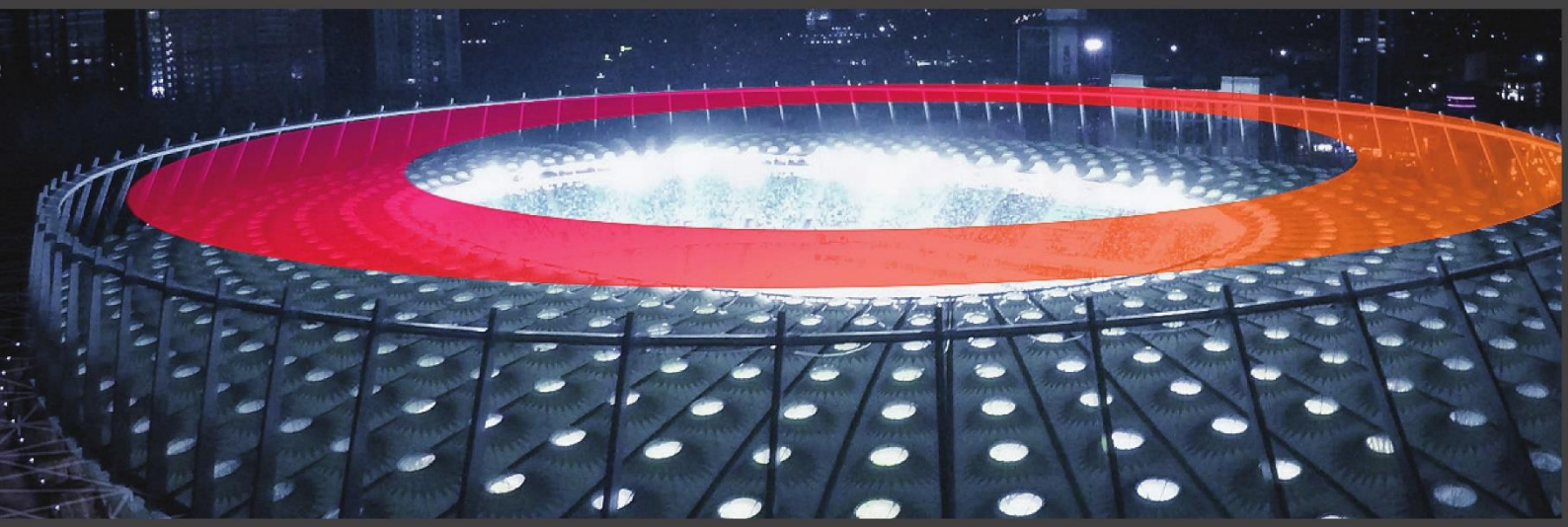
allot
See. Control. Secure.



Application Control Gateway

ACG2000 (16.5.510)
User Guide

See. Control. Secure.

Contents

1 Introducing the Application Control Gateway

1.1 Overview

Whether you are a small business with no IT expertise, a growing mid-size business, or running a big enterprise with distributed branches and offices – intelligent insight and control of your applications and user behavior is fundamental for your business success and reputation.

The Allot Application Control Gateway (ACG) is the next generation in application and network management. It is a powerful platform that unifies advanced management, ML & AI analytics capabilities, and network control capabilities based on Allot Dynamic Actionable Recognition Technology (DART).

The ACG enables you to control application performance to meet your business priorities, with a low TCO. It is designed to be installed in either the heart of a small business network, or deployed at network edge points for larger enterprises.

With an intuitive UI and built-in management capabilities, it lets you save your IT resources and quickly and easily configure policies to ensure business-critical applications receive top priority.

1.2 The Modules

The ACG is comprised of six Modules which together give you the tools to see, control, and secure your network traffic.

- Service Gateway Virtual Edition (SG-VE)
- NetXplorer (NX)
- Data Mediator (DM)
- Subscriber Management Platform (SMP)
- ClearSee (CS)
- DDoS Secure Controller (DSC)

1.2.1 Service Gateway Virtual Edition (SG-VE)

Allot Service Gateway Virtual Edition (SG-VE) is designed to provide Allot's renowned Service Gateway functionality in a discrete virtual deployment environment. It is equipped with the same rich features and functions as the other Allot Service Gateway platforms, enabling the roll out of Security as a Service as

well as other revenue-generating services rapidly and cost effectively, while lowering the total cost of ownership and accelerating ROI.

1.2.2 NetXplorer (NX)

Allot NetXplorer provides centralized visibility that is accessible to multiple clients and designed to manage a globally dispersed network infrastructure. One GUI provides centralized control of key Allot solution elements, including Service Gateways, Subscriber Management Platform (SMP), Data Mediator, and ClearSee. Allot NetXplorer server is accessible from multiple clients concurrently – facilitating user identity management and authentication.

1.2.3 Data Mediator (DM)

The Data Mediator is an auxiliary mediation element that collects data records from the Service Gateway and SMP and prepares them for upload to ClearSee.

1.2.4 Subscriber Management Platform (SMP)

Allot's solution utilizes user awareness and user-based policy management provided by Allot SMP.

The SMP provides IP:user matching using the following interfaces:

- DHCP
- Active directory (utilizing a special AD agent)
- SOAP API (the standards of which can be found at: https://tools.ietf.org/html/draft-box-http-soap-00

The SMP maintains a database of user policy and quota that can be provisioned with the following interfaces:

- Active directory LDAP query (utilizing a special AD agent)
- SOAP API

1.2.5 ClearSee (CS)

Allot ClearSee collects raw data from the Service Gateways as well as control plane elements including the Allot Subscriber Management Platform and employs a cutting-edge data warehouse designed for fast look-up, processing, and export. The data warehouse features a columnar structure and uses massive parallel processing (MPP) to handle big data with extreme efficiency.

ClearSee Network Metrics provides realtime network monitoring as well as long term dashboards that allows drill down and filtering for in depth analysis.

ClearSee Network Analytics (additional license required) self-service provides a full complement of web-based tools for manipulating and analyzing large varieties and volumes of data with extreme ease and efficiency.

1.2.6 DDoS Secure Controller (DSC)

Allot's DDoS Secure Controller integrates protection against bots infiltrating client devices and DDoS attacks into one package. The DSC works round-the-clock to protect the network and notify the administrator of any malicious activities.

1.3 Managing Passwords

In order to facilitate installation and initial configuration, Allot provides default values for all required passwords.

It is **ESSENTIAL** for security that these default passwords be changed **AS SOON AS POSSIBLE**. In this section each default password is listed, along with instructions on how to change it.

1.3.1 SSH Admin Password

Allot provides end-users with SSH access to the system via a user privilege called "**admin**".

NOTE **Allot STRONGLY recommends that the default passwords are changed to ensure a minimum level of security.**

- User Name: admin
- Default Password: allot

To change the SSH Admin password:

1. Log into the system via SSH.
2. Enter **admin** for the login and the admin password and then press **<Enter>**.
3. Enter **passwd** and then press **<Enter>**.
4. You will be asked to enter the current password and click **<Enter>**
5. When prompted enter a new password and press **<Enter>.** The password must be between 5 and 8 characters. You can use a combination of upper and lower case letters and numbers.
6. Re-enter the new password and press **<Enter>**.

1.3.2 SSH Root Password

The SSH Root password is required for certain actions in the CLI and gives complete access to the system. Therefore it should only be given to trusted users.

The default values are as follows:

NOTE **Customers are strongly advised to change default passwords on first login. Not doing so represents a security risk.**

- User Name: root
- Default Password: bagabu

Changing the Root Password

1. Access the Server using the SSH Admin log in and password.
2. Switch to SSH Root user with the following command:
   su -
3. Enter the root password, and then press **<Enter>**.
4. Enter **passwd** and then press **<Enter>**.
5. Enter a new password and press **<Enter>.** The password must be between 5 and 8 characters. You can use a combination of upper and lower case letters and numbers.
6. Re-enter the new password and press **<Enter>**.

1.3.3 iLO Password

The iLO is the Server Management Software used on HP servers provided by Allot. It is a way to access and manage the Server remotely. The default details of the iLO are as follows:

- Default User Name: USERID
- Default Password: Password10
- Default IP: 10.4.4.4
- Default Subnet: 255.255.0.0
- Default Gateway: 10.4.0.1

NOTE **If you enter an incorrect user name and password, or a login attempt fails, iLO imposes a security delay.**

NOTE **It is possible to change the default user name and password for the iLO by selected User Management on the System Configuration screen (see above), selecting Edit/Remove User > Action and entering the desired values when prompted.**

To change the iLO password, follow the steps below:

1. Reboot the server.
2. Log in to the iLO using the correct user name and password.
3. Select Administration from the Left hand menu and open the User Administration tab.

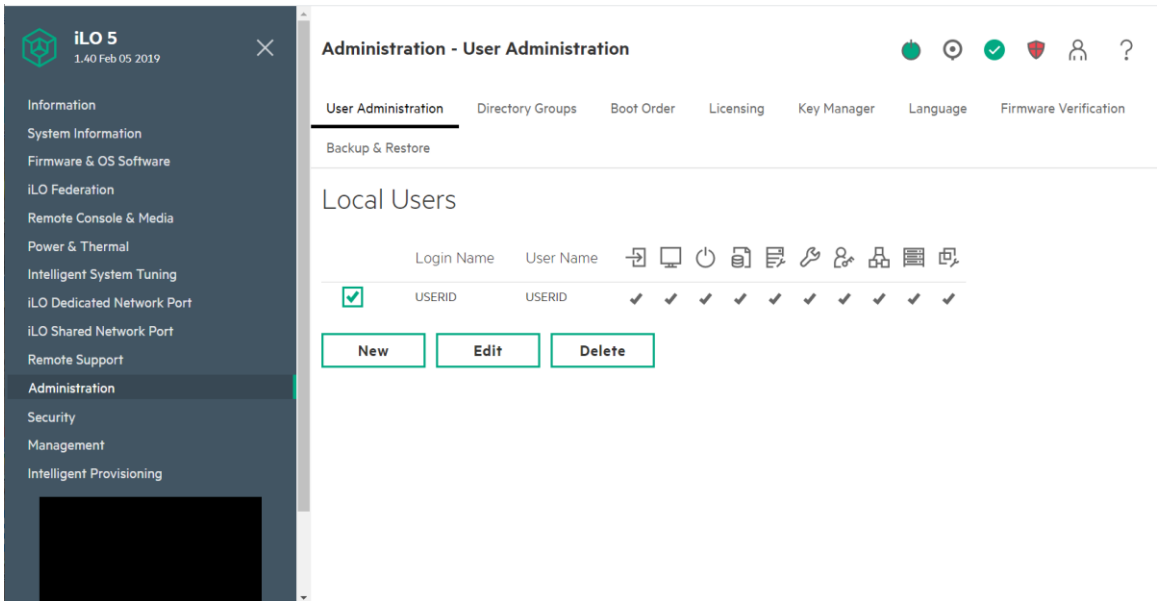


Figure 1-1: iLO User Administration Screen

4. In the Local Users area select USERID and click Edit.

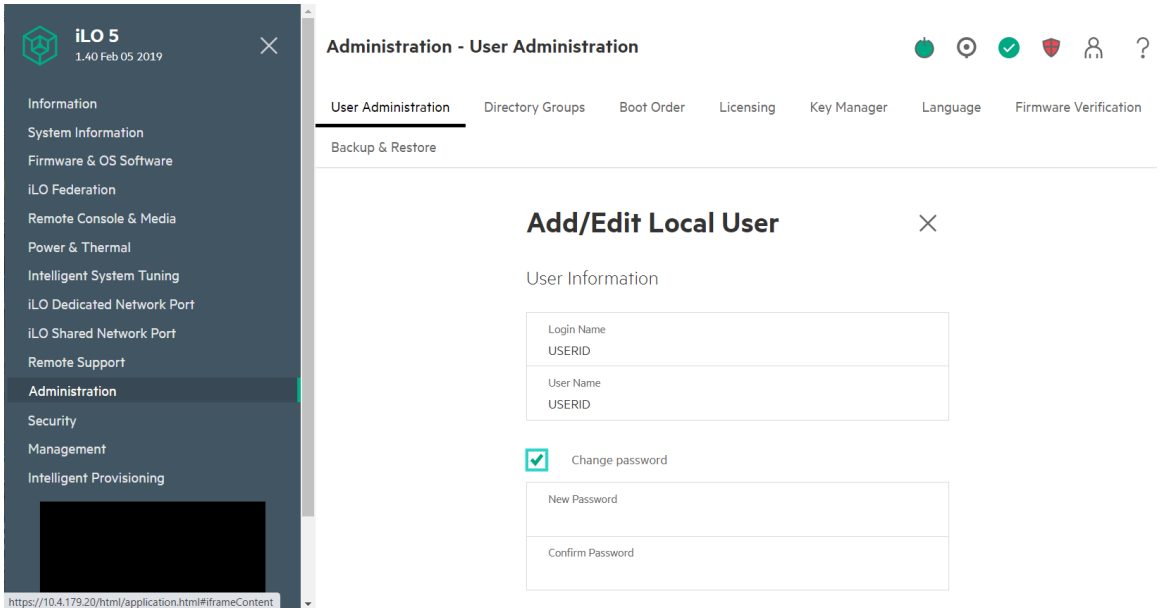


Figure 1-2: iLO Add/Edit Local User Screen

5. Select the Change Password checkbox and enter the new password in both the New Password and Confirm Password fields.

6. Click Update User to save the new password.

2 ACG Hardware

The ACG2000 is a standalone server upon which essential Allot Virtual Modules come pre-loaded. It has all you need to see, control, and secure your entire network.

Figure 2-1: ACG2000

2.1 Packing List

Verify that the following items are included with the ACG2000 and Bypass units:

- ACG2000 System pre-installed on a single HP server. There are two possible physical products which can be identified by running the following command in the iLO.

  ```
  getinfo -S | grep "Product Name"
  ```

  See Appendix 2 for specific information regarding hardware specifications.
- Pair of AC power IEC-320 C13/C14 cables
- 4 transceivers. Depending upon your order, the transceivers and Bypass (see next chapter for information about the Bypass) may be either copper or fibre. Make sure the transceivers, Bypass, and included cables are all the same type. This User Guide will is illustrated using 1gbps copper in all examples.

NOTEs **All Transceivers MUST be provided by Allot specifically for ACG2000. Any other Transceivers will not function in the ACG2000.**
The Appendix includes photographs of the other compatible Bypass units and transceivers.

- Ethernet cable straight CAT6 RJ45_2_RJ45 3m for management (Allot P/N C243010)

NOTE **Cables to connect from the ACG2000 to the Bypass are included with the Bypass Unit. Cables to connect from the Bypass Unit to the Network are not provided by Allot.**

NOTE **The following components of the ACG2000 are replaceable and hot swappable: Power Supply Units and Hard Disk Drives.**
The following components are replaceable but NOT hot swappable: NIC cards, RAM and RAID cards.

2.2 Front Panel

2.2.1 Front Panel Buttons and LEDS Description

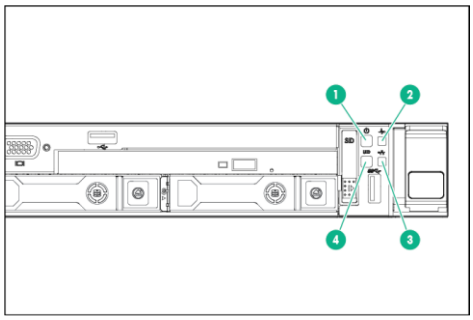


Figure 2-2: ACG2000 Front Panel Buttons and LEDs

DESCRIPTION	STATUS
1 - Power LED/Power on Button	Solid green = Power is on Flashing Green = Powering up Solid Amber = Stand by Off = Power is off Off = No network activity
2 - Health LED	Flashing Green = iLO is rebooting fault Flashing Amber = System is degraded Flashing Red = System critical Solid Green = The system is working normally

DESCRIPTION	STATUS
3 - Network Status LED	Solid Green = Network is connected Flashing Green = Network is Active Off = No network activity
4 – UID Button/LED	Flashing Blue = Reboot or upgrade in progress Solid Blue = Activated Off = Deactivated

2.2.2 Front Panel Connectors

There are no connectors on the front panel of the ACG2000

2.3 Rear Panel

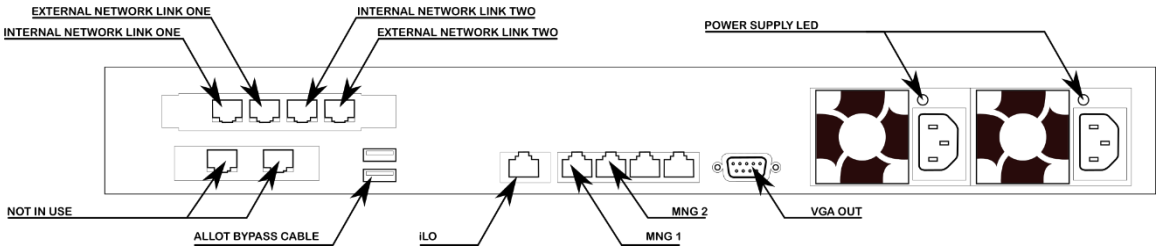


Figure 2-3: ACG2000 Rear Panel

- Regardless of transceiver type, the four network ports are divided into two distinct links: “Link One” and “Link Two”. **Do not mix links.** Connect the internal and external sides of Link One before utilizing either port of Link Two.
- **MNG1 & MNG2** are two RJ-45 connectors (1G Copper) which are used to connect the ACG2000 to the network. MNG2 acts as a redundant port for MNG1.
- The **iLO Port** is used to connect the iLO system to the network. For more information see Chapter 3.
- The **Allot Bypass Cable** can be plugged into either of the rear USB 3.0 ports.

All other ports are **not currently in use**.

2.3.1 Power Supply

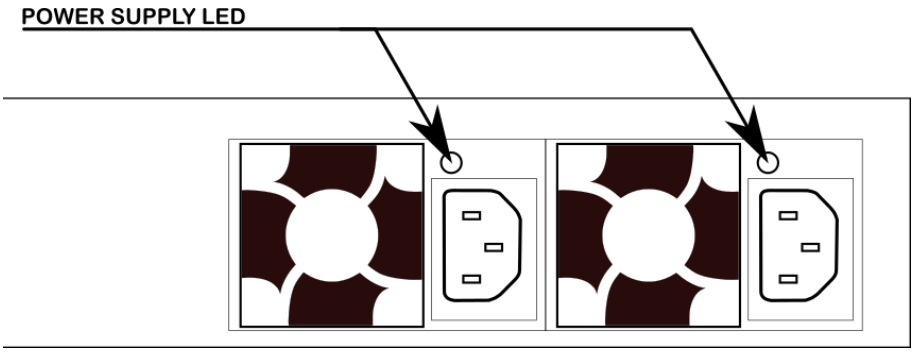


Figure 2-4: ACG2000 AC Power Feed

The ACG2000 contains two built in power supply modules and a dual line feed for redundancy purposes. Each line feed drives one power supply. It is possible for the unit to operate normally with only one of the two power supplies active. The AC Power Input LEDs glows solid green when the unit is receiving power. If an LED is not on it means that the unit is not getting any power from that power supply.

NOTE The AC power supply automatically adapts to voltages between 100 V and 240 V, 50/60 Hz.

3 Hardware Installation

3.1 Planning Your Deployment: The Server Room

This equipment is intended to be installed by trained service personnel and in environments where access by unauthorized personnel is restricted (Restricted Access Location). The ACG2000 complies with the requirements for operator access.

Please note that the power resources used by the ACG2000 must be planned and installed by a qualified electrical engineer only. Before installing or using ACG2000, please read all Safety Information carefully to avoid electrical hazards that can result in injury or loss of equipment.

In addition, be aware that all network and power connections to the ACG2000 are from the rear of the device so there must be adequate space behind the unit for safe access at all times.

This chapter is to be used in planning the power requirements and resources for the ACG2000 system, as well as mounting the equipment. Topics which are covered include:

- AC Power Source Requirements
- AC Cabling Requirements and Overcurrent Protection
- Space and Airflow Requirements
- Environmental Specifications
- Mounting Instructions

3.1.1 Power Source Requirements

Installation of this equipment must comply with local and regional electrical regulations governing the installation of information technology equipment by licensed electricians. This equipment is designed to operate in installations covered by NFPA 70, 1999 Edition (National Electric Code) and NFPA-75, 1992 (code for Protection of Electronic Computer/Data Processing Equipment).

NOTES **To reduce the risk of personal injury, fire, or damage to the equipment, do not overload the AC supply branch circuit that provides power to the rack. Consult the electrical authority having jurisdiction over wiring and installation requirements of your facility.**

Protect the server from power fluctuations and temporary interruptions with a regulating uninterruptible power supply. This device protects the hardware from damage caused by power surges and voltage spikes and keeps the system in operation during a power failure.

When installing more than one ACG, you may need to use additional power distribution devices to safely provide power to all devices. Observe the following guidelines:

- Balance the power load between available AC supply branch circuits.
- Do not allow the overall system AC current load to exceed 80% of the branch circuit AC current rating.
- Do not use common power outlet strips for this equipment.
- Provide a separate electrical circuit for the ACG2000.

3.1.2 Electrical Grounding Requirements

The server must be grounded properly for proper operation and safety. In the United States, you must install the equipment in accordance with NFPA 70, 1999 Edition (National Electric Code), Article 250, as well as any local and regional building codes. In Canada, you must install the equipment in accordance with Canadian Standards Association, CSA C22.1, Canadian Electrical Code. In all other countries, you must install the equipment in accordance with any regional or national electrical wiring codes, such as the International Electro technical Commission (IEC) Code 364, parts 1 through 7. Furthermore, you must be sure that all power distribution devices used in the installation, such as branch wiring and receptacles, are listed or certified grounding-type devices.

Because of the high ground-leakage currents associated with multiple servers connected to the same power source, Allot recommends the use of a PDU that is either permanently wired to the building's branch circuit or includes a non detachable cord that is wired to an industrial-style plug. NEMA locking-style plugs or those complying with IEC 60309 are considered suitable for this purpose. Using common power outlet strips for the server is not recommended.

3.1.3 AC Power Cord Specifications

Allot provides a set of 2 x IEC-320 C13 to C14 Power Cords Black 2.5m 10A.

Figure 3-1: IEC-320 C13 to C14 Power Cord

All power cords used must meet the following specifications:

- Use copper conductors only.
- The cord must have the appropriate cross-sectional dimension for the current rating.
- The cord must have insulation material suitable for at least 75 °C.
- The cord must have local safety approvals, and preferable additional approvals such as UL, CSA, TUV or VDE.
- The flexible cord and attachment plug cap length must not exceed 4.5 m (15 ft.).
- For a cord set assembly, the cords must be protected against physical damage and arranged in appropriate cable ducts.
- Connector:
  - Wall outlet end - Cords must be terminated in an industrial grounding-type male plug designed for use in your region.
  - Connector unit end - The connectors that plug into the AC receptacle on the unit must be an approved IEC 320, C13 type female connector.

3.1.4 Space and Airflow Requirements

To allow for servicing and adequate airflow, observe the following space and airflow requirements when deciding where to install a rack:

- Leave a minimum clearance of 63.5 cm (25 in) in front of the rack.
- Leave a minimum clearance of 76.2 cm (30 in) behind the rack.

- Leave a minimum clearance of 121.9 cm (48 in) from the back of the rack to the back of another rack or row of racks.

The ACG2000 draws in cool air through the front door and expel warm air through the rear door. Therefore, the front and rear rack doors must be adequately ventilated to allow ambient room air to enter the cabinet, and the rear door must be adequately ventilated to allow the warm air to escape from the cabinet.

When vertical space in the rack is not filled by a server or rack component, the gaps between the components cause changes in airflow through the rack and across the servers. Cover all gaps with blanking panels to maintain proper airflow.

3.2 Environmental Specifications

Operating temperature	10°C to 35°C (50°F to 95°F), Relative humidity (%RH) 8% to 80% Maximum Altitude
Operating relative humidity	8% to 80%
Operating altitude	3,048 m

3.3 Rack Mounting the ACG2000

NOTES **To reduce the risk of personal injury or damage to the equipment, be sure that:**
The leveling jacks are extended to the floor.
The full weight of the rack rests on the leveling jacks.
The stabilizing feet are attached to the rack if it is a single-rack installation.
The racks are coupled together in multiple-rack installations.
Only one component is extended at a time. A rack may become unstable if more than one component is extended for any reason.
Always plan the rack installation so that the heaviest item is on the bottom of the rack. Install the heaviest item first, and continue to populate the rack from the bottom to the top.

