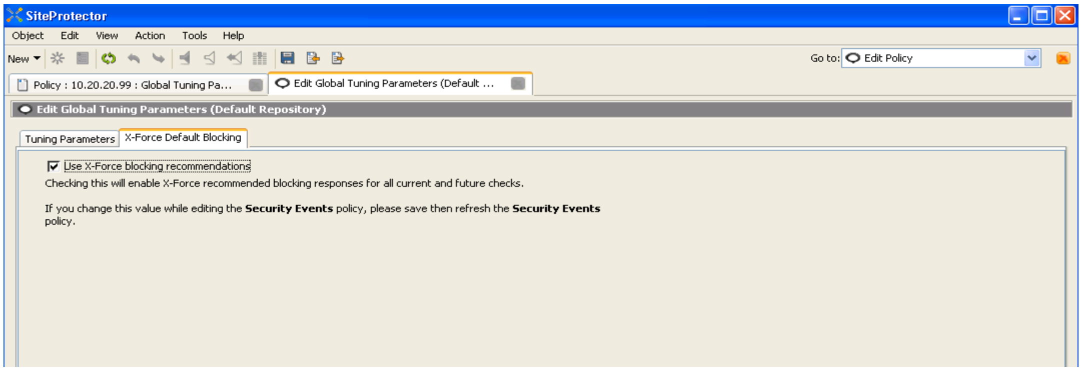
1. From the left navigation tree on **SiteProtector** select **View → DEVCONNECT → Default Repository → Shared Object,** double click on **Global Tuning Parameters** to continue.


SiteProtector
Object Edit View Action Tools Help
New
Go to: Policy
Policy : 10.20.20.99 : Global Tuning Pa...
Agent Type: Crossbeam IPS
Agent Version: 2.0
Agent Mode:
My Sites
10.20.20.99
DEVCONNECT
Default Repository
Shared Objects
Global Tuning Parameters
Protection Domains
Response Objects
Group Settings : Default : version 1
Update Settings : Default : version 6
G Series
Locally Configured Agents
localhost

Shared Objects (Default Repository)

Object Type	Agent Version(s)	Last Modified	Last Modified By
Global Tuning Parameters	2.0	2008-06-08 11:05:36 EDT	
Protection Domains	2.0	2008-06-08 11:05:36 EDT	
Response Objects	2.0	2008-06-08 11:05:36 EDT	

2. The **Edit Global Tuning Parameters (Default Repository)** box will appear**.** Select the **X-Force Default Blocking** tab and check the **Use X-Force blocking recommendation** check box**.** From the top menu bar on **SiteProtector** select **Action → Save Policy** to continue.

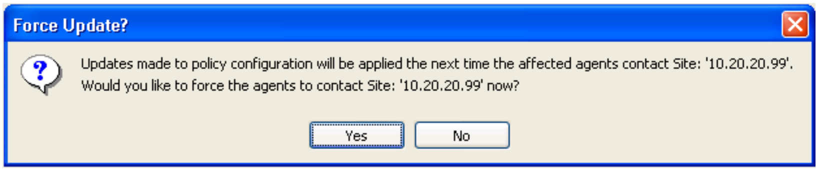

SiteProtector
Object Edit View Action Tools Help
New
Go to: Edit Policy
Policy : 10.20.20.99 : Global Tuning Pa...
Edit Global Tuning Parameters (Default ...
Edit Global Tuning Parameters (Default Repository)
Tuning Parameters
X-Force Default Blocking

☑ Use X-Force blocking recommendations

Checking this will enable X-Force recommended blocking responses for all current and future checks.

If you change this value while editing the **Security Events** policy, please save then refresh the **Security Events** policy.

3. The **Force Update?** Box will appear, select **Yes** to continue.



Updates made to policy configuration will be applied the next time the affected agents contact Site: '10.20.20.99'. Would you like to force the agents to contact Site: '10.20.20.99' now?

7.8.3. Updating Protection

The IPS must support current vulnerability and threat information and possess online help that describes each event, affected platforms, corrective action, and active hyperlinks with additional details. Security content updates should support both manual and automated mechanisms and be available at regular intervals and also in an immediate fashion when late-breaking threat emergencies occur. Updates should not require physical access to the appliance.

In the Proventia Network IPS appliances, there are two ways to apply X-Press Updates (both security and firmware updates) to the appliance:

- Right-click the group or appliance and select Update > Apply XPU.
- Configure the Update Settings policy and apply the policy to the appliance

The timing and frequency of updates can be changed by adjusting the options on the Update Settings tab.

8. General Test Approach and Test Results

8.1. Test Approach

All feature functionality test cases were performed manually. The general test approach entailed verifying the following list while attacks were being blocked by the IBM Proventia System:

- LAN/WAN connectivity between all locations
- Registration of Avaya H.323 and SIP IP telephones in Remote Site A with Corporate HQ Avaya Communication Manager
- Registration of Avaya Communication Manager in Remote Site C with Corporate HQ Avaya Communication Manager
- Registration of Avaya SIP IP telephones with Avaya SIP Enablement Services
- Verification of the DHCP relay configuration
- Inter-office calls using G.711 mu-law & G.729 codecs
- Verifying that DSCP and 802.1p Priority QoS values are not altered by the IBM Proventia Network Intrusion Prevention System.
- Verifying that Avaya Modular Messaging voicemail and MWI work properly.
- Verifying that Avaya IA 770 INTUITY AUDIX voicemail and MWI work properly.
- Retrieving Voicemail messages from Remote locations
- Features Tested: attended/unattended transfer, conference call participation, conference call add/drop, multiple call appearances, caller ID operation, call forwarding unconditional, call forwarding on busy, call park, call pick-up, bridged call appearances

8.2. Test Results

All feature functionality, serviceability, and performance test cases passed. VoIP traffic and voice features worked properly while service attacks were being blocked by the IBM Proventia Network Intrusion Prevention System.

