Appliance User Guide

nAppliance Networks

Release 01/04/2009

Version 1.0.20

NAPPLIANCE APPLIANCE PRODUCT END USER AGREEMENT

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS. BY INSTALLING AND USING SOFTWARE AND HARDWARE INCLUDED WITH THE NAPPLIANCE PRODUCT, YOU (THE 'END USER') ARE AGREEING TO BE BOUND BY THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, IMMEDIATELY RETURN THE PRODUCT TO NAPPLIANCE INC.

1. CERTAIN DEFINITIONS

1. "nAppliance Appliance" means the nAppliance hardware and software that includes, without limitation: licensed software, hardware, support, and professional services.

2. "Open Source Software" means software included in the nAppliance Appliance which is licensed and made available under the terms and conditions of the GNU General Public License version 2.

3. "Licensed Software" means nAppliance Proprietary Software and Open Source Software together.

4. "nAppliance Proprietary Software" means nAppliance proprietary software that may be included in the nAppliance Appliance, including enhancements, updates, bug fixes and upgrades thereto that may be provided to End User from time to time.

2. LICENSE

(a) License Grant. Subject to full payment of all applicable fees and to the terms of this end user agreement (the "Agreement"), nAppliance hereby grants to End User, a non-transferable, non-exclusive license to use the Licensed Software and related product documentation (the "Documentation") with the nAppliance Appliance for the duration of the Agreement. This license allows the End User to install the nAppliance Appliance on a network supporting the number of active nodes specified by the nAppliance Appliance Purchase Agreement. nAppliance shall have the right to conduct audits periodically upon advance notice to verify compliance with the terms of this Agreement.

(b) License Restrictions. End User may use the Licensed Software solely with the nAppliance Appliance. Except as otherwise

permitted by the GNU General Public License version 2, End User agrees not to modify, translate, reverse engineer, de-compile or disassemble the Licensed Software; or to create derivative works based on the Licensed Software.

(c) Other Restrictions. End User agrees to safeguard copies of the Licensed Software against disclosure, copying or use by unauthorized persons. End User agrees that it will not use, or allow use of, the nAppliance Appliance for any improper purpose (including without limitation, testing the integrity of any network other than those it is authorized to test). End User agrees that it will not, and will not allow, reverse engineering of the hardware included in the nAppliance Appliance. End User shall ensure that the provisions of this Agreement are not violated by End User's employees, contractors or agents. End User agrees to indemnify nAppliance for any third party claims related to the breach of this or any other provision of this Agreement by End User, its agents, contractors, or employees.

(d) Open Source Software. The use distribution and modification of Open Source Software is governed by the terms and conditions of the GNU General Public License version 2 which can be viewed at http://gnu.org and which is hereby incorporated by reference. Copies of the source code for Open Source Software may be obtained by contacting nAppliance via email at source@nAppliance.com. nAppliance may charge End User a fee equal to its cost for copying and distributing such source code. Nothing in this Agreement is meant to modify or supercede any terms and conditions of the GNU General Public License version 2 and if there is a conflict between the Agreement and the GNU General Public License version 2, the terms of the GNU General Public License version 2 shall control.

3. TITLE

End User acknowledges and agrees that all right, title and interest in the Licensed Software and Documentation, including all intellectual property rights therein, is retained by nAppliance or its suppliers, subject only to the license granted to End User hereunder. This license is not a sale and does not transfer to End User any title or ownership in or to the Licensed Software or the Documentation.

4. MAINTENANCE

End User shall have the option of purchasing maintenance services from nAppliance for a fee. Maintenance may include the following:

(a) Software Updates. Software updates will be provided by nAppliance at its sole discretion to End User from time to time. Updates may include software enhancements, upgrades, minor updates, and bug fixes.

(b) Hardware Repair or Replacement. For End Users purchasing maintenance services, nAppliance will use commercially reasonable efforts to repair or replace defective hardware within two (2) business days in accordance with the terms of the hardware warranty set forth in Section 4 (b) of this Agreement. End User is responsible for returning defective hardware to nAppliance within seven (7) days of receipt of replacement hardware. If nAppliance does not receive returned defective hardware within seven days nAppliance may charge End User the cost of the replacement hardware, such charges to be invoiced by nAppliance to End User in accordance with Section 7.

(c) Support. nAppliance will provide phone and email support to End Users Monday-Friday between 7:00 a.m. and 5:00 p.m. Pacific Time. nAppliance will use commercially reasonable efforts to reply to support requests within one (1) business day.

(d) Technical Support Incidents. End Users who purchase maintenance are entitled to twelve (12) technical support incidents per year. Support for technical support incidents above twelve (12) per year will be provided on a time and materials basis.