1. Install the server into the rack. Follow the instructions provided by your rack manufacturer.
2. Plug in the networking cables as per Physical Network Configuration, Chapter 4.2
3. Connect the power cord to the rear of the server.
4. Use the Velcro strips on the back of the power unit to secure the power cord(s).

NOTE To reduce the risk of electric shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into RJ-45 connectors.

5. Connect the power cord to the AC power source.

NOTES To reduce the risk of electric shock or damage to the equipment:
Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.
Unplug the power cord from the power supply to disconnect power to the equipment.
Do not route the power cord where it can be walked on or pinched by items placed against it. Pay particular attention to the plug, electrical outlet, and the point where the cord extends from the server.

4 Bypass and Physical Network Set-up

4.1 External Bypass Unit

The ACG2000 operates with an external Bypass Unit. The Bypass Unit is a mission-critical subsystem designed to ensure network connectivity at all times. The Bypass mechanism provides "connectivity insurance" in the event of a subsystem's failure. Each Allot Bypass unit features low insertion loss (< 1dB) in both Normal mode and Bypass mode and fast switching time (< 10mSec) between modes. The ACG's Network ports must be connected to the External Bypass Unit. This is to ensure continuous service in the event of failure. The Application Control Gateway should be ordered with appropriate Bypass Unit as it will not boot without being connected to one.

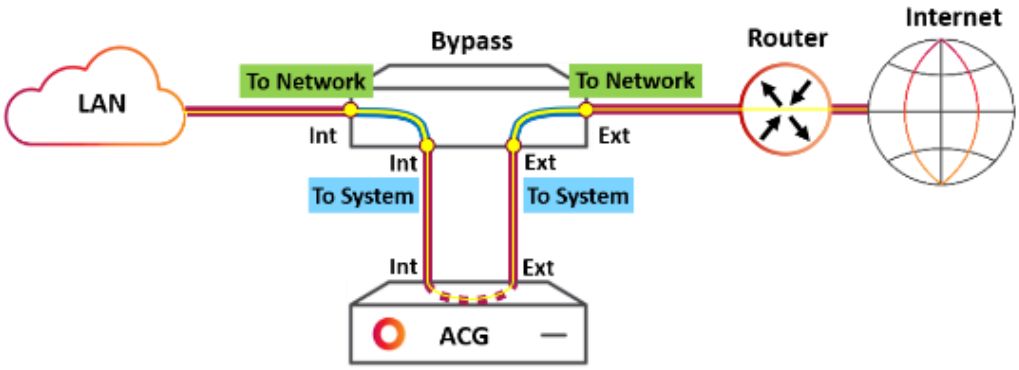


Figure 4-1: The Bypass directs traffic to the ACG

Should the ACG stop operating (for example, in the case of power failure) the network traffic flows straight through the Bypass, bypassing the ACG altogether. The Bypass Unit allows users on the LAN experience uninterrupted internet access whether or not the ACG is online.

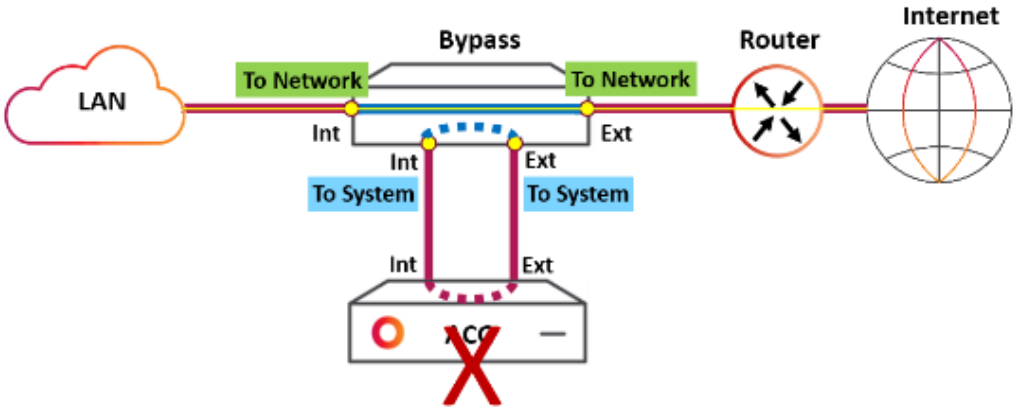


Figure 4-2: The Bypass redirects traffic in case of failure

They Bypass unit and ACG 2000 are somewhat customizable. Depending upon your order, the transceivers and Bypass may be either copper or fibre. Make sure the transceivers, Bypass, and included cables are all of the same type. This User Guide is illustrated using 1gbps copper in all examples.

The HD 8 Copper Bypass Unit supports up to 4 links (8 ports), and is used here to illustrate how to network the ACG and Bypass together. While other bypass units may look different, the principles of how to wire them together remains the same.

In terms of Management, the Bypass unit is connected to the ACG2000 via a single USB cable.

The Appendix includes a list of all Bypass Units that are compatible with the ACG2000 along with photographs and an explanation of ports.

4.1.1 HD 8 Copper Bypass Unit

The HD 8 Copper Bypass Unit (previously known as the Allot Multi-Port Bypass works in conjunction with the ACG2000.

The HD 8 Bypass Unit includes connectors for up to 2 links on the ACG2000. In addition, the HD 8 Bypass Unit includes two D-type 9-pin connectors (DB-9) for connection to the ACG2000 via special DB-9/USB cables (available from Allot).

The HD 8 Bypass Unit is a passive optical device with no need for external power connection. It is powered by the ACG2000 as long as the ACG2000 is powered on. It

will move automatically to bypass mode when ACG2000 is powered off, or by being forced to bypass mode as protective action is taken. There is no way to have a single link go into bypass independently. When moving to Bypass mode **all** links are switched into Bypass.

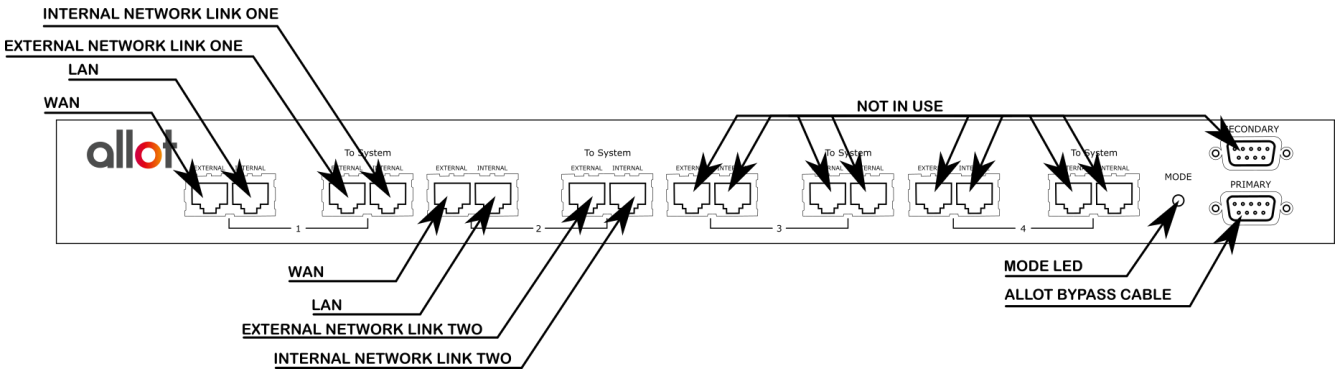


Figure 4-3: HD 8 Copper Bypass Unit

HD 8 Bypass Unit LEDS Description

The following indicator can be used to identify the operation of the blade:

- **Mode LED** is **STEADY GREEN** when the Bypass Unit is operating normally and **OFF** when the Link is in Bypass mode.

HD 8 Bypass Unit Front Panel Connectors

- **Links 1-4** connect to the network (on the left of each link) and the ACG2000 (on the right of each link). Only links 1 and 2 are in use.
- **Primary** connects to either USB port on the ACG2000.
- **Secondary** is not in use.

4.1.2 External Bypass Control Cabling

The HD 8 External Bypass Unit is connected to the ACG2000 by a Single USB Unit Cable (1:1) connected to the Primary port on the Bypass Unit and one of the two USB ports on the rear of the ACG2000. This cable is provided with the Bypass unit.

NOTE **To avoid damage, use ONLY the cable provided with the Bypass Unit for connection to the ACG2000.**

Figure 4-4: Allot USB Bypass Cable

4.2 Physical Network Configuration

The ACG2000 is, by default, prepared to interface with the Bypass unit. The following procedure connects the two units together and onto your network:

1. Use the supplied management cable to connect the PRIMARY management terminal on the Bypass to either USB port on the rear of your ACG2000.
2. Using the included Cat 6 cables, connect the Bypass to the ACG2000. Then use your own cables to connect the Bypass to the internet and to your network. Every link between the Bypass and the ACG require a corresponding connection between the Bypass to the internet and internal network. Follow the diagram below:

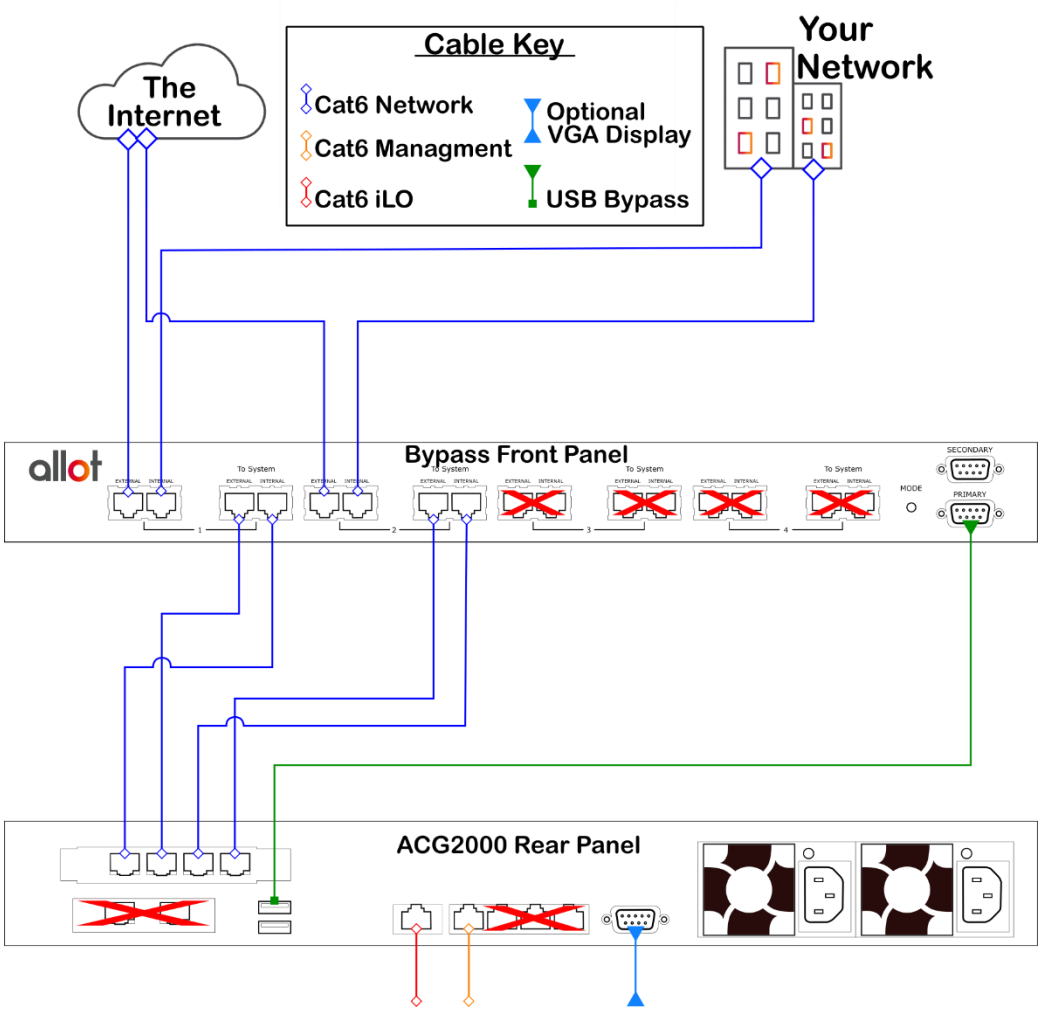


Figure 4-5: Network Diagram

3. Power up the ACG2000.

5 Setting Up the iLO Connection

5.1 Setting the IP for the iLO

1. Connect a keyboard, mouse, and display to the ACG2000 to set the iLO's IP address via the BIOS/UEFI.
2. Power up the ACG2000.
3. When the initial screen appears press **F9** to open “System Utilities”.

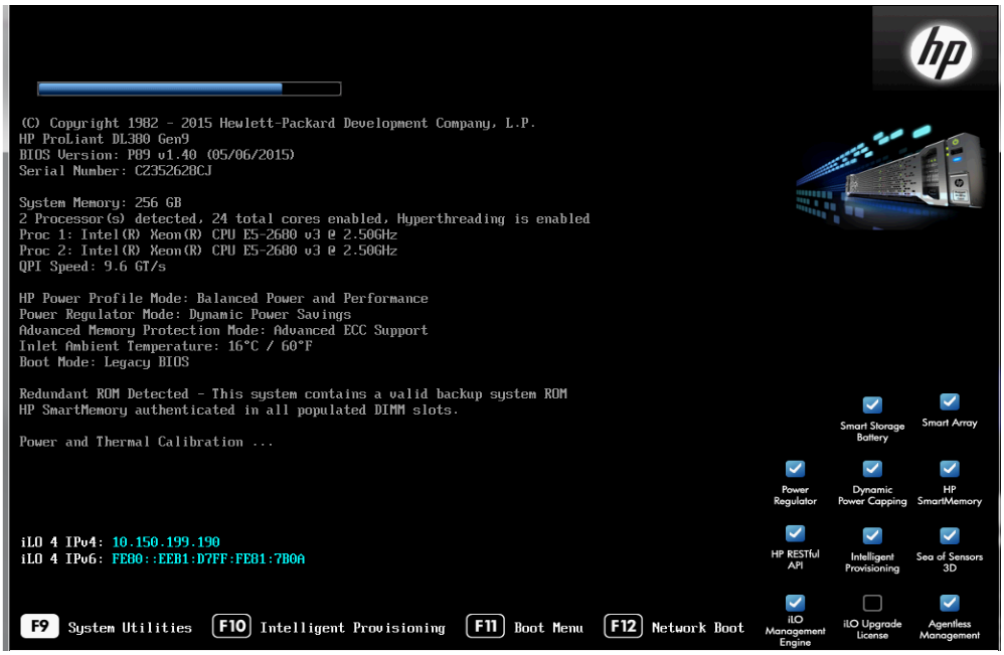


Figure 5-1: Initial Screen

The System Utilities screen opens.

4. Select **System Configuration**.

Figure 5-2: System Utilities Screen

The System Configuration Screen opens.

5. On the System Configuration screen select **Network Options.**

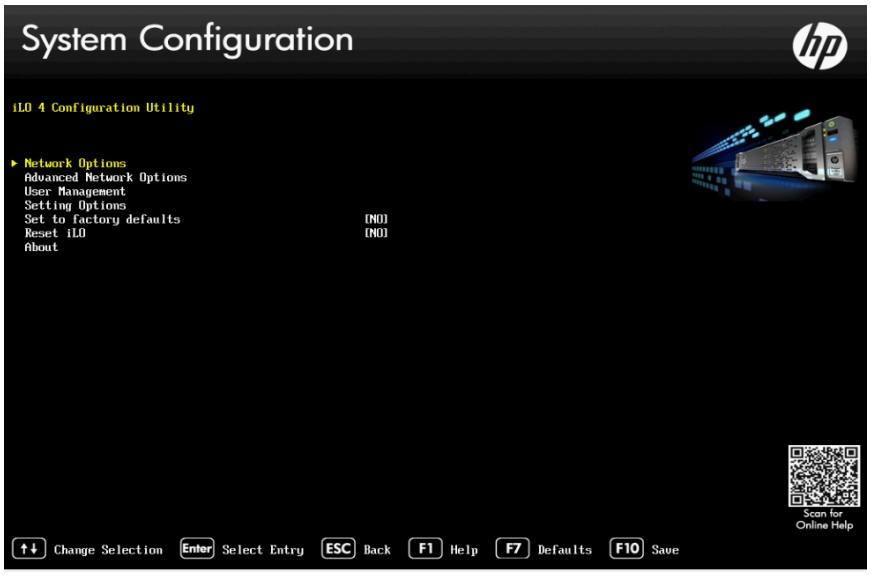


Figure 5-3: System Configuration Screen

6. Define your iLO parameters such as IP address and Subnet Mask.

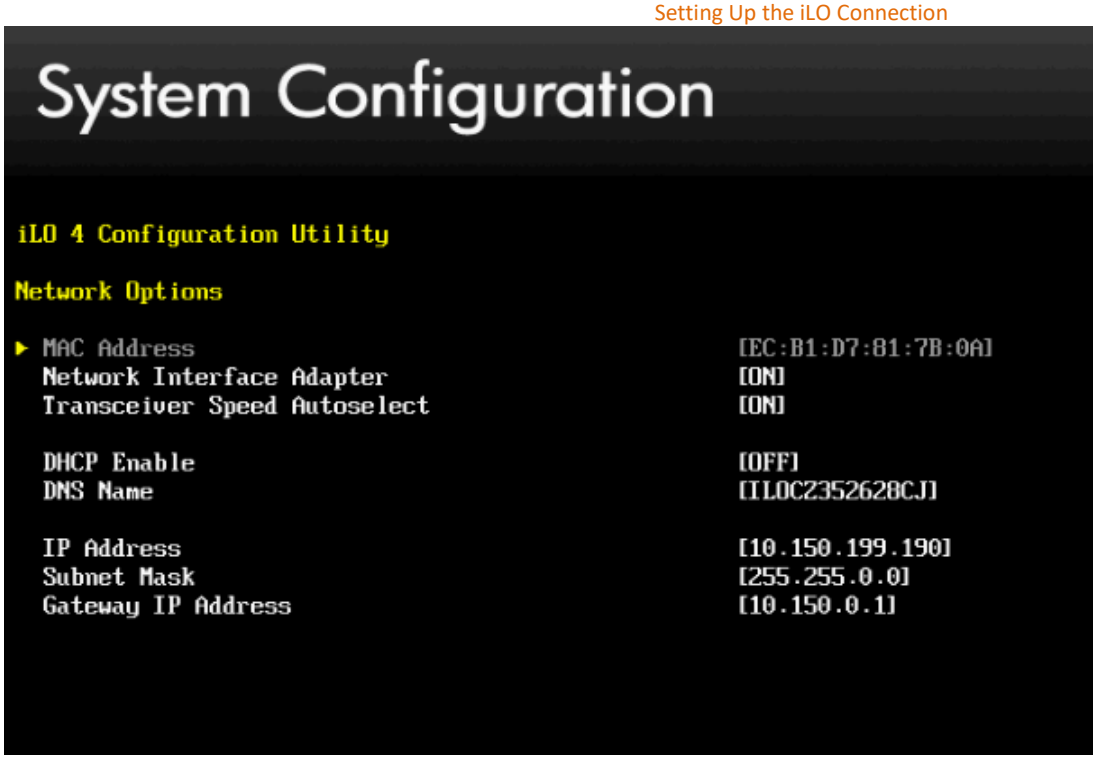


Figure 5-4: Network Options Screen

7. Press **F10** to save your settings.
8. Press **Esc** to return to the System Configuration screen.
9. Select **Reboot the System.**

5.2 Logging into the iLO

1. Connect the iLO Port on the back of the ACG2000 server to a dedicated switch for access to the internet.
2. Enter the IP address for the iLO into a web browser (Internet Explorer or Edge recommended).

NOTE If you are using Safari or Chrome you must use the Java based option.

3. Enter the iLO User Name and Password and click **Log In**.

Figure 5-5: iLO log in screen

The iLO Overview screen opens.

4. Select **Remote Console** from the list of options on the left of the screen.

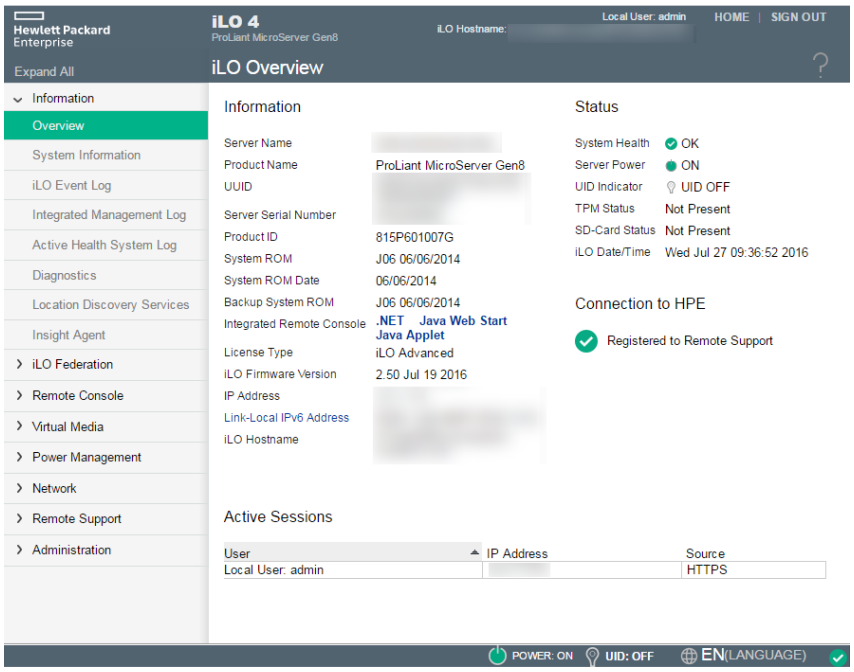


Figure 5-6: iLO Overview Screen

The iLO Remote Console Screen opens.

5. Select either the **.NET Integrated Remote Console** (for IE and Edge browsers) or the **Java Integrated Remote Console** (for all other browsers) and click LAUNCH. If either .NET or Java needs to be updated you will be informed and directed to the appropriate website.

NOTE **It is also possible to download the iLO Mobile App from this page, for use on iOS and Android mobile devices.**

The CentOS Login screen appears. Log in with the Admin password.

6. The Remote Console opens.

6 Deploying the Modules

6.1 Getting Started

The following Modules are preloaded on the ACG2000 and only require deployment.

- **SG-VE**
- **NetXplorer**
- **Data Mediator**
- **Subscriber Management Platform***
- **ClearSee**
- **DDoS Secure Controller***

NOTES **The ACG2000 comes with a file titled "acg2000***.tgz". Retain this file for troubleshooting purposes. It can be found under /opt/allot/**
The starred modules are optional. Providing a false IP address will render an optional module non-functional without detrimentally impacting the overall ACG2000 system.

To simplify the deployment process, have the following information available **before** starting the deployment.

- Host (Server) IP
- Unique IPs **for each Module**
  - Legitimate IP addresses for **every** module you wish to use
  - False IP addresses for any module you don't want to activate
- Subnet Mask
- Gateway IP
- DNS
- SG-VE license key
- NetXplorer licenses key [this includes all NMS functionalities]

For assistance contact your network administrator.

6.2 Configuring the Network Parameters

After mounting the ACG2000 in a standard server rack and connecting it to the power supply and bypass (as shown in Hardware Installation), it is time to set up the Host.

1. Power up the ACG2000.
2. Log into the ACG2000 via iLO (see Logging into the iLO)
3. Open the Terminal screen.
4. Access the server using the SSH Admin log in and password.
5. Switch to SSH Root user with the following command:

```
su -
```

6. Enter the root password, and then press **<Enter>**.
7. Run the following command to open the Network Configuration Menu:

```
/root/netmenu.sh
```

```
  Initial  Network  Configuration  Menu

#  I/F            MAC Address                  IP Address                  NETMASK         UP
1) eno1        : 4:18:82:66:ab:b8                          10.4.70.130        255.255.0.0  V
                                                           Not-defined                V
2) eno2        : 94:18:82:66:ab:b9                         Not-defined                .
3) eno3        : 94:18:82:66:ab:ba                         Not-defined                .
4) eno4        : 94:18:82:66:ab:bb                         Not-defined                .
5) eno49       : 48:df:37:29:80:54                         Not-defined                .
6) eno50       : 48:df:37:29:80:55                         Not-defined                .
7) Gateway     : 10.4.0.1
8) Hostname    : aio.allot.local
9) DNS         : 8.8.8.8
10) MNGT I/F   : eno1
11) NTP        : 0.centos.pool.ntp.org 1.centos.pool.ntp.org
12) Clear All Network Configuration
13) Quit

Choose a number of an item to configure or Enter to Refresh screen :
```

Figure 6-1: Network Configuration Menu

NOTE A DNS must be entered or else the deployment will not complete.