9. Verification Steps

While the IBM Proventia Network Intrusion Prevention System is in place, the general verification steps include:

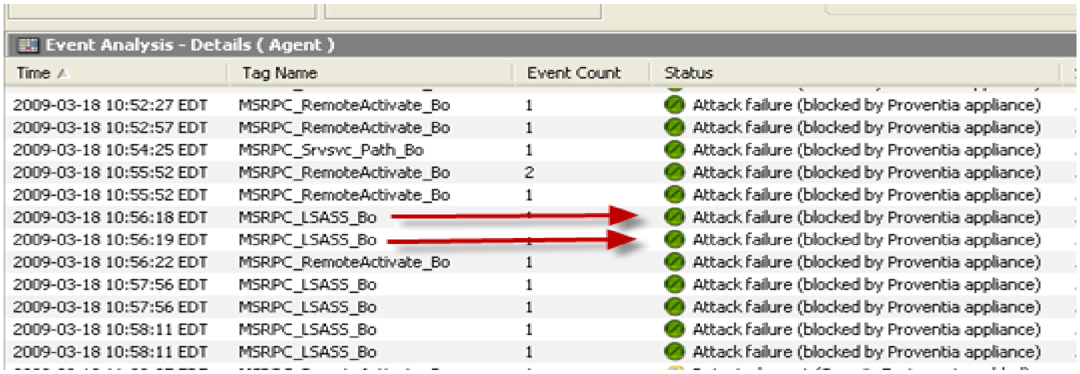
1. Verifying the DHCP relay through the network is functioning by confirming that the Avaya IP telephones receive their IP addresses from the DHCP server connected to the Brocade FastIron SuperX Switch.

2. Check that the Avaya H.323 IP telephones have successfully registered with Avaya Communication Manager using the **list registered-station** command.

3. Check that the Avaya SIP IP telephones have successfully registered with Avaya SIP Enablement Services (SES) listng the Registered Users on the SES administrative GUI.

4. Place internal and external calls between the digital telephone and IP telephones at each site.

5. Verified attacks were being blocked using the SiteProtector interface.



Event Analysis - Details (Agent)

Time	Tag Name	Event Count	Status
2009-03-18 10:52:27 EDT	MSRPC_RemoteActivate_Bo	1	✓ Attack failure (blocked by Proventia appliance)
2009-03-18 10:52:57 EDT	MSRPC_RemoteActivate_Bo	1	✓ Attack failure (blocked by Proventia appliance)
2009-03-18 10:54:25 EDT	MSRPC_Srvsvc_Path_Bo	1	✓ Attack failure (blocked by Proventia appliance)
2009-03-18 10:55:52 EDT	MSRPC_RemoteActivate_Bo	2	✓ Attack failure (blocked by Proventia appliance)
2009-03-18 10:55:52 EDT	MSRPC_RemoteActivate_Bo	1	✓ Attack failure (blocked by Proventia appliance)
2009-03-18 10:56:18 EDT	MSRPC_LSASS_Bo	1	✓ Attack failure (blocked by Proventia appliance)
2009-03-18 10:56:19 EDT	MSRPC_LSASS_Bo	1	✓ Attack failure (blocked by Proventia appliance)
2009-03-18 10:56:22 EDT	MSRPC_RemoteActivate_Bo	1	✓ Attack failure (blocked by Proventia appliance)
2009-03-18 10:57:56 EDT	MSRPC_LSASS_Bo	1	✓ Attack failure (blocked by Proventia appliance)
2009-03-18 10:57:56 EDT	MSRPC_LSASS_Bo	1	✓ Attack failure (blocked by Proventia appliance)
2009-03-18 10:58:11 EDT	MSRPC_LSASS_Bo	1	✓ Attack failure (blocked by Proventia appliance)
2009-03-18 10:58:11 EDT	MSRPC_LSASS_Bo	1	✓ Attack failure (blocked by Proventia appliance)

10. Conclusion

These Application Notes describe the configuration steps for integrating IBM Proventia Network Intrusion Prevention System with an Avaya telephony infrastructure. For the configuration described in these Application Notes, the IBM Proventia Network Intrusion Prevention System was responsible for monitoring and blocking security threats before they impact endpoints throughout the network.

11. Additional References

The documents referenced below were used for additional support and configuration information.

The following Avaya product documentation can be found at http://support.avaya.com.

[1] *Administrator Guide for Avaya Communication Manager, Document Number* 03-300509.

[2] *Installing, Administering, Maintaining, and Troubleshooting SIP Enablement Services*, *Release June 2008*, Issue 6.0, Document Number 03-600768

[3] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 2.0,* Document Number 16-300698.

[4] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Installation and Maintenance Guide Release 2.0,* Document Number 16-601943.

[5] *Modular Messaging Release 3.1Messaging Application Server Administration Guide for Avaya Modular Messaging with the Avaya MAS and MSS,* February 2007.

[6] *Avaya IA 770 INTUITY AUDIX Messaging Application Release* 5.0 Administering Communication Manager Servers to Work with IA 770, January 2008.

The IBM product documentation can be found at

[7] http://www.iss.net/support/documentation/index.php

The Brocade product documentation can be found at http://www.Brocadenet.com/.

[8] *Brocade FastIron Configuration Guide* with sections as follows:

- *FastIron X Series Chassis*
  - *FastIron SuperX*
- *FastIron Layer 2 Compact Switches*
  - *FastIron GS*

12. Change History

Issue	**Date**	**Reason**
1.0	5/07/2009	Initial issue
1.1	6/16/2009	Updated Figure 1 and text in Sections 2.3 & 2.4

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.