(e) Bug Fixes. The discovery of errors in the nAppliance Appliance ("Bugs") by End user shall not be deemed a technical support incident. Bugs should be promptly reported via email by End User to nAppliance at bugs@nAppliance.com. nAppliance will use commercially reasonable efforts to fix Bugs in a timely manner.

(f) Other Technical Support. Additional technical support services are available, at nAppliance's discretion, on a time and materials basis.

5. LIMITED WARRANTY

(a) Software. nAppliance warrants to End User only that the media on which the Licensed Software is recorded shall be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date of shipment by nAppliance. End User's sole and exclusive remedy, and nAppliance's sole and exclusive liability, shall be replacement of the media in accordance with this limited warranty.

(b) Hardware.

(i) Limited Warranty. nAppliance warrants only to End User that hardware furnished to End User under this Agreement will be free from defects in materials and workmanship for a period of ninety (90) days following shipment by nAppliance. nAppliance's sole and exclusive liability and End User's sole and exclusive remedy under this section 5(b) is to, at nAppliance's sole discretion, repair or replace without charge any non-conforming hardware. nAppliance shall repair or replace such hardware within a reasonable time period. Returned hardware and parts shall become nAppliance's property. End User agrees to assist nAppliance in identifying the circumstances under which the hardware failed.

(ii) Warranty Exclusions. The warranty under this section 5(b) does not apply to any hardware that has been subjected by End User or a third party to: (a) operating or environmental conditions contrary to nAppliance's specifications, (b) damage, misuse or neglect, (c) improper installation, repair or alteration, (d) modifications, other than by nAppliance, or (e) third party software, firmware or hardware that interferes with operation of such hardware. This warranty also excludes expendable items, such as fuses or other similar parts that fail from normal use.

(c) WARRANTY DISCLAIMER.

(i) The licensed software and documentation is provided "as is." except for the limited warranties granted in sections 5 (a) and (b), nAppliance expressly disclaims and negates all warranties for the nAppliance appliance, whether expressed, implied, statutory or otherwise, and nAppliance specifically disclaims any implied warranties of merchantability, fitness for a particular purpose, non-infringement of intellectual property or other violation of rights. nAppliance does not warrant that the nAppliance appliance will meet end user's requirements or that the operation of the licensed software will be uninterrupted or error free.

(iii) Some states or countries do not allow exclusion or limitation of incidental or consequential damages or limitation on how long an implied warranty lasts, so the above limitations or exclusions may not apply to End User. This warranty gives End User specific legal rights and End User may also have other rights, which vary from state to state or country to country.

6. LIMITATION OF LIABILITY AND DAMAGES

(a) In no event shall nAppliance, its suppliers or its distributors be liable for any indirect, special, incidental or consequential damage, including without limitation, loss of data, lost profits or cost of cover arising from the use of the nAppliance appliance, or any defect in the nAppliance appliance, however caused and on any theory of liability. This limitation shall apply even if nAppliance, its suppliers or its distributor shall have been advised of the possibility of any such damage. In particular, but without limitation, nAppliance, its suppliers and its distributors shall have no liability for the loss of any information stored or communicated or attempted to be stored or communicated within any system using the licensed software.

(b) The maximum aggregate liability of nAppliance and its suppliers for any claim arising out of use of the nAppliance appliance, or any defect in the nAppliance appliance, on any and all theories of liability, including without limitation negligence by nAppliance, shall in all events be limited to return of the amounts actually paid to nAppliance for the defective licensed software or hardware, less depreciation of such amounts linearly over a three-year period, which the parties agree constitutes a reasonable rate of depreciation.

7. FEES

End User shall pay to nAppliance the fees for the nAppliance Appliance in effect at the applicable delivery date requested by End User in accordance with the nAppliance Appliance Purchase Agreement, and nAppliance shall invoice End User for all such fees. nAppliance may increase fees at its discretion, provided that fee increases will not be effective until 30 days after notice to End User. All payments due hereunder to nAppliance shall be paid to nAppliance not later than thirty (30) days following the date of the applicable invoice. In addition to the fees, End User will pay all charges, including without limitation transportation charges, insurance premiums, and shall be responsible for all taxes (except nAppliance's U.S. income taxes), duties, costs of compliance with

export and import controls and regulations, and other governmental assessments.