8. Fill out items 1, 7, 8, 9, 10, and 11. This sets up the Host with appropriate network connections.
9. Select item 13, and then choose “Apply Changes”

6.3 The ACG Wizard

The ACG Wizard allows for quick setup of all the ACG's modules in one procedure. The Wizard can be run before or after connecting the hardware to the internet.

1. Open a web browser and visit **http://<host_ip_address>:5000** (where <host_ip_address> is the IP address on line 1 of the network configuration menu) to open the Allot ACG2000 Deployment Wizard.
2. The wizard opens to the Server Prerequisite Check and Installation screen.

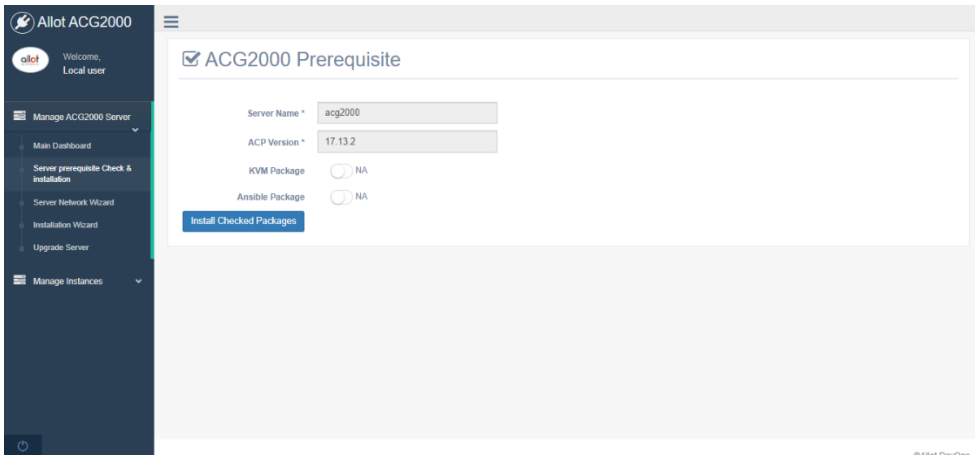


Figure 6-2: Prerequisites Screen

3. Select both the **KVM Package** and **Ansible Package** options and click **Install Checked Packages**. KVM and Ansible must be installed at this point for the ACG2000 to function properly. Installation will take several minutes.
4. When the installation of the packages is complete, the Wizard will automatically move to the Server Network Installation screen.

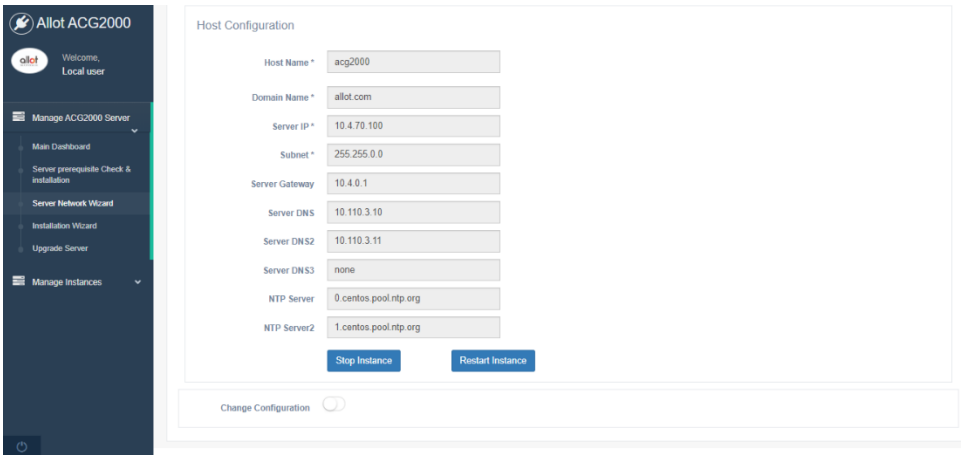


Figure 6-3: Server Network Screen

5. Confirm that all the information you entered in netmenu previously is here and accurate and select **Change Configuration**. Click **Apply Changes**.

NOTE **Even if you do not change any of the information, you must select Change Configuration and click Apply Changes, otherwise the deployment will fail.**

6. In the left sidebar menu, click **Installation Wizard** to set the network data for the Modules. The Wizard opens to AOS Configuration.

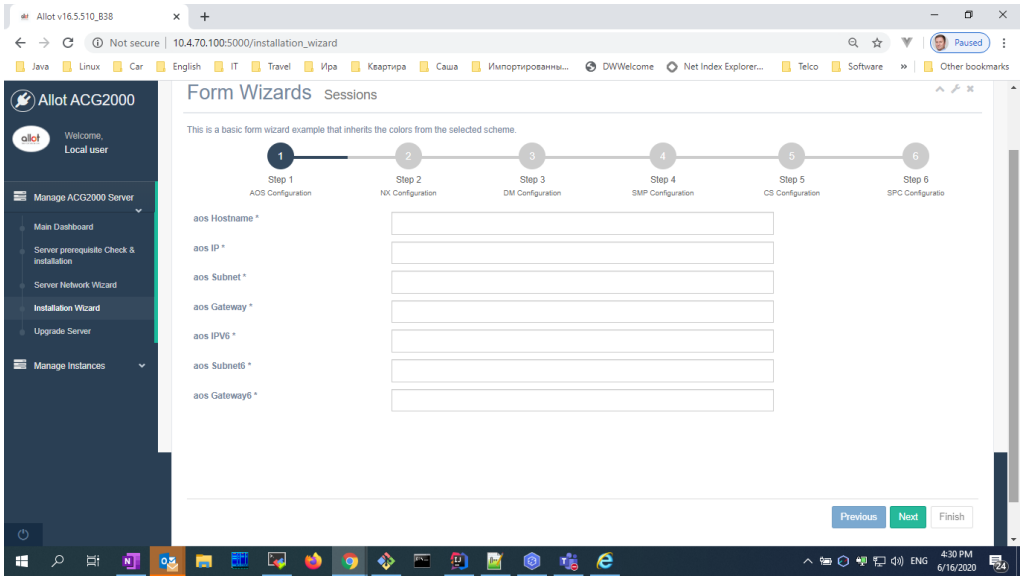


Figure 6-4: AOS configuration screen

7. For AOS, enter a Hostname, unique IP, Subnet, and Gateway. IPv4 addresses should be entered in fields 2, 3, and 4. IPv6 addresses should go in fields 5, 6, and 7.
8. You must enter **none** in all the fields (either IPv4 or IPv6) you do not need to complete, otherwise the deployment will fail.
9. Click **Next** to proceed to NX Configuration.
10. Complete the NX Configuration screen and click **Next** to proceed to the DM Configuration Screen.
11. Complete the DM Configuration screen and click **Next** to proceed to the SMP Configuration Screen.
12. Complete the SMP Configuration screen and click **Next** to proceed to the ClearSee Configuration Screen.
13. Complete the ClearSee Configuration screen and click **Next** to proceed to the SPC Configuration Screen.

NOTE **The "SPC" is now DDoS Secure. When the Wizard refers to the SPC, the product actually being set up is DDoS Secure.**

14. Once you have entered the values for the SPC, click **Finish** to close the Wizard. You may also use the **Previous** button to go back to previous configuration screens. Applying the values may take a moment.
15. The Main Dashboard opens. Here you can review key information for the full system and check the status of each Module.

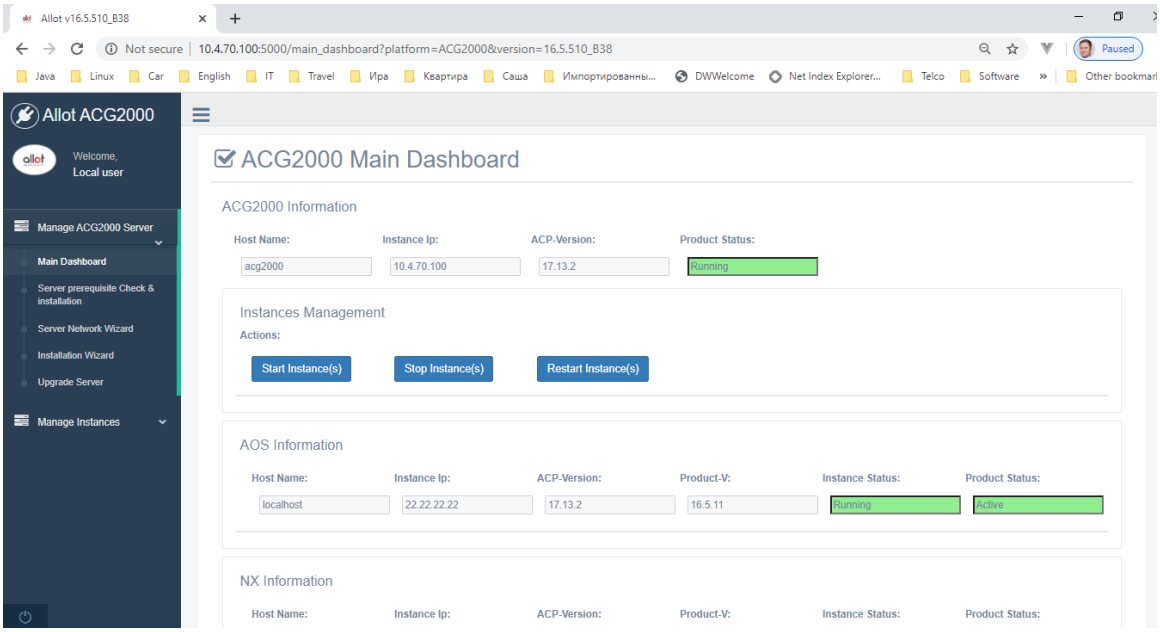


Figure 6-5: Main Dashboard Screen

16. You can select the **Manage Instances** dropdown in the left-hand menu to see the full configuration and status for each individual Module as well as buttons to Start, Stop or Restart that instance. You may also change any of the information for that Module using the **Change Configuration** toggle.
17. If at any point you wish to redeploy your Modules or change their configuration, simply access the Wizard again and rerun it. To reconfigure your ACG2000 server from scratch, follow the instructions in Reinstalling the Software.

7 Getting Started

The steps in this chapter must be completed to finish setting up the ACG2000. The procedures will be performed entirely through the NetExplorer (NX) GUI. More information about the NX system can be found in the NetXplorer Operation Guide and the NetXplorer Installation and Administration Guide.

7.1 Accessing your NetXplorer

Use the following procedure to access the NX system for the first time. The application runs on Java and will prompt for an update if needed.

1. Access the **ACG Main Dashboard** by navigating to <ip_address>:5000/main_dashboard.

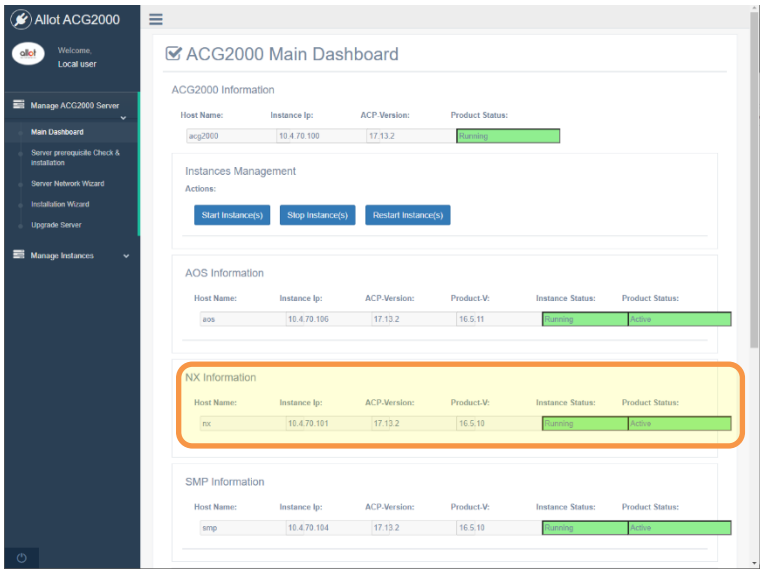


Figure 7-1: The ACG Main Dashboard, with the NX Information pane highlighted

2. Copy the **Instance Ip** under the **NX Information** pane.

3. Open a new tab in your browser and navigate to the copied IP address. To do this, paste the IP address into the address bar and then hit **<enter>**. The NetXplorer Launcher appears.

Figure 7-2: The NetXplorer Launcher

4. Click **Install Java JRE first.** When prompted, select your operating system. The **Java JRE Setup Wizard** downloads.
5. Run the **Java JRE Setup Wizard**. When the Java installation has concluded, go back to the **NetXplorer Launcher.**
6. Click **Launch NetXplorer**. The browser downloads a small file called **netxplorer.jnlp**. When asked whether to keep or discard this file, select **keep**.

7. Run **netxplorer.jnlp**. The file verifies its own integrity and then opens the **Allot NetXplorer Log On Screen**.

Figure 7-3: The Allot NetXplorer Log On Screen

8. Enter your User Name and Password

7.2 Licensing your System

The ACG needs two license keys set before beginning normal operation. Make sure you have your license keys ready before performing the following procedures.

7.2.1 Enabling NetXplorer Server

In order to manage the ACG using NetXplorer, NetXplorer Server must be enabled by entering the appropriate key. This key may be entered at installation or at any time following.

To enable NetXplorer Server:

1. Select **Tools > NetXplorer Application Server Registration** from the NetXplorer Menu bar.

The NetXplorer Application Server Registration dialog box appears.

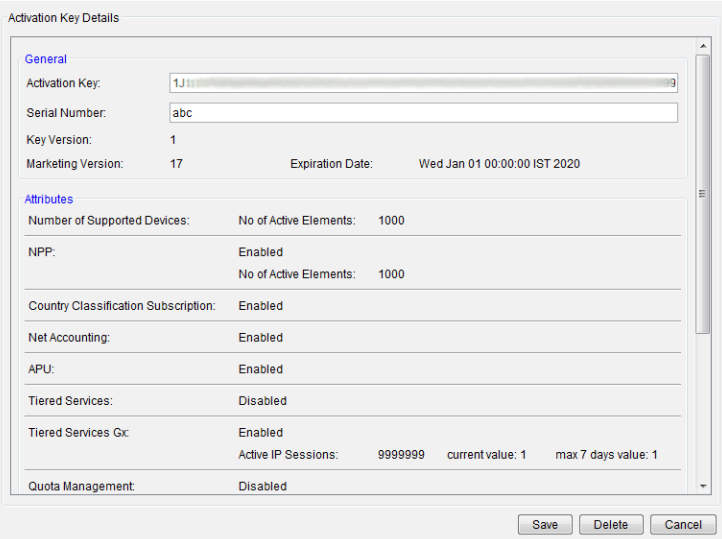


Figure 7-4: NetXplorer Application Server Registration Dialog

2. Enter the Activation Key and Serial Number provided by Allot to enable the NetXplorer Server functionality.
3. A Key Version, Marketing Version and Expiration Date will be generated automatically after clicking **Save**.
4. The number of devices supported by the key is indicated.
5. If Enforcement Policy Provisioning is enabled by the key that has been entered, it will be indicated (along with the maximum number of accounts) after **NPP**. For more information, see the NPP User Guide.
6. If Classification of Hosts by Country is enabled by the key that has been entered, it will be indicated after **Country Classification Subscription**.
7. If Accounting information is enabled by the key that has been entered, it will be indicated after **Net Accounting**.
8. If Service Catalog updates via the web are enabled by the key that has been entered, it will be indicated after **APU**.
9. If Subscriber Management is enabled by the key that has been entered, it will be indicated by one of the following attributes being enabled – e.g: **Tiered Services or Quota Management.** In addition, the number of supported *active subscribers*, the current number of subscribers and the highest number of subscribers over the last 7 days will be indicated if relevant. This information is provided on the system level (i.e: for all SMP

Groups). For more information, see the SMP Installation and Administration Guide.

10. If Session Management is enabled by the key that has been entered, it will be indicated by at least one of the following attributes being enabled – e.g: **Tiered Services Gx, Volume Reporting or Cell Awareness.** In addition, the licensed maximum number of *active IP sessions*, the current number of active IP sessions and the highest number of IP sessions over the last 7 days will be indicated if relevant. This information is provided on the system level (i.e: for all SMP Groups). For more information, see the SMP Installation and Administration Guide.

NOTE **If Mobile Analytics is enabled by the key that has been entered, it will be indicated by the following attribute being enabled: Mobile Reports SMP. In addition, the number of active IP sessions, the current number of IP sessions and the highest number of IP sessions over the last 7 days will be indicated if relevant. This information is provided on the system level (i.e: for all SMP Groups). For more information, see the SMP Installation and Administration Guide.**

11. Click **Save** to enter the key and close the dialog box.

7.2.2 Licensing the ACG

The parameters available in the Service Gateway Configuration window are grouped on the following tabs:

- General
- Identification & Key
- SNMP
- Security
- Interface
- Networking
- IP Properties
- Date/Time
- Service Activation
- Slots & Boards

Each tab includes parameters that can be configured as required. After modifying configuration parameters, you must select **Save** in order for the changes to take effect. The save process prompts a reset of the Service Gateway. Resetting is sometimes required to ensure that some saved parameter values are committed and activated on the Service Gateway. To license the ACG, you will need to access the Identification and Key tab.

Identification & Key

The **Identification & Key** tab includes parameters that provide system information and activate optional Service Gateway modules.

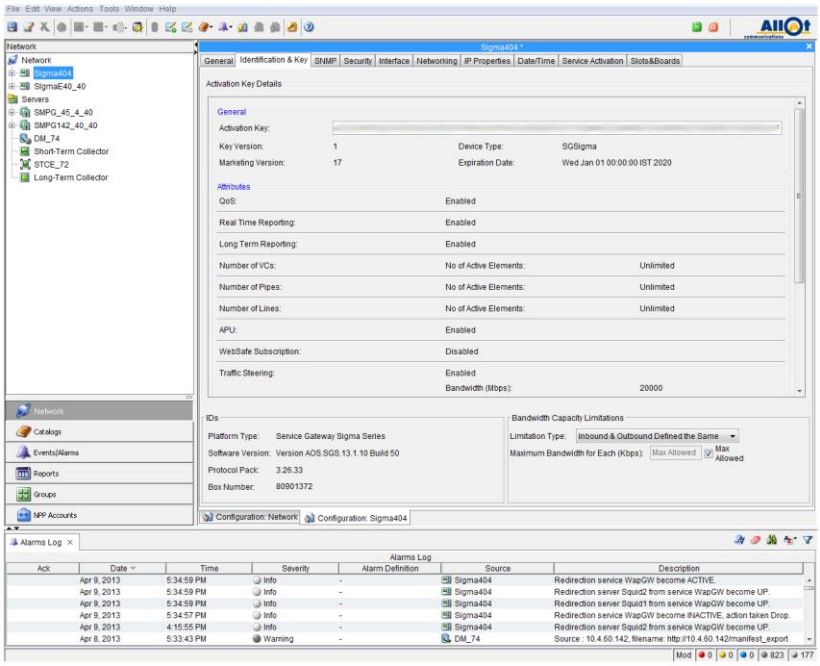


Figure 7-5: Configuration - Identification & Key Parameters

The **Identification & Key** tab includes the following parameters:

PARAMETER	DEFINITION
Activation Key	The activation key enables the Service Gateway. Enter the activation key supplied to you at purchase. The functionality enabled by the key is summarized in the fields below the key.
Serial Number	The Serial Number of the Service Gateway.
Key Version	For Internal Use Only
Marketing Version	For Internal Use Only
Device Type	The Type of Service Gateway.

PARAMETER	DEFINITION
Expiration Date	The expiration date of the entered Activation Key.
QoS	Quality of Service is enabled/disabled on the Service Gateway.
Real Time Reporting	Real Time Reporting is enabled/disabled on the Service Gateway. Real Time Reporting requires an appropriate key to be enabled.
Long Term Reporting	Long Term Reporting is enabled/disabled on the Service Gateway. Long Term Reporting is enabled by default.
Number of Lines	The maximum number of Lines that may be defined on the Service Gateway. This field also indicates the current number of lines and the highest number of lines during the last seven days.
Number of Pipes	The maximum number of Pipes that may be defined on the Service Gateway. This field also indicates the current number of pipes and the highest number of pipes during the last seven days.
Number of VCs	The maximum number of Virtual Channels that may be defined on the Service Gateway. This field also indicates the current number of VCs and the highest number of VCs during the last seven days.
APU	Allot Protocol Update is enabled/disabled on the Service Gateway.
WebSafe Enforcement	WebSafe is enabled/disabled on the Service Gateway, listing the number of Core Controllers covered by the license.
WebSafe Subscription	WebSafe is subscribed to the Internet Watch Foundation blacklist service. This subscription is optional
Traffic Steering	Port or URL Redirection is enabled/disabled on the Service Gateway. For further information see **Error! Reference source not found.** on page **Error! Bookmark not defined.**. If Enabled, the maximum **Bandwidth (Mbps), No of Active Elements** and **No of Subscribers** on the system level appears.

PARAMETER	DEFINITION
SP Mitigation	Listing the number of Core Controllers enabled for Service Protector as covered by the license. If this field lists a value of 0, it indicates the service is not enabled by the current license. A NetEnforcer will list this value as 1 if the service is enabled.
SP Embedded Sensors	Listing the number of Core Controllers enabled for SP Embedded Sensors as covered by the license. If this field lists a value of 0, it indicates the service is not enabled by the current license. A NetEnforcer will list this value as 1 if the service is enabled.
Mobile Reports	Listing the number of Core Controllers enabled for Mobile Reporting as covered by the license. If this field lists a value of 0, it indicates the service is not enabled by the current license. A NetEnforcer will list this value as 1 if the service is enabled.
Statistics Export	Listing the number of Core Controllers enabled for Statistics Export as covered by the license. If this field lists a value of 0, it indicates the service is not enabled by the current license. A NetEnforcer will list this value as 1 if the service is enabled.
Tethering	Listing the number of Core Controllers enabled for Tethering as covered by the license. If this field lists a value of 0, it indicates the service is not enabled by the current license. A NetEnforcer will list this value as 1 if the service is enabled.
HTTP CDRs	Listing the number of Core Controllers enabled for HTTP CDRs as covered by the license. If this field lists a value of 0, it indicates the service is not enabled by the current license. A NetEnforcer will list this value as 1 if the service is enabled.
MediaSwift – Cache Out	The Cache Out bandwidth of the MediaSwift Service, in Mbps.
Autonomous System	Listing the number of Core Controllers enabled for Autonomous System features as covered by the license.
Http Header Enrichment	Listing the number of Core Controllers enabled for HTTP Header Enrichment as covered by the license.

PARAMETER	DEFINITION
Video Data Records	Listing the number of Core Controllers enabled for VDRs as covered by the license.
Platform Type	The platform series of the Service Gateway
Software Version	The software version running on the Service Gateway.
Protocol Pack	The Protocol Pack release and version loaded into the Service Catalog of the Service Gateway.
Box Number	The ID number of the Service Gateway.
Bandwidth Capacity Limitations – Limitation Type	The way bandwidth limitations are imposed on the Service Gateway; **Inbound & Outbound Defined Separately**, **Inbound & Outbound Defined the Same** or **Half Duplex**.
Inbound Bandwidth Limited to:	The incoming bandwidth limitation of the NetEnforcer, in Kbps. Select the **Max Allowed** checkbox to allow the maximum value to be passed.
Outbound Bandwidth Limited to:	The outgoing bandwidth limitation of the NetEnforcer, in Kbps. Select the **Max Allowed** checkbox to allow the maximum value to be passed.

Once you have accessed the tab, fill in all the information to ensure smooth operations for your ACG unit.

7.3 Configuring your ACG in the NX

In order for NetXplorer to manage the ACG, it must be added to the NetXplorer's network and properly configured. The IP address of the ACG is required for this procedure.

NOTE **Initial configuration of the ACG should be performed on the ACG (via the CLI interface) before it is added to the NetXplorer configuration. Refer to the hardware manual for the specific ACG model for details.**

NOTE **In the NetXplorer GUI ACG units and Service Gateways are referred to as NetEnforcers.**

To add the ACG:

1. In the Navigation pane, right-click Network in the Network of the Navigation tree and select **New NetEnforcer** from the popup menu.

   OR

   Select Network in the Network pane of the Navigation tree and then select **New NetEnforcer** from the Actions menu.