8. TERMINATION

This agreement shall continue in effect until terminated hereunder. This Agreement may be terminated by nAppliance upon 30 days notice to End User. This Agreement shall terminate automatically if End User fails to pay fees when due and such failure is not remedied within fifteen days of the original payment due date. In addition, this agreement shall terminate automatically on End User's failure to comply with any of the restrictions and provisions herein, including without limitation any attempt to transfer this license. Upon any termination of this agreement, End User agrees promptly to destroy or return to nAppliance all copies of the Licensed Software and Documentation, including without limitation all original and archival copies thereof. No refunds shall be given for such returned materials. Notwithstanding any termination of this License, the rights and obligations set forth in section 3 (Title), section 5 (Limited Warranty), section 6 (Limitation of Liability and Damages), section 7 (Fees), section 8 (Termination) and section 9 (Miscellaneous) shall survive such termination.

9. MISCELLANEOUS

End User may not assign this Agreement without the consent of nAppliance. Any attempted assignment by End User shall be null and void. nAppliance may freely assign this Agreement. No delay, failure or waiver by either party to exercise any right or remedy under this Agreement shall operate to limit, preclude, cancel or waive any exercise of such right or remedy or the exercise of any other right or remedy. This Agreement shall be governed by and construed in accordance with the laws of the State of California without regard to conflict of laws principles or the United Nations 1980 Convention on Contracts for the International Sale of Goods. The federal and state courts of California shall have exclusive jurisdiction and venue to adjudicate any dispute arising out of this Agreement, and End User expressly consents to the personal jurisdiction of the state and federal courts of California .If any provision in this Agreement shall be found or be held to be invalid or unenforceable in any jurisdiction in which this Agreement is being performed, it shall not affect the validity of the remaining portions of the Agreement. This Agreement constitutes the entire agreement between the parties and supercedes

any prior agreement, whether written or oral, relating to the subject matter of this Agreement.

TABLE OF CONTENTS

About This Guide

Document Objectives
This document introduces the nAppliance appliance hardware and software systems and provides an overview of its features. The nAppliance appliance platforms are a combination of technologies that are integrated into a single infrastructure product.

Audience
This guide is for the IT administrators which are managing network, server or security environments.

Feedback
nAppliance Networks appreciates any comments, complaints or suggestions. Your opinion on what is right or wrong with this document is very helpful. You can contact nAppliance directly via email at:

support@nAppliance.com

Please include the document name and version.

Document Organization
This document includes the following sections:

- Chapter 1, “Introduction”, provides a general overview of the nAppliance functionality
- Chapter 2, “LCD Console”, provides an overview of the nAppliance LCD console, its features, and usage
- Chapter 3, “OneFace Web Console”, details the OneFace Web Console and remote administration of the appliances

- Chapter 4, “IPMI Network Based Management Interface”, introduces the IPMI based Lights Out Management interface and the hardware sensor reporting features
- Chapter 5, “FFRS Appliance Management Functions”, describes how to manage and configure appliances with the built-in recovery environment
- Appendix 1 is the port layouts for each hardware model.

Online Version

The latest release of this document can be retrieved via the nAppliance website at:

http://www.nAppliance.com/support/library.asp

Chapter 1: Introduction

The nAppliance hardware platform provides a powerful and reliable computing platform for various integrated software infrastructure products or applications. Using the nAppliance appliance infrastructure has the following advantages:

- System designed specifically to provide the optimum performance for the specific embedded application
- Headless design – nAppliance systems have a built in LCD sceen and keyboard, where the appliance can be installed locally by existing non-technical personal without complex cabling or configuration
- Centrally managed – nAppliances systems can be accessed and managed at the console level over the network from a central location
- Built in backups – nAppliance systems have a return to factory defaults or a return to last good configuration options built into the appliance, where by a simple local or remote command, the system can be rebuilt or restored to a prior snapshot
- Web console – Each appliance has a web based console interface. This allows an administrator to connect remotely to the system over the HTTPS protocol and manage the installation and configuration process.

The combination of the IPMI remote console functionality, the embedded Flash Based Recovery System, and the OneFace Web Console, the nAppliance environment can be completely managed remotely over a network connection .

Chapter 2: LCD Console

Many of the nAppliance models have an LCD console and keyboard located on the front of the appliance. The LCD provides a built-in computer console and keyboard, which allows the administrator to easily attach the system to the network, and configure the system network configuration without the need to attach a monitor, mouse and keyboard, or attempt to attach to the serial console.

The appliance is configured with a built-in static IP address. This IP address can be used to initially communicate with the appliance, or the administrator can configure the system's IP network for DHCP or with a static IP address from the LCD console. Once the system is on the IP network, the appliance is manageable remotely via a web console or via other interfaces available to the host operating system such as SSH or Windows Terminal Services.

The typical installation steps are:

1. Mount the appliance and install the power cord. Plug Ethernet into the Internal port on the back.
2. From the LCD Console, assign either a DHCP address or a static address. The interface can be changed later from DHCP to static.
3. On the LCD display, the IP address will be displayed. Use this IP address to attach to the appliance remotely.
4. Using the OneFace web console, the appliance can then be configured for use on the company network from your desktop remotely.

LCD Console Usage

The LCD Console has six butons. Arrows for moving through menu or display screens, an Enter button and a Cancel button.

Pressing a Right or Left arrow button will move the cursor through data etnry fields. Using the Up and Down arrows will move you through different menu selections.

The Enter button is to select and process the menu selection.

The Cancel button will cancel the operation and move you back up the menu tree.

Secure and Non-Secure modes

By default the LCD menu is in a non-secure mode. In this mode, the user can display basic stastics about the hardware such as network configurations and monitoring statistics.

To access the statistics screens, press the down arror and the display will loop through the available screens.

These statistics screens will display automatically, waiting for several seconds on each screen, then rotating through the rest of the screens. This gives local administrators the ability to see at a glance the operation of the system and see any alerts discovered by the monitoring system within the system.

LCD Operation

The following functions are available on the LCD console:

Default rotating display menu

Several statistic screens are displayed and can be rotated through by pressing the down arrow.

Secure menu – The secure menu can be accessed by pressing the CANCEL button. This will bring up a display which prompts you for your security code. The default value for this code is 1221. This should be changed during installation.

The secure menu items are:

- **Security**
- **N/W Configuration**
  - **<Interface Name 1>**
  - **<Interface Name 2>**
    - **…**
    - **Enable DHCP**
    - **Set IP**
- **Services**
  - **Microsoft Firewall**
  - **Network Connections**
    - **Stop | Start**
    - **Restart**
- **System Status**
  - **CPU Status**
  - **LAN Status**
- **Shutdown**
- **Restart**
- **Reset Password**

Security
This menu item allows you to change the security access code to access the secure menu inside the LCD menu. This can be changed to any 4 digit code the customer desires.

N/W Configuration
This function allows you to set the IP network configuration. The menu items allow you to:

1. Set the interface to DHCP. This will enable DHCP on this port and the port will automatically receive an IP address.
2. Manually set a static IP address on this port.

When the Manual IP address is set, the menu displays

IP Address
Subnet Mask
Default Gateway

The screen will display the default address 000.000.000.000 or the current defined value on these fields. These values can be changed by pressing the UP/DOWN arrows. The Right/Left arrows allow you to move from character to character. Once the value is set, press the ENTER button to save the configuration.

These value can be examined by reviewing the LAN Status screens on the LCD menu.

Services

Microsoft Firewall – this function allows you to disable or enable the Windows builtin firewall service

Network Connections – this function allows you to stop, start or restart the network services.

System Status

CPU Status – this function displays the number of CPUs on the system, and the current CPU usage.

LAN Status – this function displays each interface name, the IP address and the Sent/Received bytes actual usage counters.

Shutdown

This function shuts down the operating system and turns off the appliance.

Restart

This function reboots the operating system running on the appliance.

Reset Password

This function allows an operator to reset the operating system system password to a preset default value. The factory default password is nAppliance13. For the Windows operating system, the local administrator password is reset.

This default password can be set by the customer by editing an XML file.

The file path is:
“C:\Program Files\nAppliance\LCDservice 2.2\LCDsettings.XML”
(the LCDservice version number may vary).

The portion of the XML file to change is:

```
<ADMIN_PASSWORD>
        <ENABLE_PASSWORD_RESET>1<\...>
<DEFAULT_ADMIN_PASSWORD>nAppliance13</…>
</ADMIN_PASSWORD>
```

If a site security policy does not allow this functionality, this function can be disabled. To disable this function, change the ENABLE_PASSWORD_RESET value to 0.

Chapter 3: OneFace Web Console

The nAppliance OneFace is an nAppliance proprietary web console which is hardware and application aware and allows the system administrator to fully interact and manage the hardware and software configurations from a remote web interface.