2. The NetEnforcer Properties - New dialog is displayed.

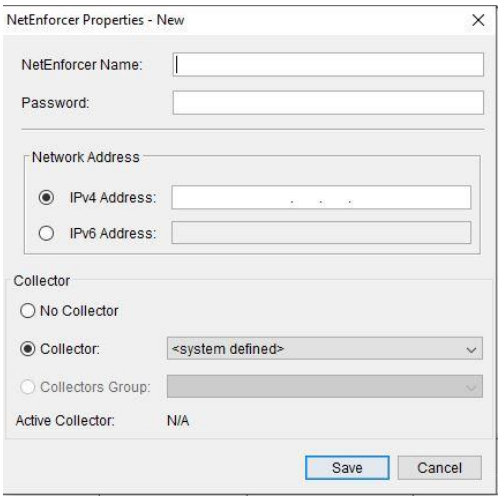


Figure 7-6: NetEnforcer Properties – New Dialog

3. Enter the Name you want the ACG referred to by, as well as the SSH Password of the ACG in the designated fields.
4. Enter the Network Address of the ACG in the designated field. This may be an IPv4 address or an IPv6 address.
5. Choose a Monitoring Collector or Collector Group for the ACG from the drop-down menus. The new ACG will transmit its monitoring data to that Collector or Group only. The default option is **<system defined>** which means that the Service Gateway will transmit its monitoring data to the internal Short Term Collector which is built into the NetXplorer server. If you do not have any Monitoring Collectors on the Network and you do not want to use the NetXplorer's internal monitoring collector, select **No Collector**.

6. Click **OK**. The ACG is added to the Navigation tree. The Add NetEnforcer operation can take up to a few minutes to complete.

To Configure the ACG via the NetXplorer:

1. In the Navigation pane, select and right-click the ACG in the Navigation tree and select **Configuration** from the popup menu.

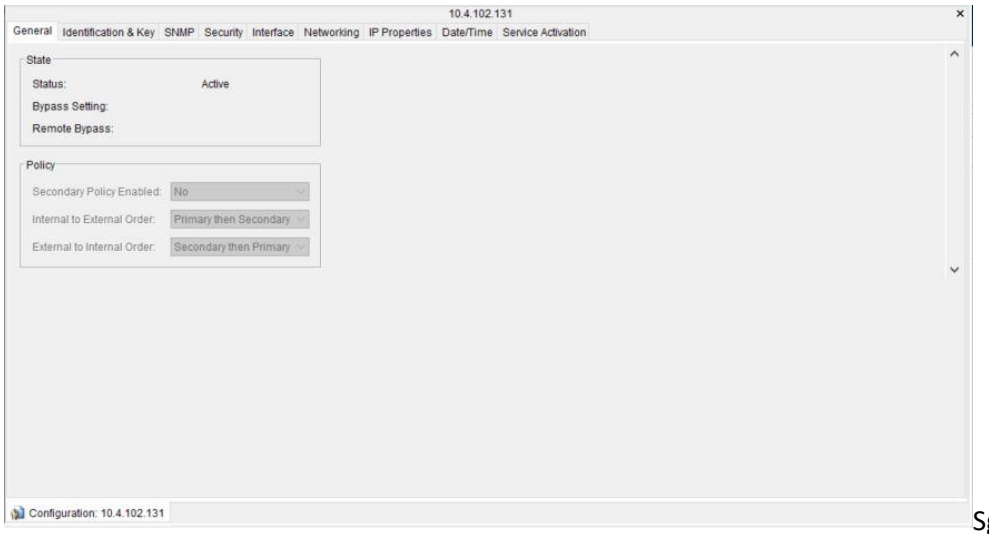
   OR

   Select the ACG in the Navigation tree and then select **Configuration** from the View menu.

   OR

   Select the ACG in the Navigation tree and then click the **Configuration** icon  on the toolbar.

2. The Configuration window for the selected ACG is displayed.



Sg

Figure 7-7: ACG Configuration

3. Configure the ACG parameters, as required.
4. Click  or select **Save** from the File menu to save the changes to the ACG configuration.

The Configuration parameters available in the ACG Configuration window are grouped on the following tabs:

- **General** – indicates the ACG's bypass status.
- **Identification and Keys** – includes parameters that provide system information and activation keys

- **SNMP** – enter the contact person, location, system name and description for SNMP purposes
- **Security** – includes security and authorization parameters
- **Interface** – includes parameters to configure the system interfaces to either automatically sense the direction and speed of traffic or use default parameters as well as parameters to define ports
- **Networking** – includes parameters that enable you to configure network topology
- **IP Properties** – enables you to modify the IP and host name configuration of your network interfaces as well as the DNS and connection control parameters
- **Date/Time** – includes the date, time and NTP server settings for the ACG
- **Service Activation** - includes IP and Port Redirection Parameters
- **Slots and Boards -** includes device layout to provide schematic device components layout (when applicable) and status information. This tab does not appear when not relevant to the ACG.

After modifying configuration parameters you must select **Save** in order for the changes to take effect. The save process prompts a rebooting of the ACG. Rebooting is required to ensure that some saved parameter values are committed and activated on the ACG.

Once the ACG is configured to work with the NX, the entire setup can be controlled through the command line. For mor information about managing the elements of the ACG through the CLI, see the AOS Operation Guide.

7.4 Adding and Configuring your Data Mediator

7.4.1 To Add a Data Mediator

1. Open NetXplorer.
    1. In the Navigation pane, right-click Servers in the Network pane in the Navigation tree and select **New Data Mediation…** from the popup menu.
    2. The Data Mediation Properties - New dialog is displayed.

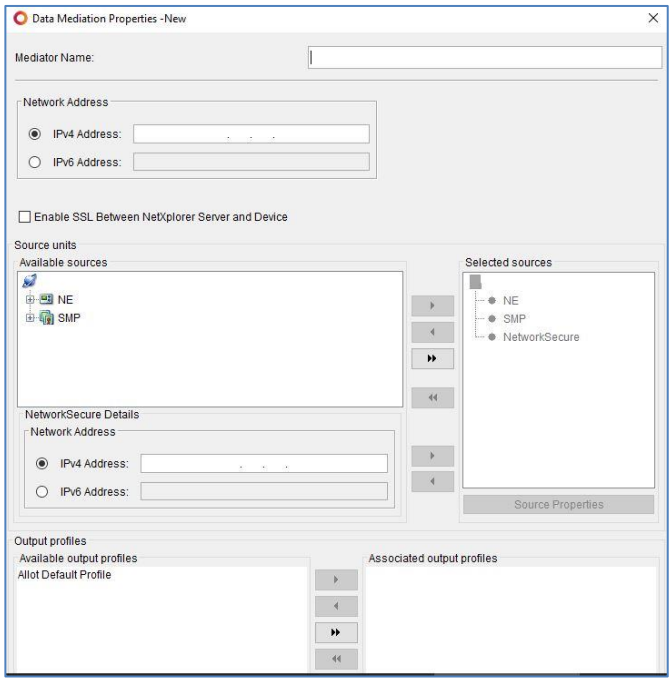


Figure 7-8: Data Mediation Properties

3. Enter the name of the Data Mediator.
4. Enter the Network Address of the Data Mediator in the designated field. This may be an IPv4 address or an IPv6 Address.
5. Select the **Enable SSL Between NetXplorer Server and Device** checkbox if you wish the connection between NetXplorer and the DM to be more secure.
6. In the Source Units area, use the arrow keys to move the ACG and SMPs from the Available to the Selected lists. Those selected will provide data to the Data Mediator.
7. To collect WSP Buckets, enter the IP address (IPv4 or IPv6) of your NetworkSecure in the NetworkSecure Details field and click the Right Button to add it to the Selected sources.

Note: **SDR, CMDR, CMCS and CMBM collection is only possible if you have included an SMP in the Selected Sources.**

CMDR, CMCS and CMBM collection requires an SMP in SMF Mode. For more information, see the SMP Installation and Administration Guide.

WSP Bucket collection is only possible if you have added the NetworkSecure IP to the Selected Sources.

- Depending on the ClearSee license you purchased with your ACG, select either the default Metrics, Analytics, or Realtime profile. For more information on Profiles, see Data Mediator Installation and Administration Guide.

8. Data Mediator Profiles
9. Click Save to add the Data Mediator to the network.

- NOTEFor more information concerning DMs, see the Data Mediator Installation and Administration Guide.

7.4.2 Data Mediator Profiles

Allot Default Profile

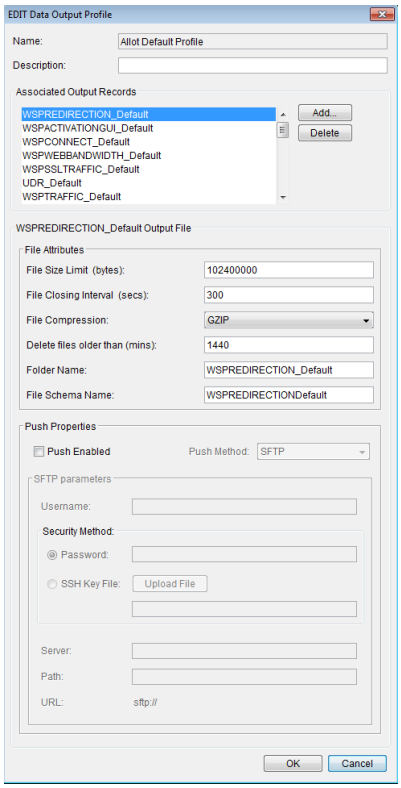


Figure 7-9: Default Data Mediation Profile

"Allot default profile" includes all the fields that appear in the DataDictionary file for the following buckets with immediate trigger (no keys and no excluding rules):

- VC
- Conv
- Conv_RTS
- Conv_RTU
- UDR
- SDR
- HDR
- VDR
- CMDR
- CMCS
- CMBS
- WSP Buckets

Note: **This Profile may be edited.**

Allot Default ClearSee Metrics Profile

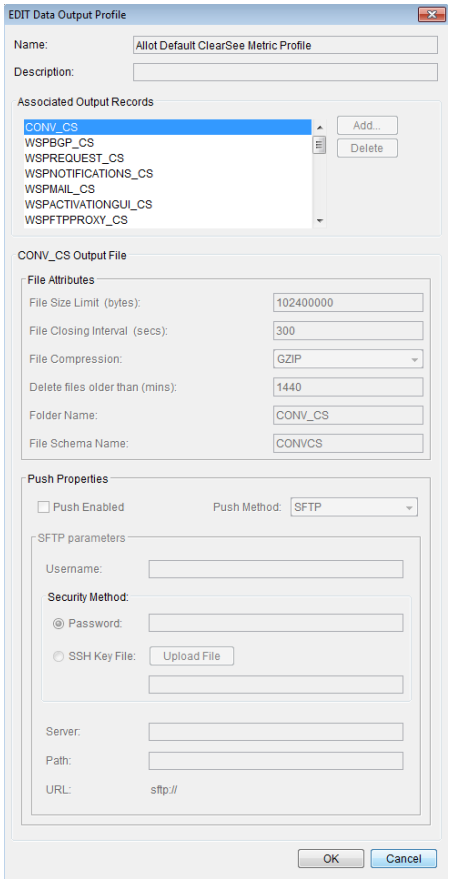


Figure 7-10: Default ClearSee Metrics Profile

Allot Default ClearSee Light profile includes all the fields of all the records that appear in the following AOS buckets with immediate trigger (no keys and no excluding rules):

- HTTP
- Conv
- SDR
- CMDR
- WSP Buckets

Note: **This Profile may not be edited and is only available with a ClearSee license.**

Allot Default ClearSee Analytics Profile

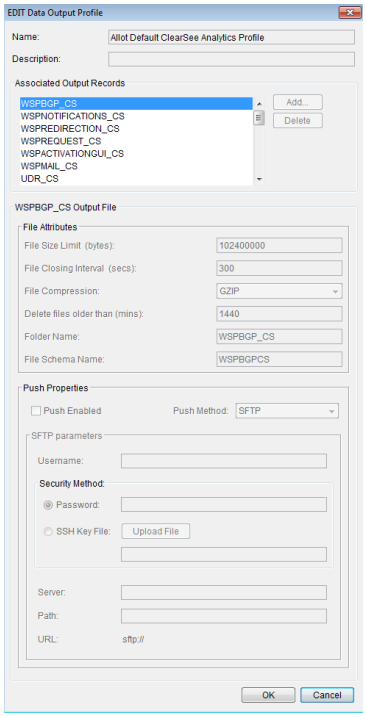


Figure 7-11: Default ClearSee Analytics Profile

Allot Default ClearSee Analytics Profile includes all the fields that appear in the following AOS buckets with immediate trigger (no keys and no excluding rules):

- VC
- Conv
- UDR
- SDR
- HDR
- VDR
- CMDR
- MOU
- HTTP
- WSP Buckets

Note: **This Profile may not be edited and is only available with a ClearSee license.**

Allot Default ClearSee Real Time Profile

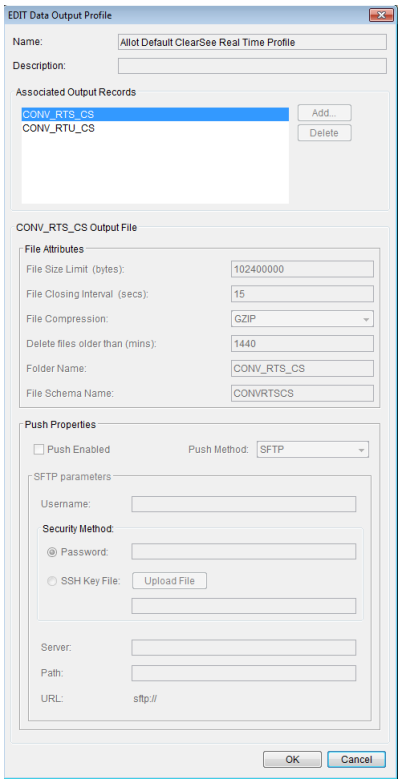


Figure 7-12: Default ClearSee Real Time Profile

Allot Default ClearSee Real Time Profile includes all the fields that appear in the following AOS buckets with immediate trigger (no keys and no excluding rules):

- Conv-RTS
- Conv-RTU

Note: **This Profile may not be edited and is only available with a Real Time Monitoring license.**

7.5 Building your ClearSee System

This procedure describes how to build the Standalone ClearSee system, which you must do after installation.

It involves defining the BI-DW instance and the DM, then configuring the system on the network, and finally performing some optional configurations.

Complete information about your ClearSee system can be found in the ClearSee Installation and Administration Guide and the ClearSee Operation Guide.

To build the Standalone ClearSee system:

1. Define the BI-DW instance, as described in Defining a BI Instance in the Navigation Pane.

   NOTE When situated in a standalone system, the BI instance is actually referred to as the BI-DW instance.

2. Define the DM, as described in **Chapter 3** of the **Data Mediator Install and Admin Guide**, and associate the ClearSee output profile with it.
3. In the NetXplorer **Navigation** pane, right-click the **Network** node, and then select **Configuration**.

   The **Network Configuration** area appears.
4. Select the **ClearSee** tab.

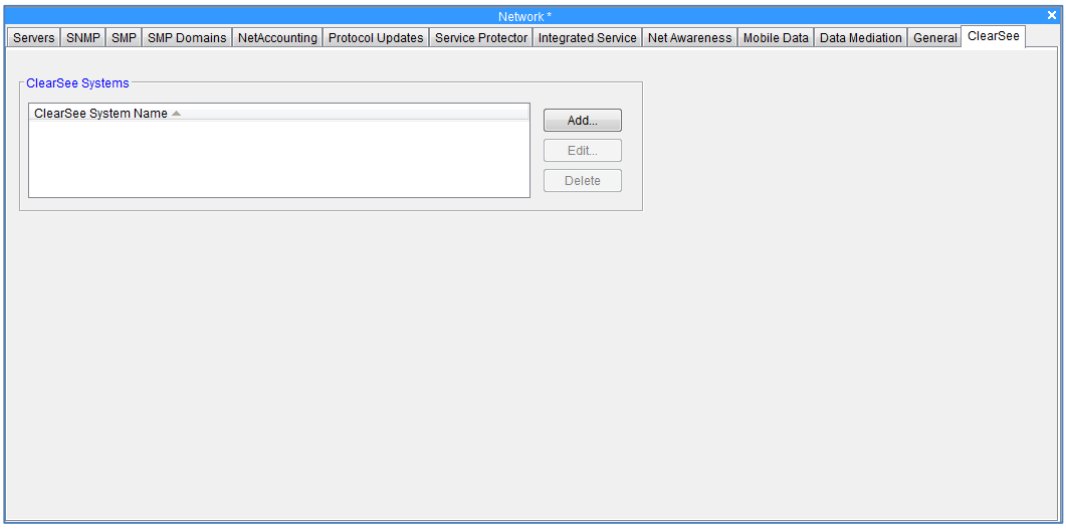


Figure 7-13: ClearSee Tab in NetXplorer

5. In the **ClearSee Systems** area, click **Add**.

   The **ClearSee System – New** dialog box appears, on the **General** tab.

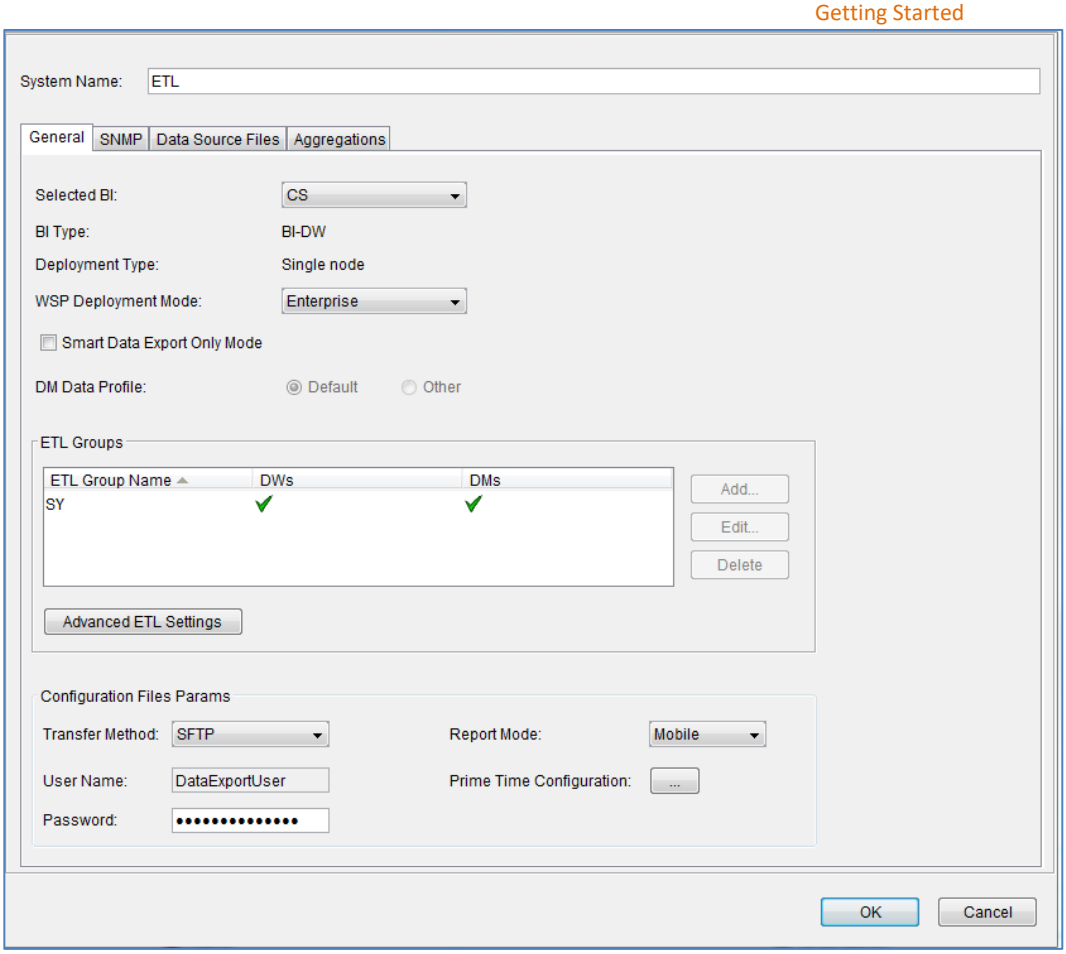


Figure 7-14: ClearSee System – Dialog Box

6. Do the following:

   - In the **System Name** field, name your ClearSee system.
   - From the **Selected BI** dropdown list, select the BI instance for your ClearSee system.

   The **BI Type** and **Deployment Type** fields are populated accordingly.

NOTE **When situated in a Standalone system, the BI instance is actually the BI-DW instance, and thus it is referred.**

   - From the **NetworkSecure Deployment Mode** dropdown list, select the appropriate mode, which determines the NetworkSecure dashboards and templates that appear for you in ClearSee.
   - If you do not intend to use ClearSee's GUI, but rather just use the ClearSee back end, then, to save resources, select **Smart Data Export Only Mode**.
   - Define the ETL group, as described in DEFINING THE STANDALONE ETL GROUP.

- From the **SNMP** tab, configure any additional SNMP traps destination.
- From the **Data Source Files** tab, define any external data files.
- From the **Aggregations** tab, configure data retention and aggregation delay.

NOTES The actions performed on the Aggregations tab are required.
As Transfer Method, the FTP option is currently not in use.

- From the **Report Mode** dropdown list, select the appropriate mode, which determines the reports and dashboards that appear for you in ClearSee. For a list of which reports, dashboards and templates appear with which modes, see the **ClearSee Operation Guide**, **Chapter 4: Reports and Dashboards, Reports and Dashboards Overview**.

7. Click **Prime Time Configuration** for Prime Time settings.
8. Click **OK**.

On the **ClearSee** tab of the **Network Configuration** area, in the **ClearSee Systems** area, the Standalone ClearSee system appears.

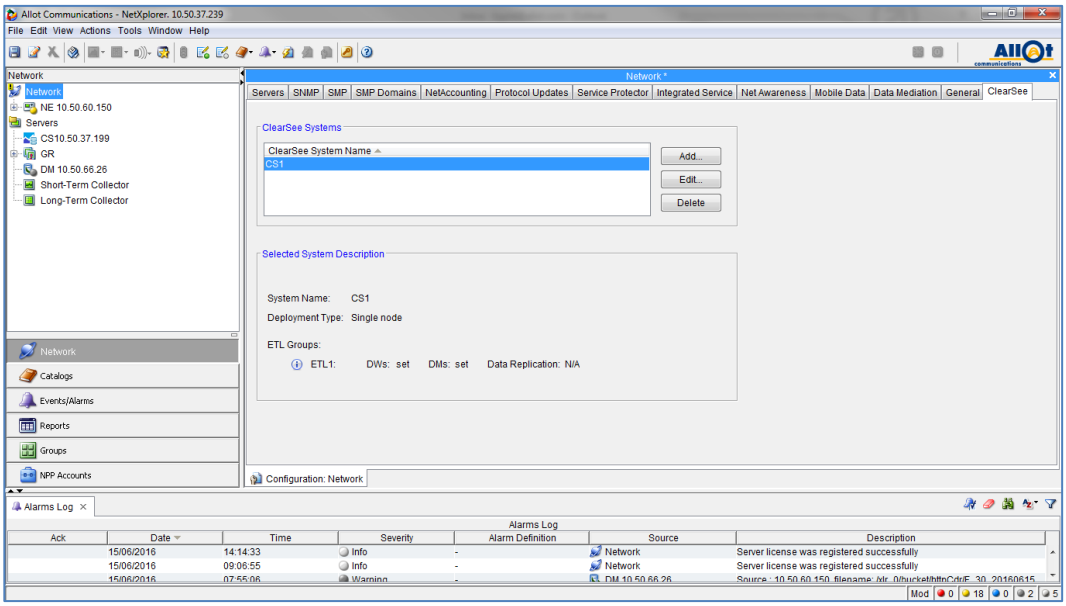


Figure 7-15: Completed ClearSee Systems Area (Standalone)

9. From the NetXplorer menu bar, click **Save** to permanently save the ClearSee system.

In the **Network Configuration** area, under **Data Mediation > Output Profiles**, a new associated output profile is automatically created, called after the name of your ClearSee system, as follows:

- If you have a Metrics license, then the name of the profile is comprised of **ClearSee Light Profile** and then your ClearSee system.
- If you have an Analytics license, then the name of the profile is comprised of **ClearSee Professional Profile** and then your ClearSee system.

10. Return to Integrating ClearSee with NetXplorer.

7.5.1 Defining a BI Instance in the Navigation Pane

Define in the NetXplorer **Navigation** pane the BI instance that you created earlier. If this is a Standalone deployment, then the instance is called BI-DW.

1. In the NetXplorer **Navigation** pane, in the **Network** tree, right-click the **Servers** node  , and then select **New ClearSee BI**.

To define the BI instance:

2. In the NetXplorer **Navigation** pane, in the **Network** tree, right-click the **Servers** node  , and then select **New ClearSee BI**.

The **ClearSee BI Properties – New** dialog box appears.

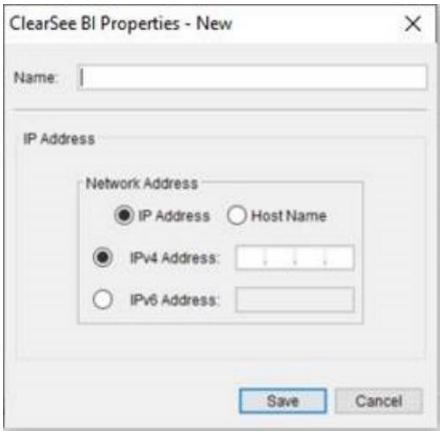
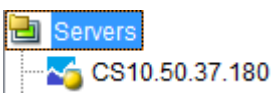


Figure 7-16: ClearSee BI Properties – New Dialog Box

3. Do the following:
   a. In the **Name** field, name the BI instance as you want it to appear in the **Navigation** pane.
   b. In the **IP Address** area, enter the IPv4 and/or IPv6 addresses of the BI instance.
   c. Click **Save**.

The BI instance appears in the **Navigation** pane, under **Servers**.



4. Click **Save** to permanently save the BI instance on the network.

7.5.2 Defining the Standalone ETL Group

This procedure describes how to define the ETL group in a Standalone deployment. Involved is adding the ETL group including the DW, and selecting the DM.

To configure the Standalone ClearSee system on the network:

1. In the **ETL Groups** area, click **Add**.

The **ETL Group – New** dialog box appears.

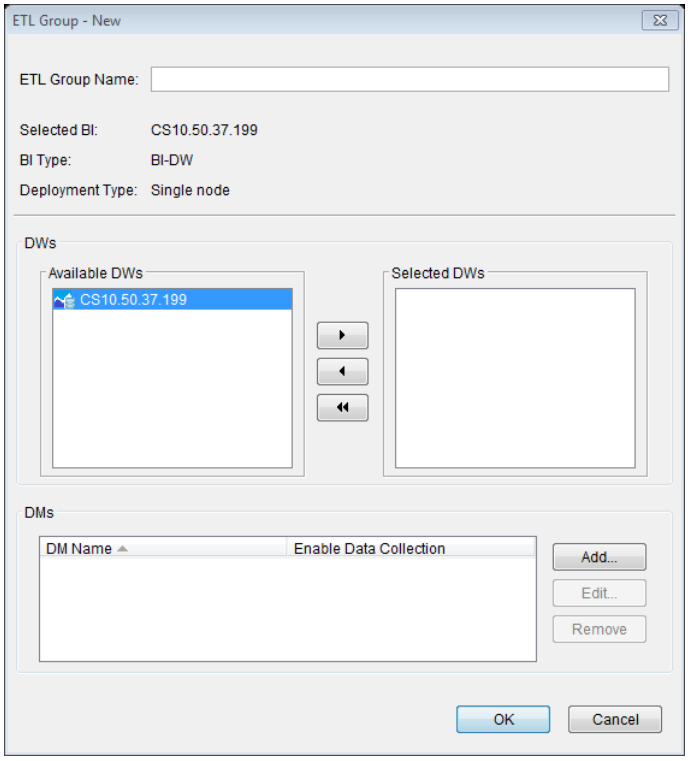


Figure 7-17: ETL Group – New Dialog Box (Standalone)

2. In the **ETL Group Name** field, name the ETL group.
3. In the **DWs** area, use the arrow key to move the BI-DW instance from **Available DWs** to **Selected DWs**.

NOTE **As this is a Standalone deployment, there is only one available DW, that which the BI-DW instance comprises.**

4. In the **DMs** area, click **Add**.

The **Add DM to ETL Group** dialog box appears.

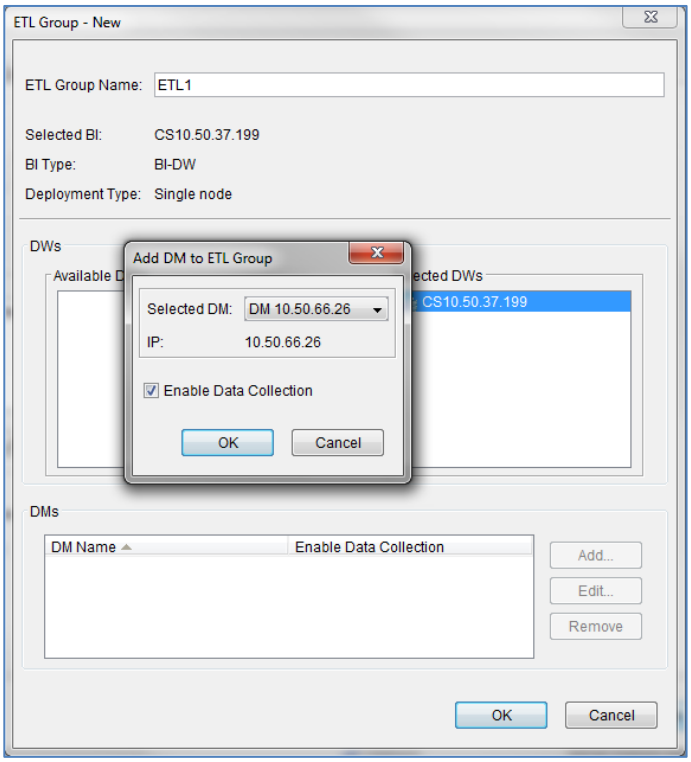


Figure 7-18: Add DM to ETL Group Dialog Box

5. Do the following:

   a. From the **Selected DM** dropdown list, select for your ETL group the DM with the associated ClearSee output file.

      In the **IP** field, the IP of the DM appears.

   b. Ensure that **Enable Data Collection** is selected.

   c. Click **OK**.

In the **DMs** area of the **ETL Group – New** dialog box, the DM appears in the table.

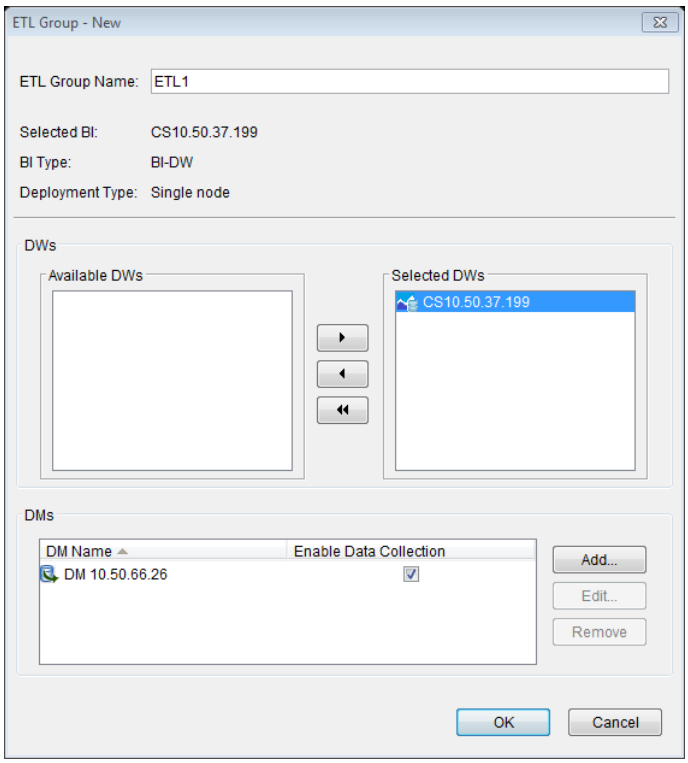


Figure 7-19: DMs Area of ETL Group – New

6. Click **OK**.

In the **ETL Groups** area of the **ClearSee System – New** dialog box, the ETL group appears.

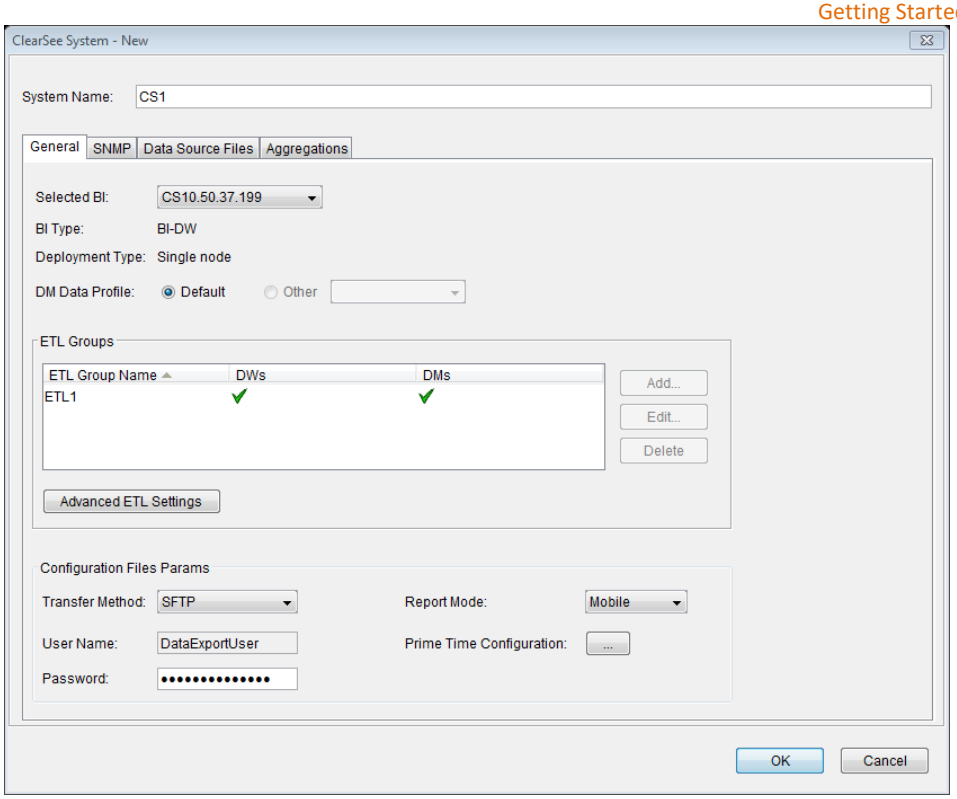


Figure 7-20: ETL Groups Area of ClearSee Systems – New

7.6 Adding your SMP Server

To add an SMP to the ACG:

1. In the Navigation pane, right-click Servers and select **New SMP** from the popup menu.

   OR

   Select Servers in the Network pane of the Navigation tree and then select **New SMP** from the Actions menu.

   The SMP Properties - New dialog is displayed.

2. Enter the Name and IP address (IPv4 or IPv6) of the SMP.
3. Select the **Enable SSL Between NetXplorer Server and Device** checkbox if you wish the connection between NetXplorer and the SMP to be more secure.

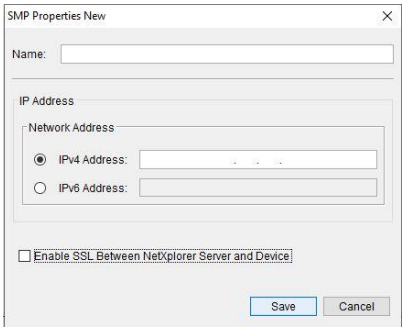


Figure 7-21: SMP Properties – New Dialog

Note: **The name defined for the new SMP cannot be left empty. It cannot be more than 128 characters long. The following characters are valid: abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890_ -@#^()+=[]{}**

Note: **If you have configured an HA SMP Cluster, you should enter the "virtual" IP address here (instead of the individual SMP Server IPs that make up the cluster).**

4. Click **Save**.

Complete information about using your SMP can be found in the SMP Installation and Administration Guide.

7.6.1 Verifying an SMP Configuration

To verify that an SMP server has been configured correctly, you can do the following:

1. In the Navigation pane, right-click the SMP server you have configured and select **Configuration** from the popup menu.

   OR

   Select the SMP Server in the navigation pane, and choose **Configuration** from the main View menu.

   The Configuration tabs appear in the Applications pane.

2. To view the SMP server configuration, click on the IP Properties tab:

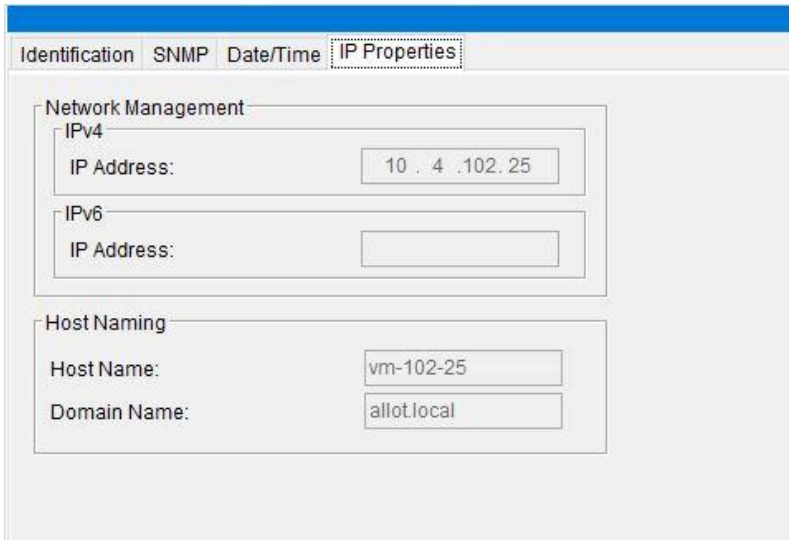
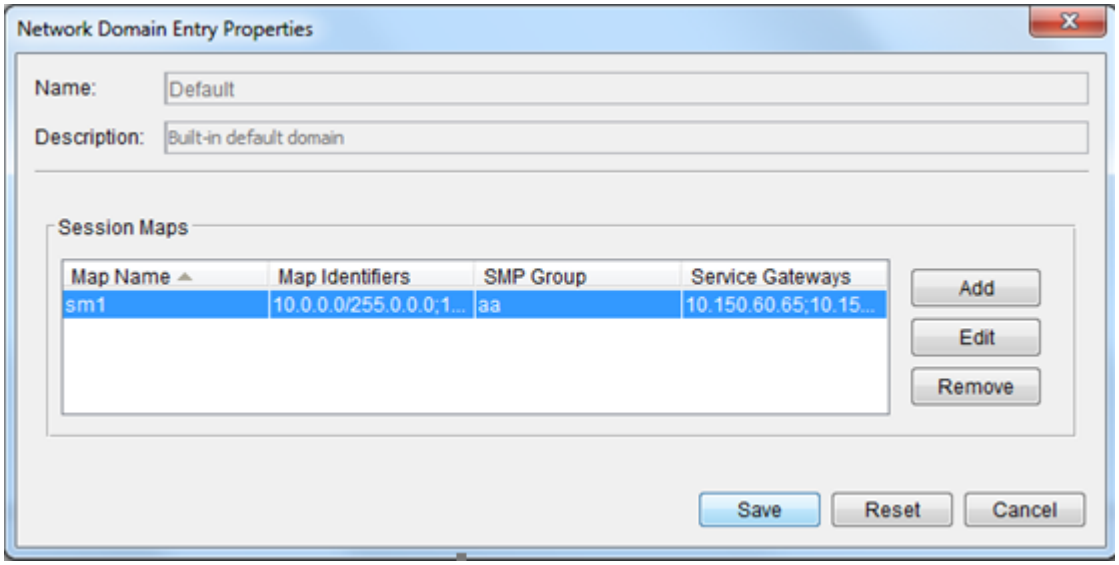


Figure 7-21: IP Properties of the SMP Server



7.6.2 Enabling Active Directory Support

Enabling Active Directory Support (Optional)

Allot's Active Directory Adapter (ADA) is a solution which enables Allot subscriber management services to be deployed in enterprise networks which use Microsoft Active Directory to manage their user authentication. Using Allot subscriber management capabilities, enterprise network administrators can monitor users' internet usage and enforce corporate policies concerning high-internet usage or control the network utilization of specific applications.

Note: **The ADA mechanism from SMP15.1 was completely refactored and improved. For further details of the changes consult with the 15.1 Software Release Notes.**

ADA associates user identification information with the IP address used and enables the application of traffic management policies on a per user basis (service plans). In order to operate, the Allot solution needs to be able to query security logs in the Active Directory Domain Server.

Note: **To this end, the Allot solution will need an AD user with wmic (Windows Management Instrumentation Command-line) for remove access and Security logs query privileges.**

The data flow of the solution was described in Chapter 1 above. The configuration of the solution consists of 6 steps, as described below:

Note: **Before beginning these 6 steps, ensure that the SMP has been added to the NetXplorer Navigation Tree as detailed here and that the SMP Group has been created in the NetXplorer as detailed here.**

Note: **It is important that the SMP is able to communicate to the Active Directory via FQDN. If needed edit the /etc/hosts file to make sure that the SMP is under the same domain as the Active Directory Server.**

- Step 1: Configure SMP to perform DHCP gleaning (Optional)
- Step 2: Configure AD Adapter file
- Step 3: Set policy source as Active Directory
- Step 4: Upload groups to NX UI
- Step 5: Create Service Plans and Add to Policy
- Step 6: Configure Active Directory Domain Server

These steps are described in detail below.

Step 1: Configure SMP to perform DHCP gleaning (Optional)

Configuring SMP to perform DHCP gleaning is an optional step. By default, if DHCP gleaning is not configured, SMP will receive an Active Directory login event which includes both user name and allocated IP. Any changes in IP due to lease expiration will not be identified however. In order to ensure that changes to the allocated IP are also recorded, you should setup the SMP to perform DHCP gleaning.

This is enabled by configuring DhcpConfig.xml and then configuring the smpGleaner.conf file (for out of band gleaning only) or configuring the Service Gateway to mirror packets (for in-band gleaning only). All of these steps are outlined earlier in the SMP Installation and Admin Guide in the section on DHCP Gleaning.

Step 2: Configure AD Adapter File

Follow the instructions below to enable the ADA and to enter the details of the Active Directory Domain Servers to be queried by the SMP. The active directory file is located in **/opt/allot/conf/ActiveDirectoryConfig.xml.** It can be configured by running the script below.

3. To enable the Active Directory Adapter, login to the SMP server and run the following script: **activeDirectoryCLI.sh -f enable**

Note: **If you wish to later disable the functionality, run: activeDirectoryCLI.sh –f disable**

4. To add the Active Directory Domain Controller attributes (Host IP, Domain Name, User and Password) to the SMP, run the following script:

   activeDirectoryCLI.sh -a -dip <DC_IP> -dname <Domain_Name> -user <AD_Admin_User> -pass <AD_Admin_Pass> -g <Default Domain Group with Quotation marks>

   For example, to add a Domain Controller with an IP of 10.10.10.10, with the domain name “allot.local”, a user name “aguero”, a password “200goals” and a default domain group called “Domain Users”, you would enter the following command:

   activeDirectoryCLI.sh -a -dip 10.10.10.10 -dname allot.local -user aguero -pass 200goals -g "Domain Users"

5. Restart the ADA process on the SMP by entering the following CLI command:
   activeDirectoryCLI.sh –reload

Step 3: Set Policy Source as Active Directory

Follow the instructions below to configure the SMP to use the Active Directory as a policy source (and to ensure that SMP is managing subscribers not sessions).

6. Open the RouterFlowRules.xml file. The file located in **/opt/allot/conf/RouterFlowRules.xml**.
7. In the **AdminParameters** section, make sure that “**QoSType**” is set to “**Subscriber**” and that **PolicySourceType** is set to “**ACTIVE_DIRECTORY**” as shown below

```
<?xml version="1.0" encoding="UTF-8"?>
<RouterFlowRules xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="RouterFlowRules.xsd">
    <ConfigurationVersion value="1"/>
```

```
<FlowRulesConfig>
    <FlowRuleList>
        <!--FlowRuleEntry RuleName = "">
            <ConditionList>
                <ParamEntry ParamName = "DATA_ACCESS_ID" Value = "Fixed_Access"/>
            </ConditionList>
            <ActionList>
                <ActionEntry Type ="AddParam" QosType = "Subscriber"/>
            </ActionList>
        </FlowRuleEntry> -->

    </FlowRuleList>
    <DefaultActionList>
        <ActionEntry Type ="AddParam" QosType = "Subscriber"/>
        <ActionEntry Type ="AddParam" PolicySourceType = "ACTIVE_DIRECTORY"/>
        <!-- <ActionEntry Type ="AddParam" ParamName = "" Value = ""/> -->
    </DefaultActionList>
</FlowRulesConfig>
</RouterFlowRules>
```

8. After configuring the RouterFlowRules.xml file, restart the smp_router process by entering the following command:

   keeperMgr –R smprouter

Step 4: Upload Groups to NX UI

Follow the instructions below to map between Active Directory Organization Units (groups) and Service Plans, and to set priority in case of conflict.

9. In the NetXplorer Navigation pane, right-click the Network and select Configuration from the popup menu

   OR

   Select Network in the NetXplorer navigation pane, and then choose Configuration from the Actions menu.

   The network tabs will be displayed in the Applications pane.

10. Select the SMP tab. The “General” sub-tab will appear. Towards the bottom of the sub-tab the “Active Directory Integration” pane is displayed. It may be necessary to minimize the “Alarms Log” in order to view this pane in full.

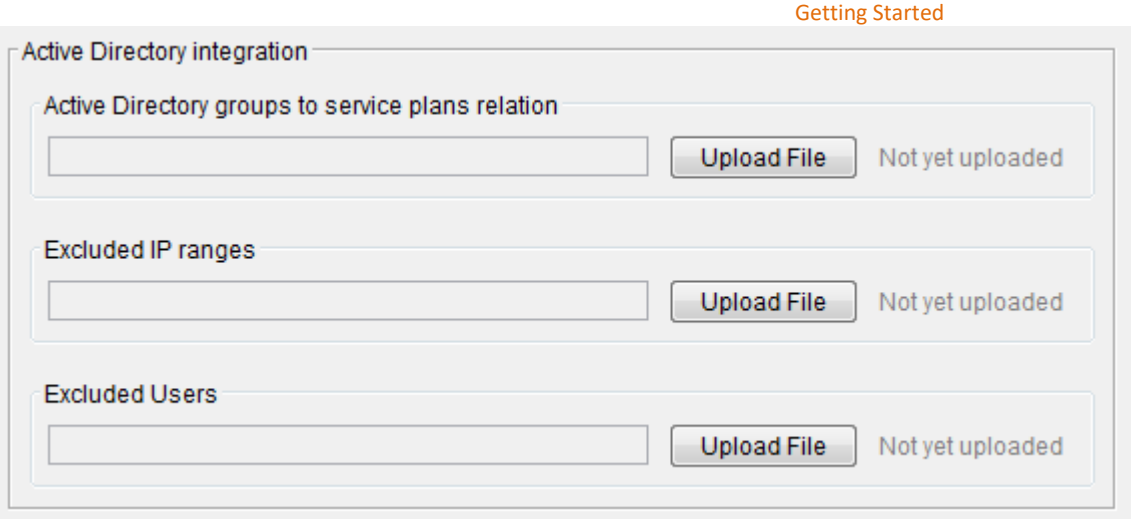


Figure 7-22: Active Directory Integration

11. Create a file to map groups to service plans. The file should be saved on the NX server in **.csv** format then uploaded to the NetXplorer by entering the path and clicking on the "upload file" button. Each line in the file should consist of group name, service plan name and priority, each separated by a comma as in the example below:

Group_1, ServicePlan_1, 45
Group_2, ServicePlan_2, 63
cs-all, cs, 27
all, all, 30

Note: **The service plan and group mapping is not case sensitive. Therefore if the active directory group is called "All" and the file uploaded includes "all" SMP will consider this to refer to the same group.**

The higher the number the higher the priority. Therefore referring to the example file uploaded above, if a user is a member of both "all" (priority 30) and "cs-all" (priority 27), that user will be mapped to the service plan associated with the "all" group.

12. If you wish to exclude certain ***IP ranges*** from being mapped to a service plan (e.g: IT servers), create an additional .csv file which lists the relevant IP range, as per the example below:

1.0.0.1-1.0.0.10
2.0.0.1-2.0.0.5

The file should be saved on the NetXplorer server in .csv format then uploaded to the NetXplorer by entering the path and clicking on the "upload file" button.