From the Web Console, the administrator can manage

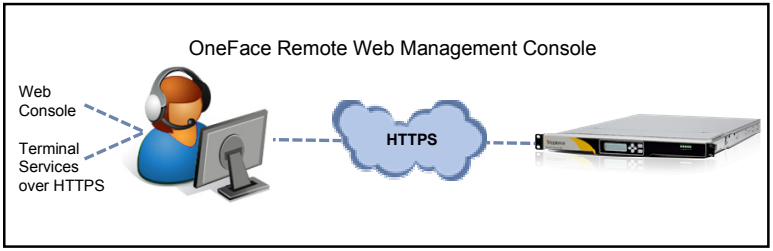
- The IP and Windows networking components
- Windows domain administration
- Windows user management
- Windows security administration
- Installation of nAppliance supplied and supported 3rd party applications
- Upload data to the appliance and run patch updates
- Backup and restore the application system image
- Connect to the Windows operating system via Terminal Services over HTTP

OneFace uses the HTTPS protocol over port 8098. To attach to the appliance OneFace application, use the following URL from your browser:

https://<ip address of Internal Port>:8098/

The Internal interface is the first interface (or Windows LAN 1) on most appliances. On the security appliances, this is the INTERNAL and not the EXTERNAL interface. The External interface will typically have a network security block and not allow access through this interface. The security appliances have a pre-defined

system access rule allowing remote web management access.



When attaching to the URL, the appliance will request a username and password. This is prompting for a Windows administrator account.

The default account is

administrator

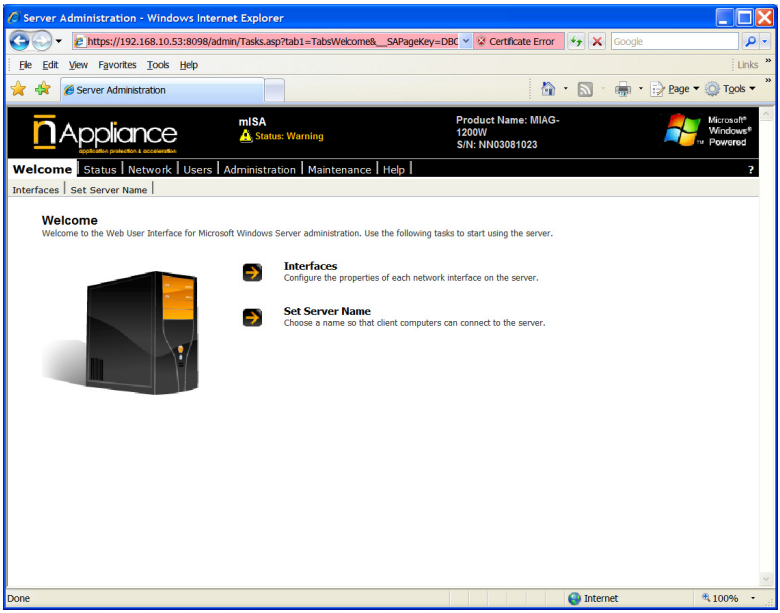
and the default password is

nAppliance13

The browser will complain of a non-signed certificate. Connect anyway. You can later assign a signed certificate to this appliance with OneFace.

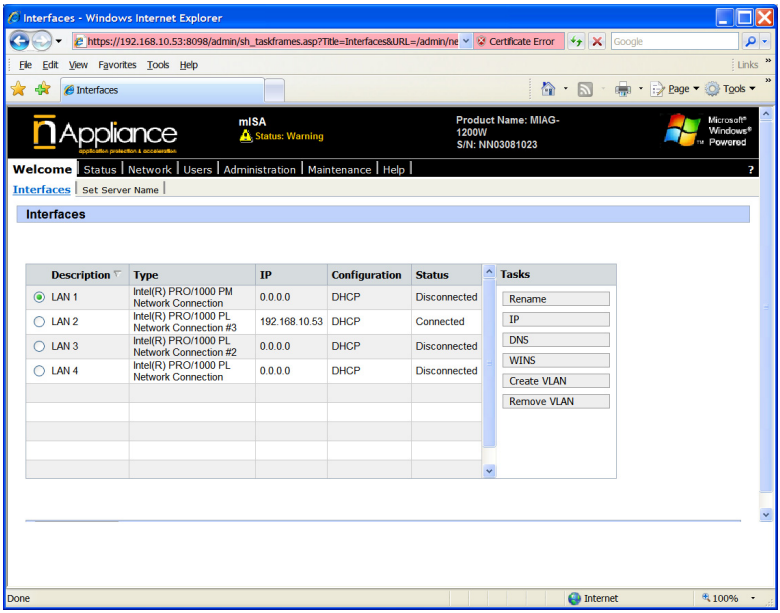
After logging in sucessfully, the initial OneFace Web Console welcome screen.

Welcome Screen



The welcome screen allows the administrator to begin the configuration of the initial IP network interfaces.