13. If you wish to exclude certain ***users*** from being mapped to a service plan (e.g: generic users), create an additional .csv file which lists the relevant user names as per the example below:

canada\user1
canada\user2
canada\user3

The file should be saved on the NetXplorer server in .csv format then uploaded to the NetXplorer by entering the path and clicking on the "upload file" button.

Step 5: Create Service Plans and Add to Policy

Now you should create service plans corresponding to the service plan names which you defined in the active directory group – service plan mapping file in step 4 above.

Full instructions for creating service plans and inserting them into the policy are contained in the SMP Installation and Administration Guide

Step 6: Configure Active Directory Domain Server

Finally you should configure the customer's Active Directory Domain Server in order to enable the AD Adapter on the SMP Server to access logon events from the security log.

AD configuration

Create a user account in the AD that will be used for the remote WMI queries. Join it to the following groups: **distributed COM users, event log readers.**

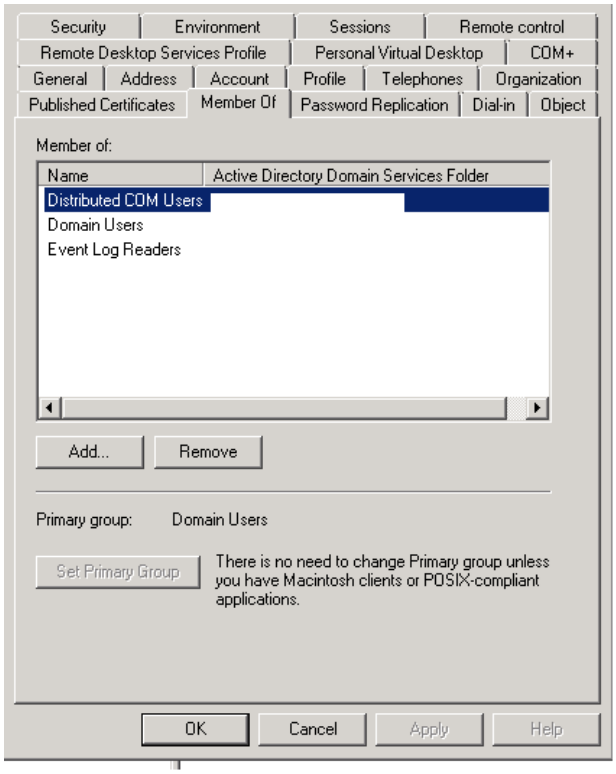


Figure 7-23: Active Directory Domain Server Configuration

Note: **Optionally, you can create a dedicated security group and grant permissions to that security group. Then you must add the user used by the SMP to that group.**

AD Domain Controller configuration

The SMP requires permissions to query all the Domain Controllers via LDAP and WMI. By default, those permissions are granted to domain admins, however if more strict permissions are desired, those permissions can be granted manually. Please note that those steps need to be executed on each DC in the domain. This includes any new DCs after they are promoted.

14. Login to the DC.
15. Run **wmimgmt.msc**
16. Right click on **wmi control** – click **security** and mark **root folder**
17. Add the relevant user (or group) and mark **allow** checkbox for **Enable Account** and **Remote Enable.**
18. Click on **Advanced**, select the user you just added, click **edit** and choose **apply to this namespace and subnamespaces**. Click **OK** several times to confirm the operation.

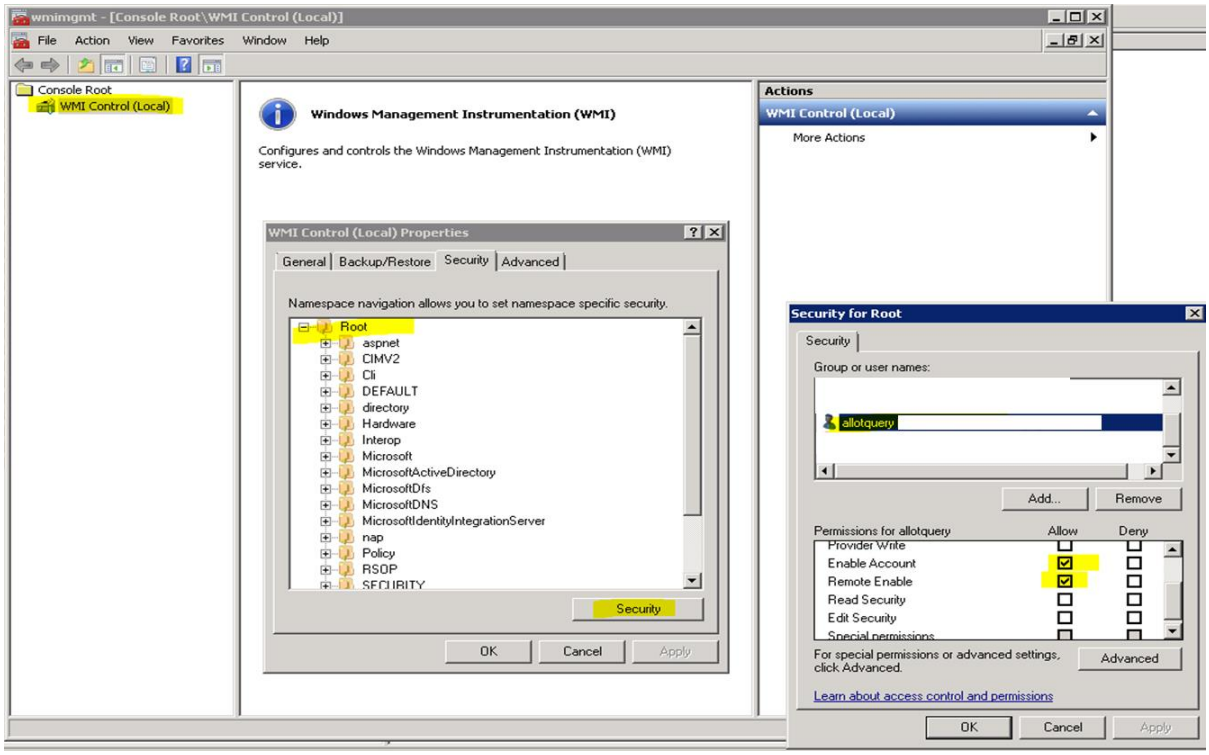


Figure 7-24: WMI Configuration on Active Directory Domain Server

Logging Events

To enable creation of the required event logs via Group Policy, you need to configure Advanced Audit Policy settings in a GPO that applies to all the DCs:

Computer configuration – polices – windows settings – security settings – advanced audit policy configuration – audit policies – logon / logoff

Enable **Success** and **Failure** for the following subcategories:

- Audit logoff
- Audit logon
- Audit network policy server
- Audit special logon

Note: **The legacy audit policy and the Advanced Audit Policy are incompatible and only one of them should be used at a given time. If the domain controllers are currently using the legacy Audit Policy, do not enable Advanced Audit Policy as it can break the auditing policy and cause unexpected results.**

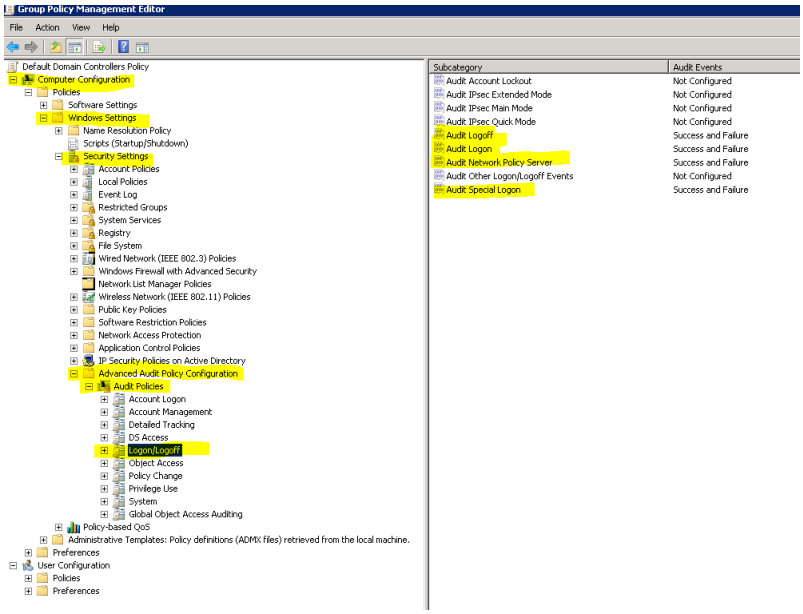


Figure 7-25: Group Policy Management Editor on Active Directory Domain Server

Firewall Configuration

The traffic between the SMP and the DCs is using DCE-RPC. This means that the communication is starting from port TCP 135 and then redirected to a random high port. If a firewall is deployed between the Allot server and the DC, it may be desirable to fix the high port for this traffic.

To fix the high WMI port, perform the following procedure on each DC:

19. Login to the DC
20. Open elevated command prompt
21. Run:
    winmgmt -standalonehost
22. Restart **Windows Management Instrumentation** service
23. This will fix the high port on TCP 24158. Note that TCP 135 is still required to be opened

8 Configuring the ACG for Visibility

The ACG monitors all your network traffic in real time and can keep you fully aware of such essential factors as application performance, capacity utilization, and network health. In addition, you can also keep an eye on what applications are actually being run on your network and mark traffic that may be a threat or is cutting into your valuable network resources.

The key to this visibility is Allot's ClearSee Network Metrics and its powerful, highly user-friendly GUI. Using the ClearSee dashboards you can look deeply into network, application, subscriber, device, and quality of experience data.

This chapter will give you a preview of the kind of information you can access quickly and easily with ClearSee using basic examples. To learn more about configuring and working with ClearSee to enjoy complete network visibility, see the ClearSee Operation Guide.

8.1 How to see what Web-based Applications your Users are Visiting

8.1.1 Step 1: Open the ClearSee GUI

1. In your browser, enter the ClearSee IP you set during installation. The login screen appears.

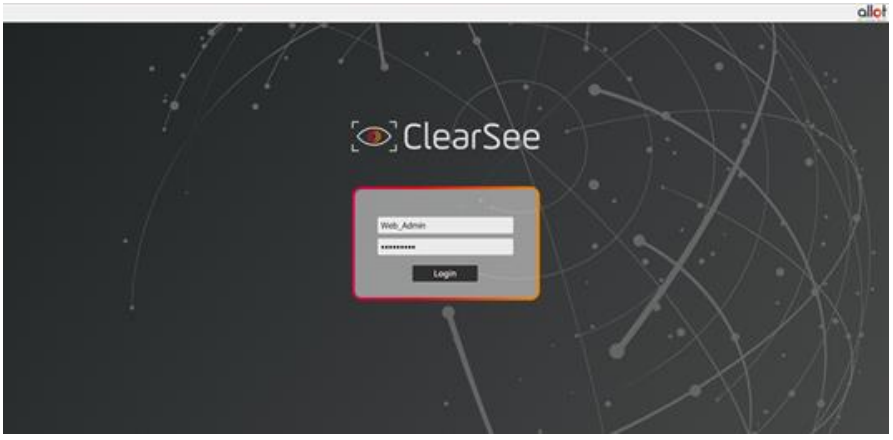


Figure 7-1: ClearSee Login Screen

2. Enter your User Name and Password and then click Login to open the ClearSee Dashboard.

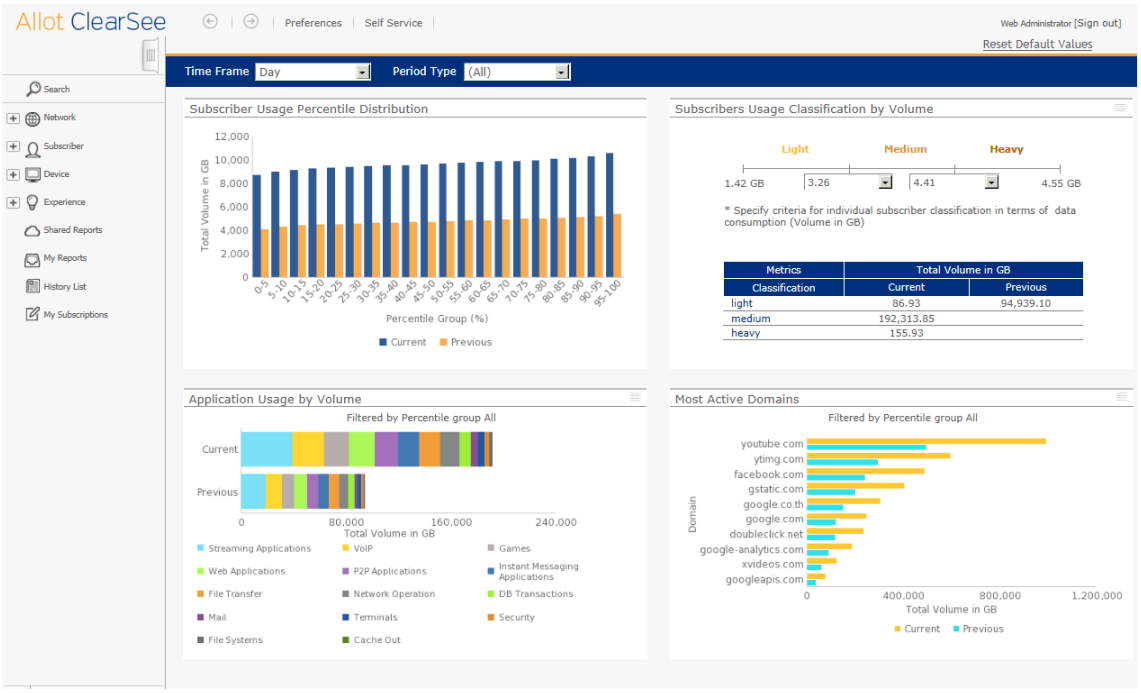


Figure 7-2: Main ClearSee Dashboard and Home Screen

NOTE **If you leave your computer, ClearSee times out after half an hour of disuse, and you will be prompted to re-enter your login credentials.**

8.1.2 Step 2: Examine the Applications Rank Report

1. Move your cursor to the left hand side of the screen to open the Reporting Panel.
2. Click on Experience and select Applications Trend.
3. The **Applications Trend** report identifies the applications responsible for the most traffic based on **Bandwidth** or **Unique Subscribers**, and displays traffic metrics for the applications.

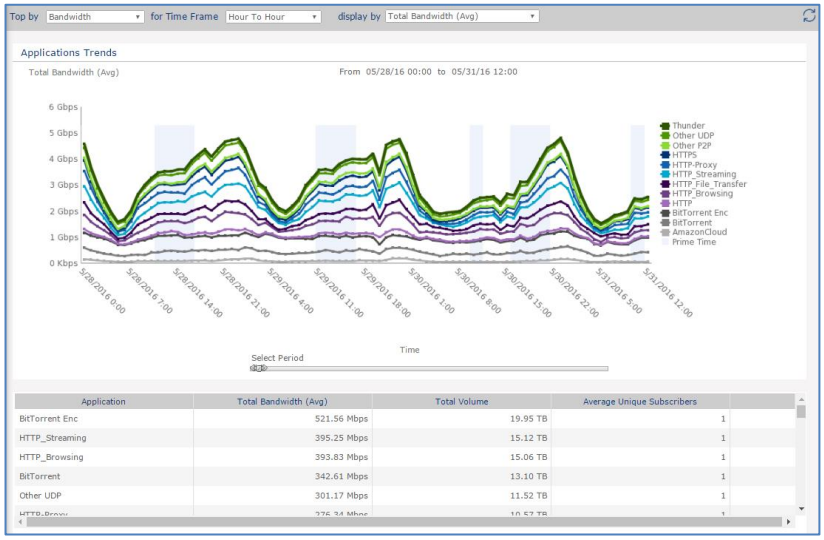


Figure 7-3: Applications Trend Report

For example, you can see here that BitTorrent and HTTP Streaming and Browsing are using up a good part of your Bandwidth, which you may wish to limit.

8.1.3 Step 3: Examine the Applications Trend Report

1. Move your cursor to the left hand side of the screen to open the Reporting Panel.
2. Click on Experience and select Applications Rank.
3. The **Applications Rank** report presents **Total Volume** and **Unique Subscribers** for the top applications on your network. It's useful for assessing which applications are trending highest in usage, and for understanding which applications are "expensive" in terms of volume per user.

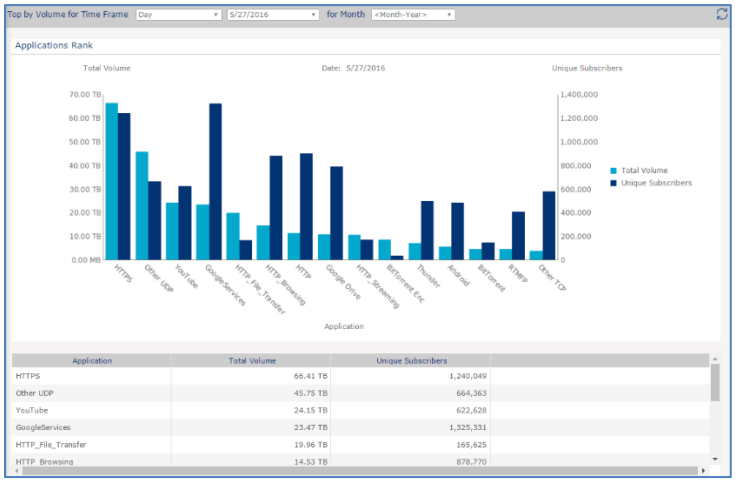


Figure 7-4: Applications Rank Report

In this example above, you can see that YouTube is using over 20 TB of network traffic with over 600,000 unique hits. These are numbers consistent with a large carrier so obviously an Enterprise will see much smaller numbers.

8.2 How to see what Websites your Users are Visiting

8.2.1 Step 1: Open the ClearSee GUI

1. In your browser, enter the ClearSee IP you set during installation. The login screen appears.

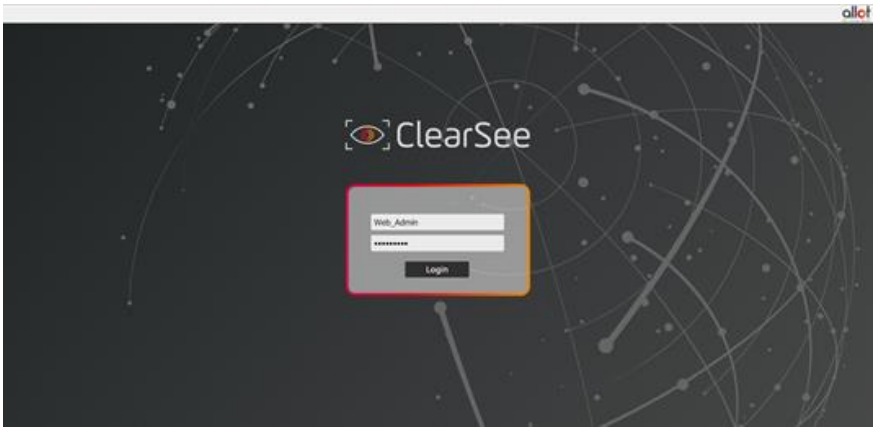


Figure 7-5: ClearSee Login Screen

2. Enter your User Name and Password and then click Login to open the ClearSee Dashboard.

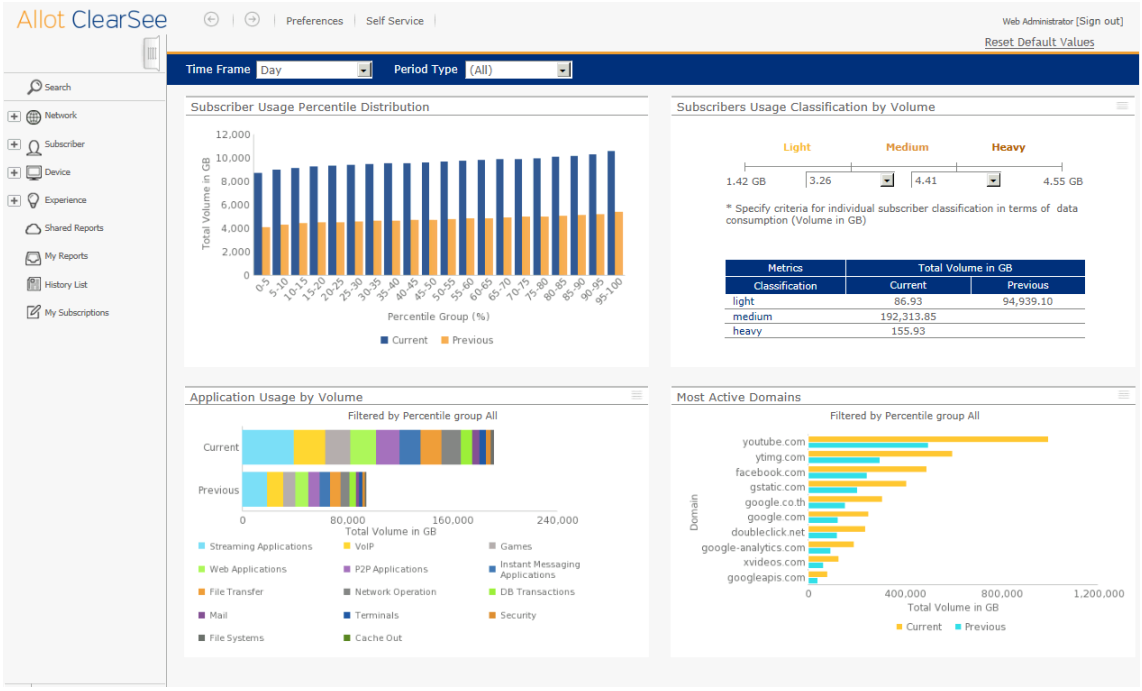


Figure 7-6: Main ClearSee Dashboard and Home Screen

NOTES If you leave your computer, ClearSee times out after half an hour of disuse, and you will be prompted to re-enter your login credentials.

8.2.2 Step 2: Examine the Most Active HTTP Domains Report

1. Move your cursor to the left hand side of the screen to open the Reporting Panel.
2. Click on Experience and select Most Active HTTP Domains.
3. The **Most Active HTTP Domains** report provides consumption metrics for the most active HTTP domains and for a selected period of time. Each bar is one of the most active HTTP domains on your network, and the taller the bar, the greater the domain rates in terms of the selected consumption metric.

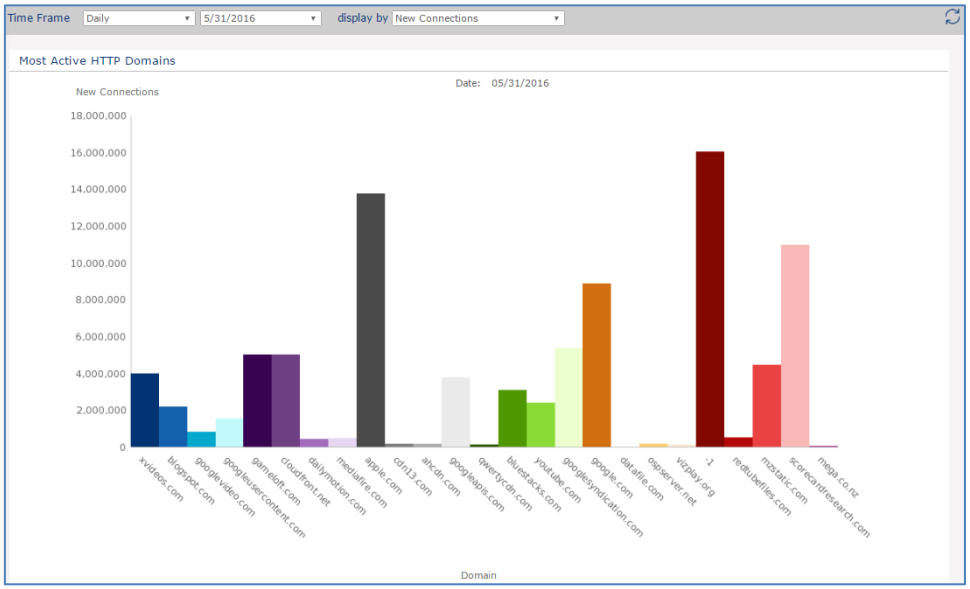


Figure 7-7: Applications Trend Report

4. For example, you can see that Apple.com and Google both see a great deal of traffic.

8.3 How to see the Traffic Statistics for a Line

NetXplorer monitors and controls a network that may include one or many Secure Service Gateways, including the SG-VE built into the ACG.

Traffic flowing through these in-line platforms falls into different pre-defined lines. Each line is further divided into Pipes that break down into Virtual Channels (VCs). Each Line, Pipe, or VC has a set of conditions that can be defined for it. When traffic flows through a Service Gateway, it is compared to the conditions you set for the first Line. If the conditions apply, the traffic is then tested against the conditions of each Pipe within that line. If the condition of the first Line does not apply, the traffic is not classified into the first Line; the packet is then tested against the conditions of the second Line.

The policy table always consists of at least one Line, the Fallback Line. This line is the last one listed in the Policy table, and its conditions are set to accept all traffic. Traffic that does not meet the conditions of any other Line is classified into the Fallback Line, and then into one of that Line's Pipes. The same classification takes place for Pipes within the Line and Virtual Channels within the Pipe. In each case, if no match is found, traffic falls into the fallback Line, Pipe, or VC. In this way every packet of internet traffic finds its home within a Line, a Pipe, and a Virtual Channel.

The fallback rule, marked with a palm icon, is like the palm of a hand, catching all unmatched traffic from higher rules.

8.3.1 Step 1: Open the ClearSee GUI

1. In your browser, enter the ClearSee IP you set during installation. The login screen appears.

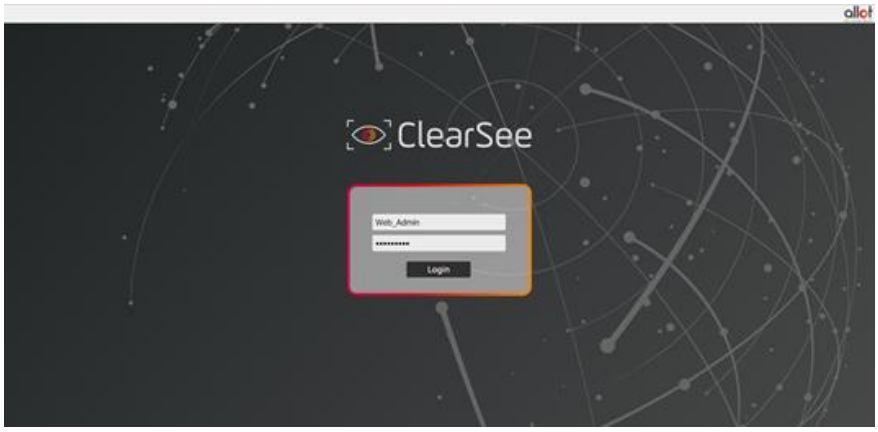


Figure 7-8: ClearSee Login Screen

2. Enter your User Name and Password and then click Login to open the ClearSee Dashboard.

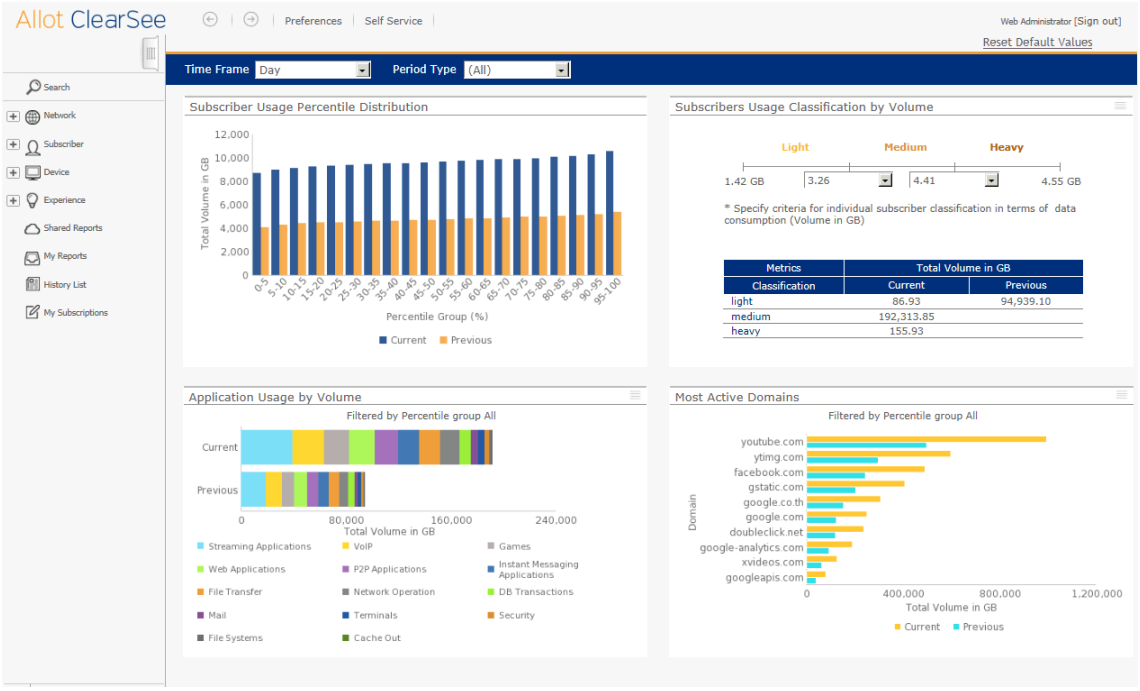


Figure 7-9: Main ClearSee Dashboard and Home Screen

NOTE **If you leave your computer, ClearSee times out after half an hour of disuse, and you will be prompted to re-enter your login credentials.**

8.3.2 Step 2: Examine the Policy Lines Dashboard

1. Move your cursor to the left-hand side of the screen to open the Reporting Panel.
2. Click on Network and select Policy Lines. A list of the ACGs on your network appears in the Available list.

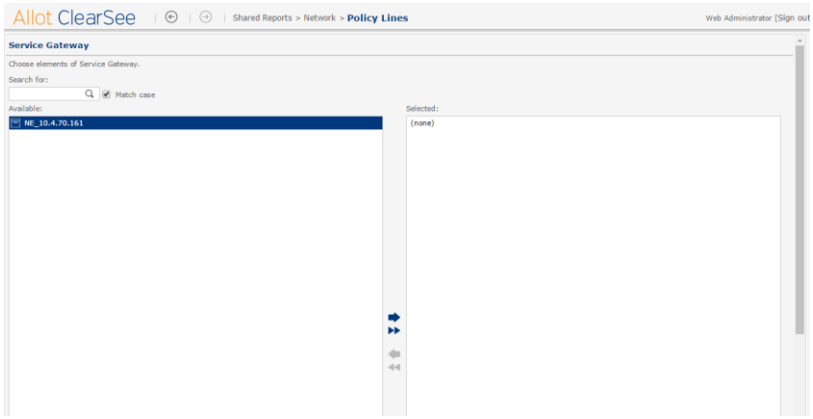


Figure 7-10: ClearSee Service Gateways

Click on your ACG and use the arrow button to move it to the Selected list.

3. Click the Run Document button at the bottom of the screen to open a list of the Lines on that ACG.
4. Click one or mores Line and use the arrow button to move them to the Selected list.
5. Click the Run Document button at the bottom of the screen to open the Policy Line Daashboard.
6. The **Policy Lines** dashboard presents network traffic for the lines in your network that you select, including information on which Pipes are carrying the most traffic, the traffic trends over the last 5 minutes and a list of each selected Line with essential traffic data.

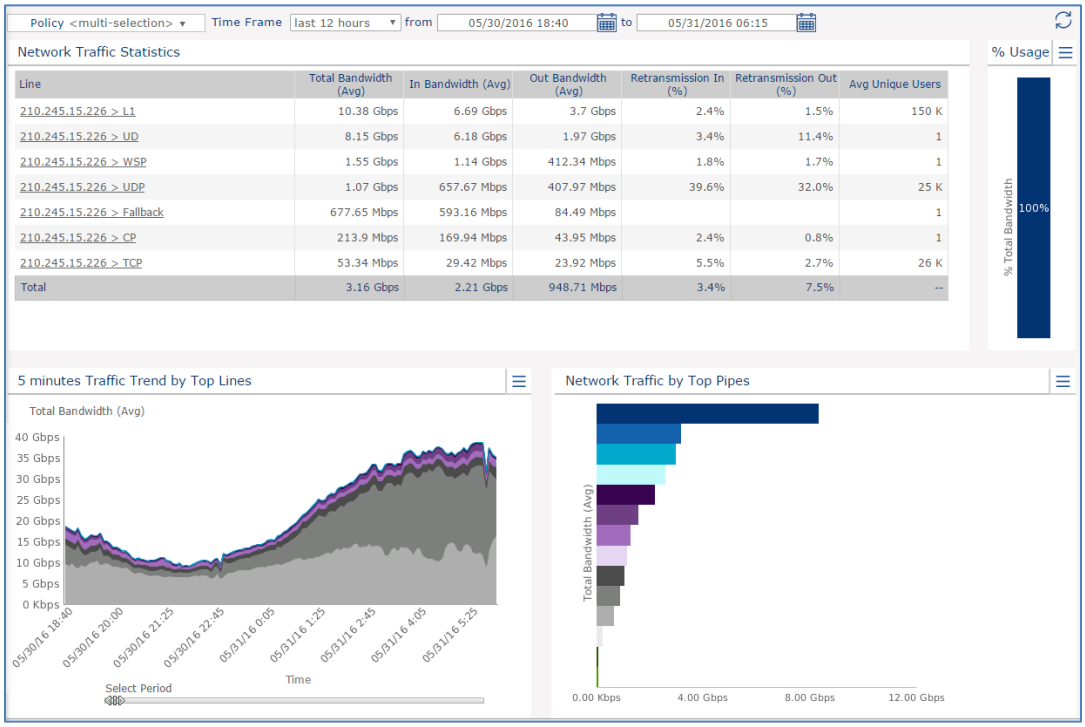


Figure 7-11: Line Dashboard

9 Configuring the ACG for Control

Using NetXplorer you can create a Policy to shape your network, ensuring that your critical applications and valuable users get the priority they need in a resource-limited network.

Right out of the Box, the ACG Default Policy can help any Enterprise take control of their network traffic. However, as your network needs grow, the ACG Policy can be configured in order to be more specialized for your specific needs using the Policy Editor found in the NetXplorer GUI. In addition your Policy can be tweaked to define Acceptable Use Policy for your entire network or on a per-user or department basis.

The key to controlling and managing traffic is creating the right Policy, and then adjusting the Conditions for each Policy Element. This control can be very broad, perhaps affecting your entire enterprise, or as specific as managing the traffic of each user in multiple offices by IP address (or User Name if you have deployed SMP).

This chapter will give you a look at ways to use NetXplorer to manage your network using basic examples. To learn more about configuring and working with NetXplorer to control your network, see the NetXplorer Operation Guide.

9.1 How to Expand your Network Policy

One method of using your NetXplorer Policy Editor to control your Network is to create a Line representing each Branch. You can then create Pipes representing each department and VCs representing each desk, for example. In the same way you can manage the traffic of a single large office by having each Line represent a department, or a floor of offices. Using NetXplorer the control is in your hands.

9.1.1 Step 1: Create the Required Hosts

In the Host catalog, create Hosts to represent the locations and users you will need for your Policy. For example you can create a Host for the IP range used by each office, then one for each department in each office, and finally if you wish, a Host to represent each IP.

For more instructions on how to create Hosts, see Chapter 6, Step 4 or the NetXplorer Operation Guide.

9.1.2 Step 2: Create your Policy

1. In the Policy Editor, right click an Element in the Enforcement Policy table and select **Insert Line/Pipe/VC** from the Actions menu. Remember that you can only create the same kind of element that you have clicked. For example, to create a Line click on an existing Line.

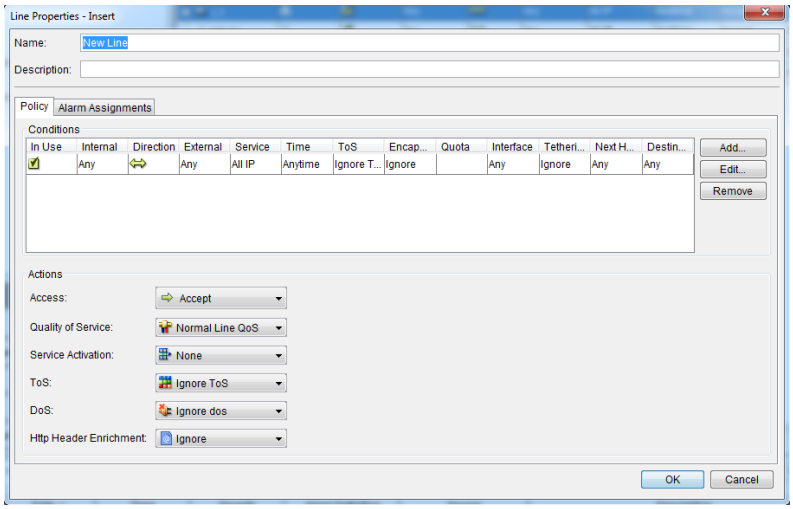


Figure 8-1: Insert Line Dialog – Enforcement Policy Tab

2. First, let's create a new Line. Enter a new name for the Line, if required. Assigning a logical name to the Line helps you to classify your traffic, such as Branch 1, or London.
3. Now in that Pipe, click on the Fallback Pipe and select Add Pipe. Do this for each Department you wish to set up with its own Pipe. For example, the Line London may now have two Pipes, Marketing and Sales.
4. Finally, in that Pipe, you can create VCs for each desk or user. For example, you can create three VCs in the Marketing Pipe of your London office and call them Steve, Carol, and Tim (or Manager, Rep 1 and Rep 2).

9.2 How to be Sure your Users get the Network Resources they Need

Once the Policy structure has been created you can then set the Quality of Service for each Line, Pipe or VC, ensuring that each department and user gets the bandwidth that they need. You do this by working with NetXplorer's versatile Quality of Service (QoS) Catalog to add Actions to your Policy elements. Once traffic is classified and distributed into the correct Line, Pipe or VC, the QoS you wish for that traffic is applied as an Action automatically.

9.2.1 Step 1: Create QoS Catalog Entries

You will need to create entries in the QoS Catalog before adding them to the Policy. For example, let's look at how this is done for a Line.

1. In the NetXplorer GUI, open the Catalogs panel in the Navigation Pane and right-click **Quality of Service.** Select **New Line Enhanced QoS** from the popup menu.

NOTES **If you are creating a QoS for Pipes, select New Pipe Enhanced QoS here, or if you are creating a QoS for VC select New VC Enhanced QoS.**

Use only Enhanced QoS entries, those that are not Enhanced are not supported by the ACG.

The Line Enhanced QoS Entry Properties dialog is displayed.

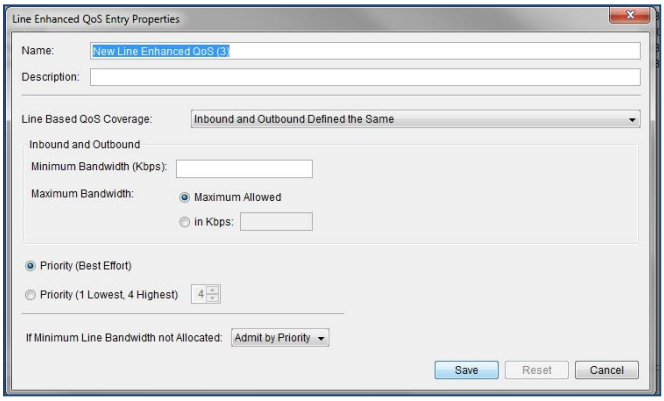


Figure 8-2: Line Enhanced QoS Entry Properties

2. Edit the name and description of the entry, if required.
3. From the **Line-based QoS Coverage** dropdown list select one of the options:
   - Inbound and Outbound Defined the Same: Define QoS for both the inbound and outbound traffic together. This option is normally used in a symmetric environment where inbound and outbound traffic requirements are identical.
   - Each Direction Defined Separately: Define QoS for the inbound and outbound traffic individually (instead of the General tab, the Inbound tab and the Outbound tab appear).
4. In the **Inbound and Outbound** area, define the Quality of Service as follows:

- (Optional) In the Minimum Bandwidth (Kbits/sec) field, enter the minimum bandwidth that will be assigned to the Line. As long as there is traffic requiring bandwidth in this channel, the bandwidth allocated will never be lower than this limit.
- (Optional) In the Maximum Bandwidth field, you may opt to assign this Line the maximum Bandwidth allowed, to enter the maximum bandwidth that will be assigned to the Line in Kbits/sec, or to enter a percentage of all the Bandwidth going through the NetEnforcer or Service Gateway to assign to the Line. The total bandwidth of all traffic allocated in this Line will not exceed this limit.
- Select Priority (Best Effort) or complete the Priority field by selecting a priority between 1 and 4 (highest). If all objects in the same Enforcement Policy level are set to Best Effort there will be no prioritization between objects. The more traffic an object requires, the more bandwidth that will be allocated to it, subject to the amount of free bandwidth available.

NOTE **Allot does not recommend using Priority (Best Effort) if other elements have Priorities 1 to 4 assigned. In such situations an element which has been assigned Priority (Best Effort) may receive a very low percentage of the available bandwidth.**

- Configure the action to be taken if minimum bandwidth is not available, by selecting one of the following options from the designated dropdown list:
  - **Admit by Priority**: Accept the new connection, but do not assign the minimum bandwidth. The new connection gets bandwidth per priority.
  - **Drop**: All packets are dropped. The user is disconnected and may see the message Connection timed-out.

NOTE **The Drop option is provided for environments such as UDP where a client does not expect acknowledgements (ACKs).**

5. Click **Save.** The new entry is saved in the QoS Catalog.
6. Repeat this for every QoS level you wish, on Lines, Pipes or VCs. For example you may wish to create three different levels of QoS, one with a very high maximum bandwidth level, one with a medium level and one with a very low bandwidth level. Or you can create them based on different priority levels.
   Remember that you need to create different QoS Catalog Entries for the Line, Pipe and VC levels.

9.2.2 Step 2: Assign QoS to the Policy

Now to make certain that each Line, Pipe or VC always gets the right amount of bandwidth, modify the Quality of Service in the Actions of the Line. The default value is Normal Priority.

7. Open the Policy Editor and select the Line, Pipe or VC you wish to assign a Quality of Service to.
8. Right click in the QoS column and select one of the QoS Catalog Entries you already created.
9. Repeat this for all Lines, Pipes or VCs you wish to configure.
10. Click Save to apply your changes.

In this way you can decide which Users or Departments have highest priority when it comes to traffic bandwidth, as well as making sure that your mission critical offices or users always have enough bandwidth, while limiting the bandwidth available to those offices which don't need as much.

9.3 How to Manage what Applications your Users Access

In today's Enterprise there are many activities and applications competing for bandwidth and your users's attentions. In addition, many IT departments are fighting the growth of "shadow IT" applications which are particularly prevalent where a company operates a BYOD policy. You can use NetXplorer to limit those distractions and ensure that your network resources are not misused.

For example, if you don't wish your users in one or all offices to be able to access Facebook, you simple create a VC in each Pipe that specifically controls Facebook traffic by assigned a Service in the Conditions of that VC.

9.3.1 Step 1: Create a New VC

11. Click on an existing VC in one of the Pipes in your Network (you can use the Fallback VC if you have no others) and select Insert Virtual Channel to open the Virtual Channel Properties – Insert dialog.

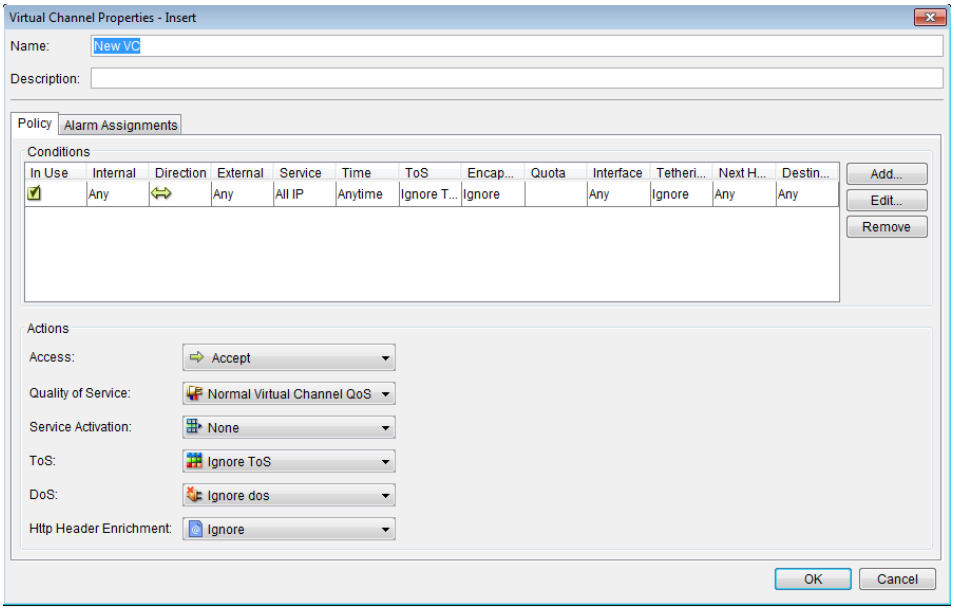


Figure 8-3: Virtual Channel Properties

12. Enter a name for the VC, such as Facebook.

9.3.2 Step 2: Set a Condition and Action for the VC

13. Double click on the Service field of the default condition (currently set to All IP) to open the list of Services.
14. Go to the Web Applications folder and click the + to expand the list.
15. Scroll down and click on Facebook. Note that the Service column now lists Facebook rather than All IP. All Facebook traffic that goes through this Pipe will not be directed to this VC.

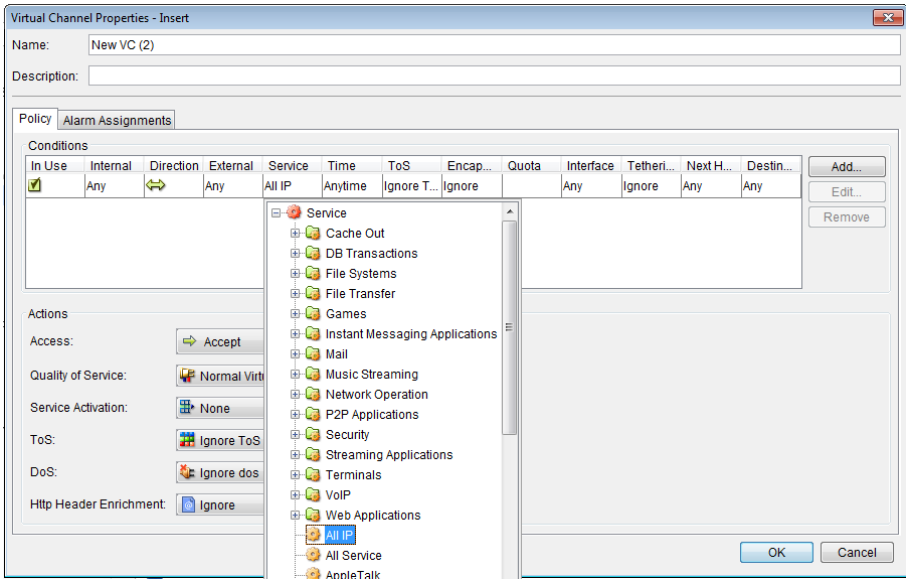


Figure 8-4: Virtual Channel Properties – Service Condition

16. You can now select an Action in the lower portion of the dialog to determine what happens to the Facebook traffic.
    For example you can select Drop or Reject from the Access drop down list to stop all Facebook traffic from reaching your users in that Pipe.
    Another approach would be creating a VC QoS entry (similar to what we did above) with a very low maximum bandwidth or priority and assigning that to this VC in the Quality of Service field.
17. When you are done, click OK, then select Save in the menu bar to apply your new changes.
18. If you wish the same VC to apply to multiple to Pipes you can create the same VC in each, or if there are a large number use the VC Template feature which you can find described in the NetXplorer Operation Guide.

10 Configuring the ACG for Security

Allot's ACG uses DDoS Secure to make use of application and traffic visibility and control to prevent attacks and enable users to use the Internet and cloud applications safely and productively by filtering web content, defending against viruses attacks and stopping phishing e-mails before your users even see them.

This chapter will give you a look at ways to use DDoS Secure to tackle some web security needs using basic examples. For more information on using and configuring DDoS Secure, see the DDoS Secure Operation Guide and DDoS Secure Installation and Administration Guide.