Welcome – Interfaces

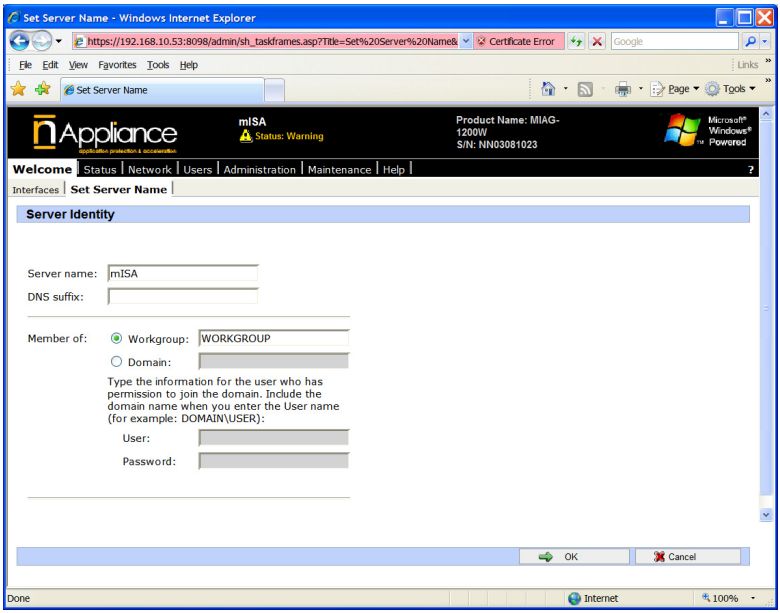


Selecting the Interfaces tab manages the network interfaces. This function coorisponds to the Windows Control Panel Network Connections.

This screen allows you to set the parameters for every available physical interface.

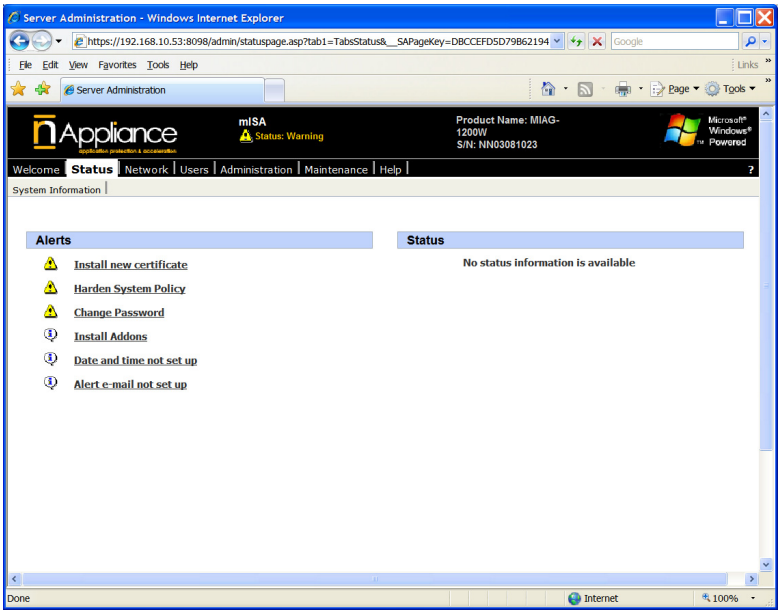
Rename – Rename the Interface. Default is usually LAN <x>.
IP – Set the IP Address parameters.
DNS – Set the DNS configuration and domain name.
WINS – Set the WINS configuration.
Create VLAN – Define a VLAN associated with this port.
Remove VLAN – Remove the VLAN associated with this port.

Set Server Name



The Set Server Name allows the administrator to define the domain parameters, and to join to a Windows Domain.

Status Screen



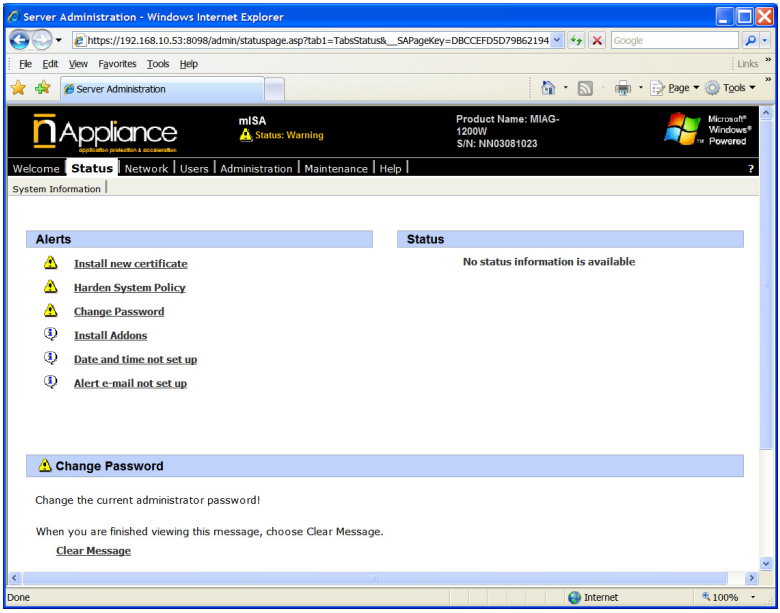
The Status screen displays a list of security and health alerts or status messages. The OneFace web console run a process which analyzes the system for issues. Clicking on any of the Status messages will display a detailed message describing specific issue.

The messages described above show following alerts:

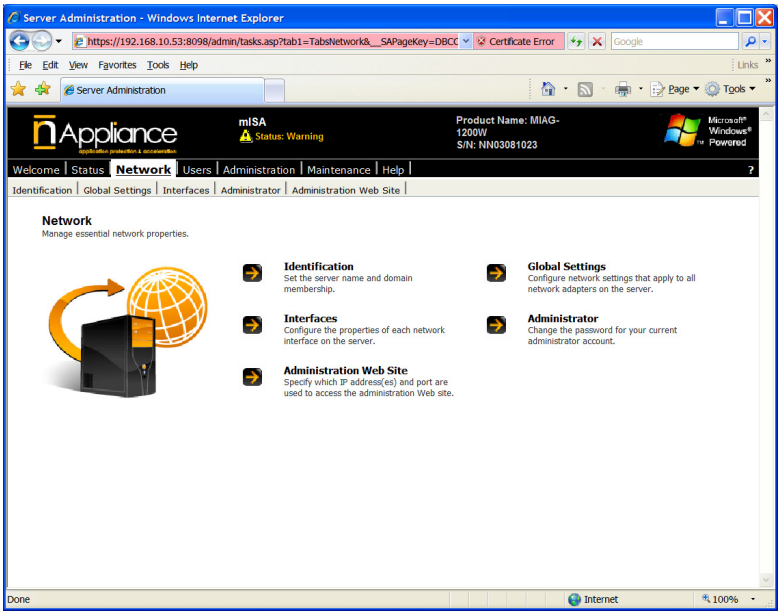
- Install new certificate – the default system has a self-signed certificate. Installing an official certificate will remove the warning messages when attaching via the Web Console.
- Harden System Policy – The default configuration allows configuration via the Web Console by any Internal IP Address. This system recommends

tighening the access a to specific address or networks.

- Change Password – The system is still configured with the factory default password. This should be changed during the initial installation.