10.1 How to Mitigate Incoming and Outgoing Attacks

10.1.1 Step 1: Configure DDoS Secure Basic Settings

Before you get started, a DDoS Secure must have an IP address, default route, a hostname, a time zone and an NTP server. For systems with DNS, a domain name and a DNS server are also required. In the following procedures, the user's input will be **bold**. Specific variables that need to be adjusted for every installation will be *italicized.*

1. Access the device using the SSH Admin log in and password
2. Switch to SSH Root user with the following command

```
su -
```

3. Enter the root password and then press **<Enter>**
4. At the shell prompt type **cli** to enter the CLI utility

```
SPC-3-46:~# cli
SPC-3-46]
```

5. At the CLI prompt type **configure** to enter configuration mode

```
SPC-3-46] configure
SPC-3-46(config)]
```

6. At the CLI configuration prompt, set up IP addressing and routing for the administration network

```
SPC-3-46(config)] ip address 10.0.1.10/24 default-route 10.0.1.1
```

The default route is automatically checked for connectivity through the administration network.

7. Set up host and domain name for the appliance

```
SPC-3-46(config)] hostname ctrl
ctrl(config)] ip domain-name allot.example.com
```

8. Configure the IP address of the DNS server (repeat if multiple DNS servers are used)

```
ctrl(config)] ip dns-server 10.0.5.1
```

9. The DNS setting is automatically verified. When installing an SPC, publicly available NTP servers registered in the DNS as pool.ntp.org are also automatically tried. If the servers aren't reachable from this network, a WARNING line appears.
10. It is also possible to manually define the NTP server. The maximum stratum level accepted is 14.

```
ctrl(config)] ntp-server 10.0.5.2
```

11. Configure the system time zone

NOTE Pressing the <TAB> button expands the list of built in time zones.

```
ctrl(config)] timezone Asia/Tel_Aviv
```

12. Exit the CLI configuration mode and reboot the appliance

```
ctrl(config)] exit
ctrl] system reboot
```

After setting the Network Parameters, consult Chapter 3 of the DDoS Secure Installation and Administration Guide for information on other basic configuration elements such as adding sensors or managing users.

10.1.2 Step 2: Create DDoS Secure Groups and Policies

Creating Groups

Subnet groups, or simply groups, are the basis for all traffic classification within Allot DDoS Secure. All flood detection and traffic statistics gathering is done on a per-group basis.

Every IP packet received by the DDoS Secure is seen as coming from a group and going into a group, based on its source and destination IP addresses. Each group is defined as a named set of IP subnet prefixes (e.g., 10.144.22.0/23). No multiple groups can include the same prefix. If an IP address of a host matches a prefix in a group, the IP address and the host are said to belong to that group, or be in the group.

For information on creating Groups, see Chapter 4 of the DDoS Secure Installation and Administration Guide.

Creating a DDoS Secure Policy

For a notification of an attack to be sent, a policy must be configured. A policy consists of filters and actions. A policy is a collection of filters (also called conditions), Actions perform something when all of the conditions match an event, for example, an email can be sent or event importance can be changed or subscriber plan can be changed via the SMP. To successfully send notifications, both filters and actions must be configured in a policy (policy will not send any notifications if there are no conditions and, obviously, it won't send any notifications if there are no actions configured). An Action will be performed only if ALL conditions match an event.

For more information on DDoS Secure Policies, see Chapter 5 of the DDoS Secure Installation and Administration Guide.

10.1.3 Step 3: Prepare the DDoS Secure GUI

The DDoS Secure GUI is accessible using a web browser. HTTPS access is required to work with the DDoS Secure GUI.

Open up your browser and browse to **http://<DDoS Secure Controller IP>/webui.** You will be presented with the main login screen. Enter your DDoS Secure GUI username and password.

Once you have successfully logged in you will see a screen similar to the one below. The level of detail available may be limited by the rights your administrator has granted.

NOTES The GUI requires a resolution of 1024x768.

The administrator can control user access with fine granularity and may limit access to specific DSS units and specific groups. For more information see the DDoS Secure Installation and Administration Guide.

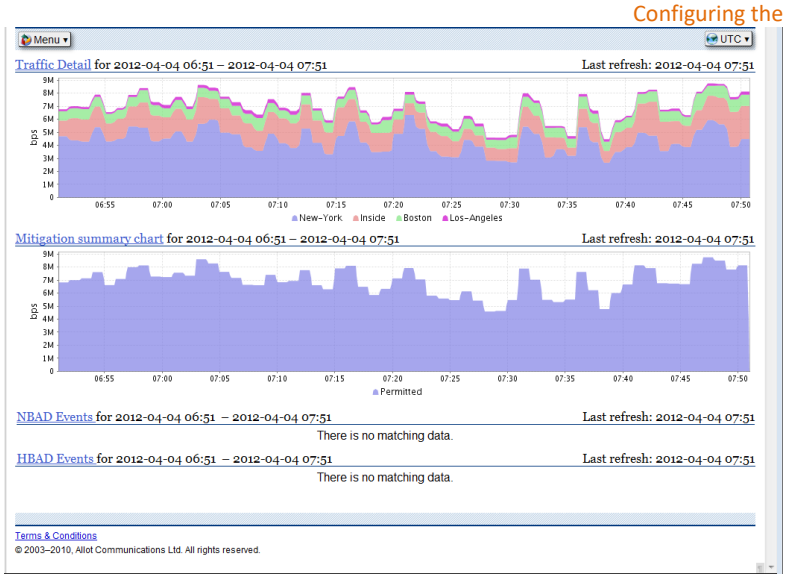


Figure 9-1: DDoS Secure Start Page

Upon login, you are presented with a preset Start Page displaying the last hour of traffic, a Mitigation summary chart, and the active & inactive events at this time. This page displays a snapshot of what's going on at this moment. The screen auto refreshes every few seconds.

The name of each section (**Traffic Detail** for example) is clickable and links to the appropriate page or chart.

10.1.4 Step 4: Defend Against Incoming Attacks with NBAD Mitigation

NBAD is Network Behavioral Anomaly Detection. NBAD technology in the DDoS Secure is used to detect incoming DDoS attacks. NBAD detects incoming attacks, or Floods, usually resulting from infected machines on the internet or on your own network.

Once a flood is detected, the **sensor** will do a packet capture and run an analysis on it. If the flood is long enough, subsequent captures occur every 3 minutes to the max tracking time of one hour.

To see any incoming attacks, select NBAD from the main menu and click Activity.

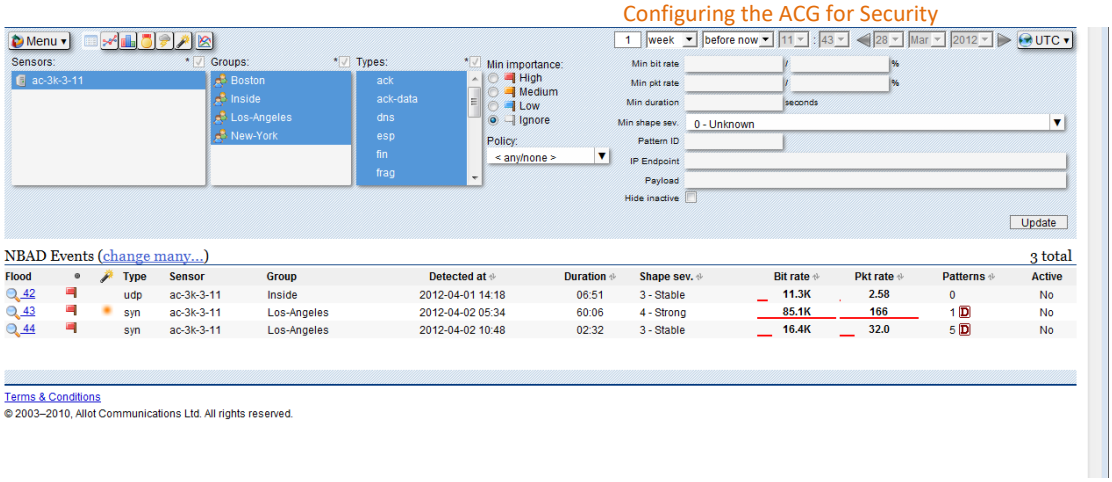


Figure 9-2: NBAD Activity View

The dynamic packet filtering feature responds dynamically to attacks detected in the network.

Once an attack is detected, a signature is created in the DDoS Secure and packets matching the signature are filtered out before DPI classification and actions (QoS and steering) take place.

For information on understanding and mitigating NBAD attacks, see Chapter 5 of the DDoS Secure Installation and Administration Guide.

10.1.5 Step 5: Defend Against Outgoing Attacks with HBAD Mitigation

HBAD - Host Behavioral Anomaly Detection - detects the infected machines in your network launching attacks, to stop outgoing attacks.

Typically these are workstations infected with botnet software, and they are identified according to their behavioral patterns. Infected machines frequently demonstrate huge numbers of connections to the network, and these profiles are used for detection.

The DDoS Secure monitors all of the traffic on the network with users put into groups by IP address (see above).

To see any outgoing attacks, select HBAD from the main menu and click Activity.

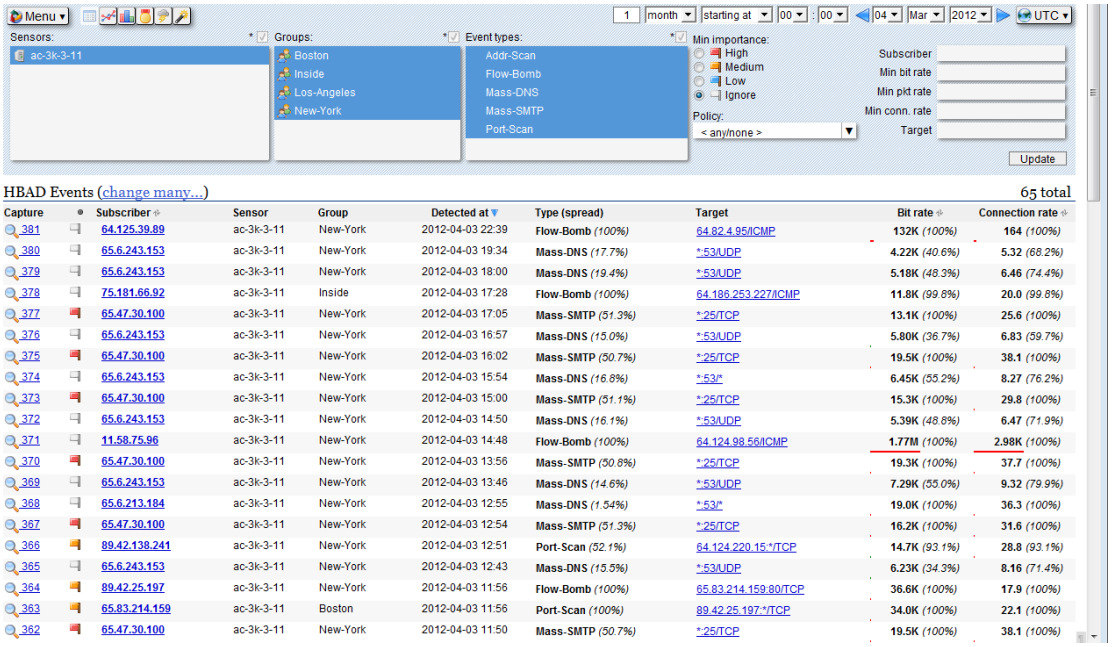


Figure 9-3: HBAD – Activity View

These attacks can then be mitigated making use of policies created in the NetXplorer and then implemented on the SMP, to ensure that outgoing attacks are blocked before they leave your network.

For information on understanding and mitigating HBAD attacks, see Chapter 6 of the DDoS Secure Installation and Administration Guide.

11 Shutting Down the ACG2000

The ACG2000 can be shut down at any time by running the following command from the CLI:

```
shutdown
```

Any user with superuser privileges can power down the system.

All the modules of the ACG will independently restart themselves when the system is turned back on. This process can take up to 30 minutes to complete.

12 Reinstalling the Software

If you are advised by Allot Global Support Services (GSS) that you need to reinstall your ACG2000 software, use the following procedure to restore the software, then use the Deployment Wizard as described in Section 4.

NOTE You must be logged in with Superuser privileges to complete this process.

1. Enter the root directory by typing:

```
# cd /
```

2. From the command line, run the following command to stop all installed Modules running on the ACG2000 server:

```
# stop
```

3. Delete all modules from the server by running the following command

NOTE This command is the point of no return. After running it, you MUST do a full reinstallation of the ACG2000 software to continue using ANY of the Modules.

```
# clean
```

4. From the command line, type:

```
# cd /opt/allot
```

5. Check the Allot Knowledge Base to ensure you download the most current software version, and then type the following as a single line.

```
# wget -nv -r -np -nH --cut-dirs=3 -R index.html
ftp://10.110.10.52/SIO/16.5.510_B36/ACG2000_<CURRENT
VERSION NUMBER>/ --user XXX --password XXX
```

The software will consist of the following files:

- allotplatform.tgz
- allotplatform.ver
- install.py

```
[root@aio12 allot]# ll
total 59091840
-rw-r--r--  1 root  root  60510014187 May 24 13:46 allotplatform.tgz
-rw-r--r--  1 root  root           34 May 24 13:47 allotplatform.ver
-rwxr-xr-x  1 root  root        23124 May 24 13:47 install.py
drwxr-xr-x  3 root  root           20 May 21 13:16 logs
drwxr-xr-x. 2 admin allot          39 May 26 06:39 products
```

6. Run the following commands to install:

```
# chmod 755 install.py
# python install.py -m install -p sio -f
ACG2000_<CURRENT VERSION NUMBER>.tgz
```

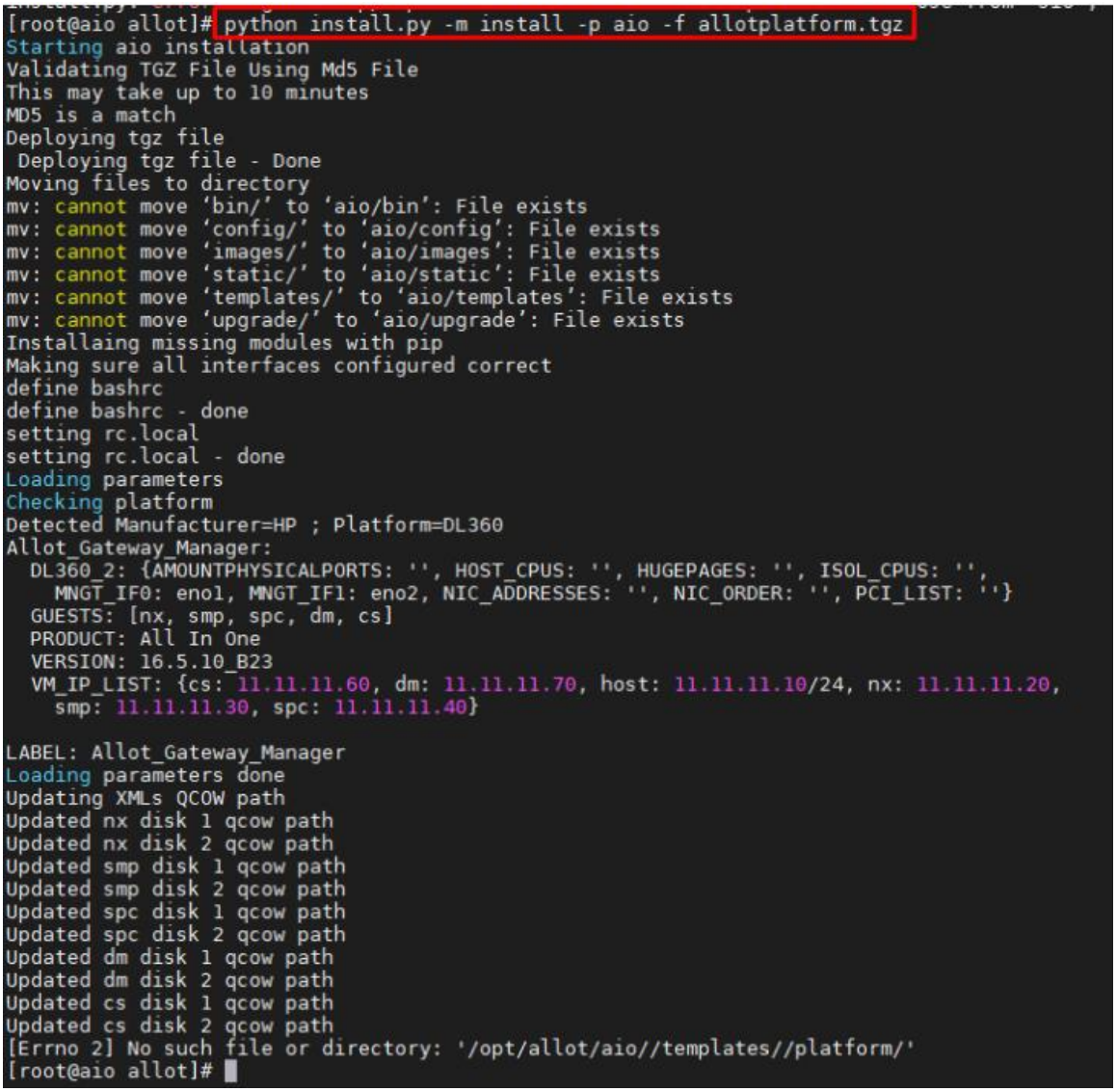


Figure 11-1: install.py Output

7. To check installation progress, type:

```
# ls /opt/allot/sio/images/
aos  cs  dm  nx  smp  spc README.md
```

After completing the above procedure, follow the steps in Chapter 4, “Deploying the Modules”, to finish configuring your ACG2000.

Appendix 1: The Bypass

Bypass and Physical Network Set-up was covered extensively in Chapter 4. For the entirety of the setup, the example was used of the HD 8 Copper Bypass Unit. The HD 8 Copper is not the only Bypass Unit compatible the with ACG2000. No matter what Bypass you choose to use, make sure you refer back to Chapter 4 for setting up the equipment. While the ports types and layout may differ between Bypass models, the networking layout stays the same.

Ensure that when your ACG and Bypass Unit arrive, the Bypass, transceivers, and any included network cables are all of the same type. Make sure you have WAN and LAN cables of the same type as well, for connecting the Allot equipment into your network. It is not possible to mix cable types on a single Bypass Unit.

The ACG2000 hardware only offers support for two links. As such, only two links will be used on the Bypass Unit, no matter how many links the Bypass is capable of supporting.

Bypass Options for the ACG2000

The table below details the three Bypass Units that are compatible with the ACG2000.

PRODUCT NUMBER	DESCRIPTION	SUPPORTED INTERFACES
SG-BP-EXT-8P-MM-A	HD 8 Multi-Mode Fiber Bypass	1G, 10G
SG-BP-EXT-8P-SM-A	HD 8 Single-mode Fiber Bypass	1G, 10G, 40G, 100G
SG-BP-EXT-8P-COP-A	HD 8 Copper Bypass	1G

The HD 8 Bypass Unit (previously known as the Allot Multi-Port Bypass) works in conjunction with the ACG2000 and is available with copper, Single Mode Fiber or Multi Mode Fiber interfaces and with RJ45 or Dual-LC connectors.

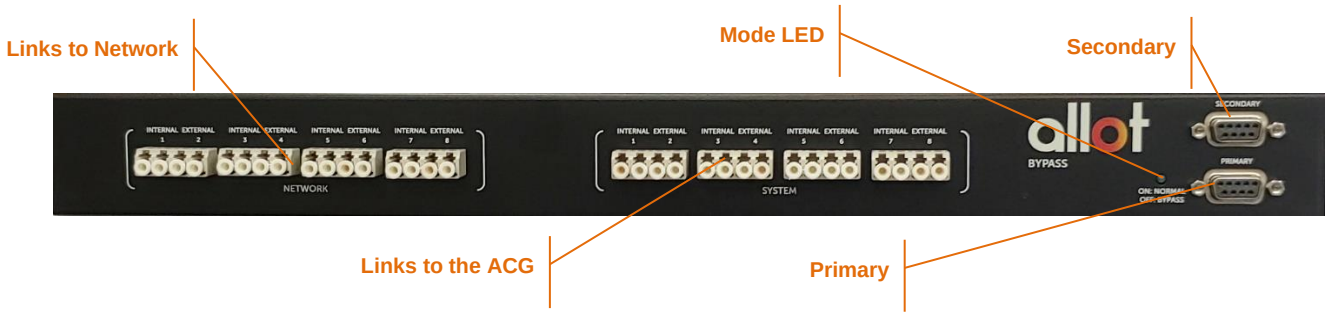


Figure Appendix-1: HD 8 Single-Mode Fiber Bypass Unit (Dual LC)

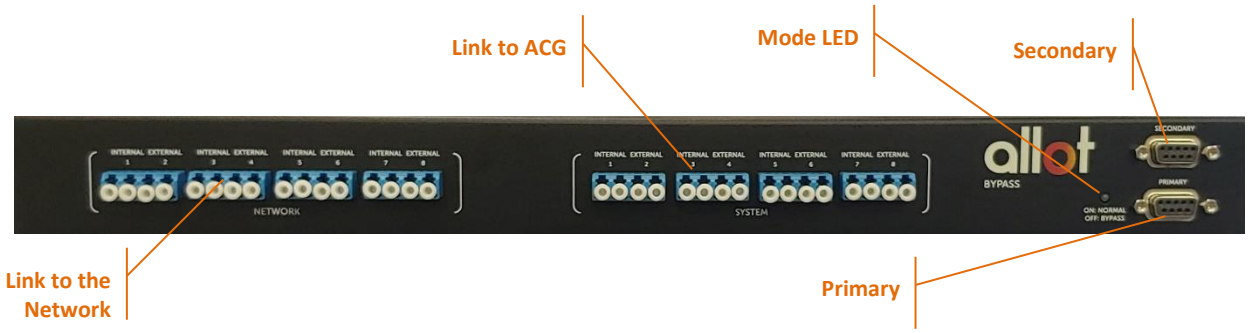


Figure Appendix-2: HD 8 Multi-Mode Fibre Bypass Unit

Figure Appendix-3: HD 8 Copper Bypass Unit

NOTE **Use Multi-Mode 50µm or Single-Mode 9µm fiber optic cables CROSS with LC-LC Duplex connectors (not provided) to connect ports of the switch and the router.**

HD 8 Bypass Unit LEDS Description

The following indicators can be used to identify the operation of the blade:

- **Mode LED** is **STEADY GREEN** when the Bypass Unit is operating normally and **OFF** when the Link is in Bypass mode.

HD 8 Bypass Unit Front Panel Connectors

- **Network Ports 1-4** connect to your network. Be sure to insert the Internal and External connectors into the correct ports on the Bypass Unit. In addition please note that in fiber Bypasses, on each Duplex LC connector on the Bypass unit's front panel the Tx connector is the left LC connector and the Rx is the right LC connector.
- **System Ports 1-4** connect to the SG. Be sure to insert the Internal and External connectors into the correct ports on the Bypass Unit. In addition, please note that in Fiber Bypasses, on each Duplex LC connector on the Bypass unit's front panel the Tx connector is the left LC connector and the Rx is the right LC connector.
- **Primary** connects to the USB port on the SG
- **Secondary** is not in use.

Appendix 2: Hardware Specifications

The ACG2000 is, as of July 2020, available on two slightly different hardware platforms. Both take the form of HPE DL360 1U rack servers. While the capabilities of the two hardware platforms (herein referred to as revision or rev. 1 and 2) differ, the ACG2000 suite has been shown to offer consistent performance regardless of hardware revision.

Identifying Your ACG2000 Hardware

The hardware can identify itself to you remotely via a command line procedure. After identifying the revision of your ACG2000, you can examine its specifications on the appropriate table of specifications below.

To remotely identify the hardware revision used by your ACG2000:

1. Log into the iLO. For more details, see Logging into the iLO
2. Enter the following command:

```
getinfo -S | grep "Product Name"
```

The terminal will return the name of the hardware.

- ACG2000 rev. 1 is built on HPE DL360 Gen9 servers and identifies as such in the command line.
- ACG2000 rev. 2 is built on HPE DL360 Gen10 servers, and will identifies as such in the command line.

ACG2000 Hardware Information

ACG2000 Revision 1	
Part	Specs
CPU	2 x Intel Xeon – 14 Core, 2.4GHz, 35MB L3 Cache, 120W
RAM	8 x HPE 16GB DDR4, 2400MHz, CAS-17-17-17
HDD Storage	6 x 300GB HDD, 12Gb/s SAS interface, 15000rpm
Power Supply	2 x 800W Flex Slot Platinum, Hot-swappable
ACG2000 Revision 2	
Part	Specs
CPU	2 x Intel Xeon Gold – 16 Core, 2.3GHz, 22MB L3 Cache, 125W
RAM	8 x HPE 16GB DDR4, 2933MHz, CAS-21-21-21
HDD Storage	5 x 480GB SDD, SATA interface
Power Supply	2 x 800W Flex Slot Platinum, Hot-swappable