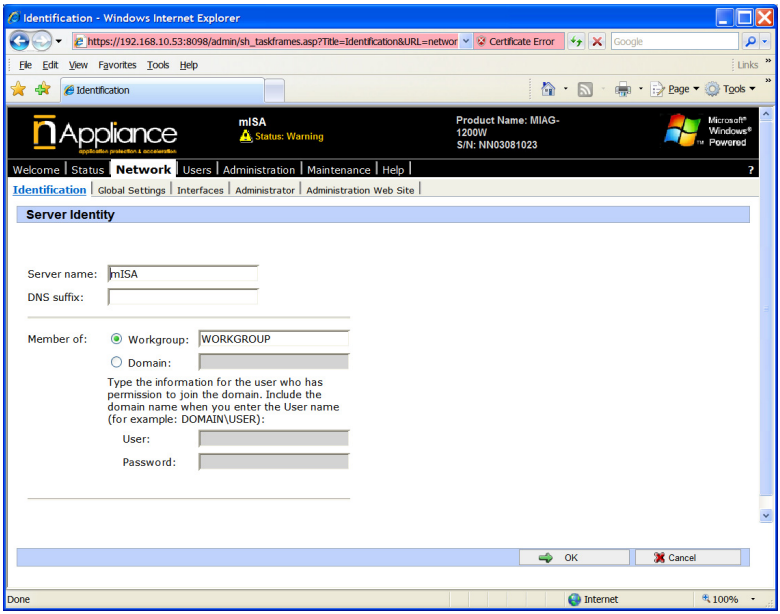


Network Screen



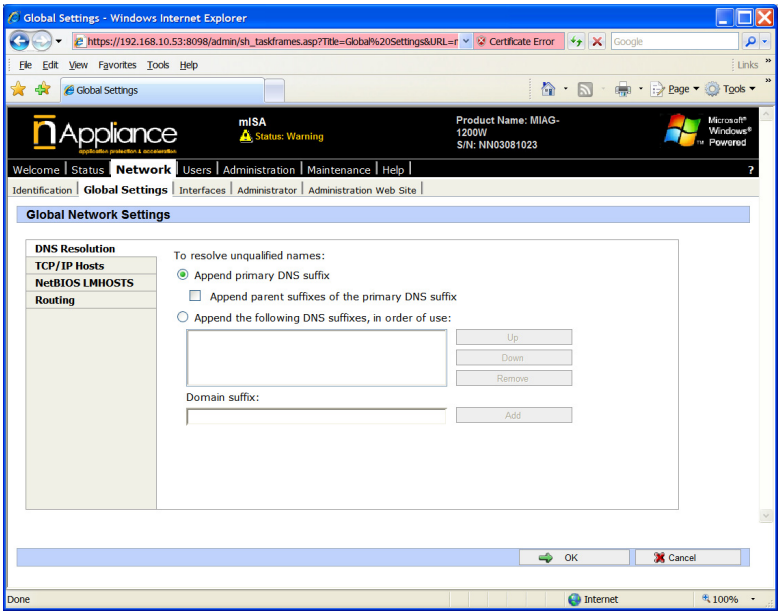
The Network Screen has several functions for administration of network interfaces, Windows domain administration, Network routing, Administrator password maintenance and administration of the Web Console interface.

Identification Tab



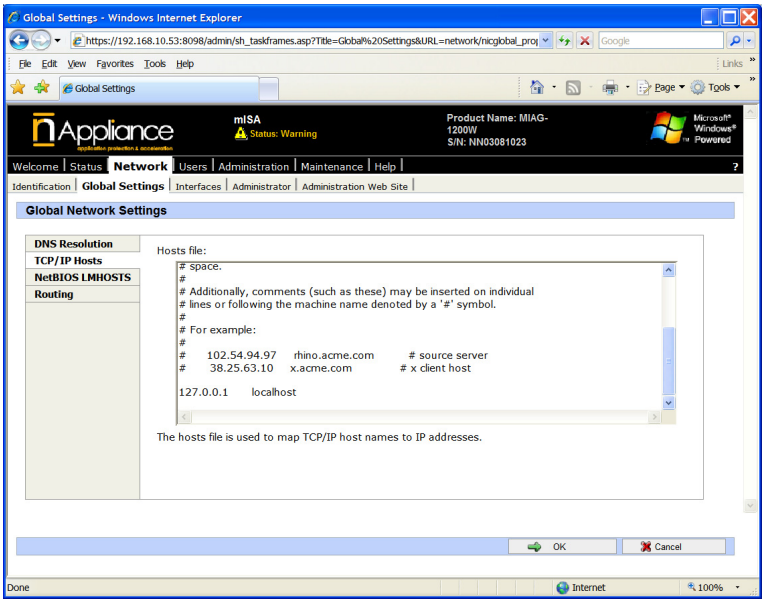
The Identification screen manages the Server name (IP Hostname), the DNS suffix, and joins the appliance to a windows domain.

DNS Resolution Tab



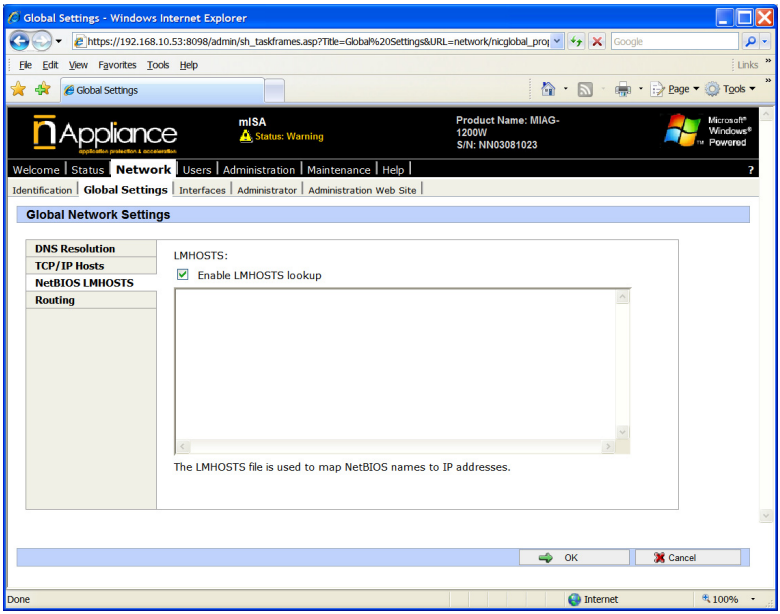
The Global Settings DNS Resolution screen manages the DNS resolution function. The domain suffixes and domain searches are defined.

Global Settings Tab – TCP/IP Hosts



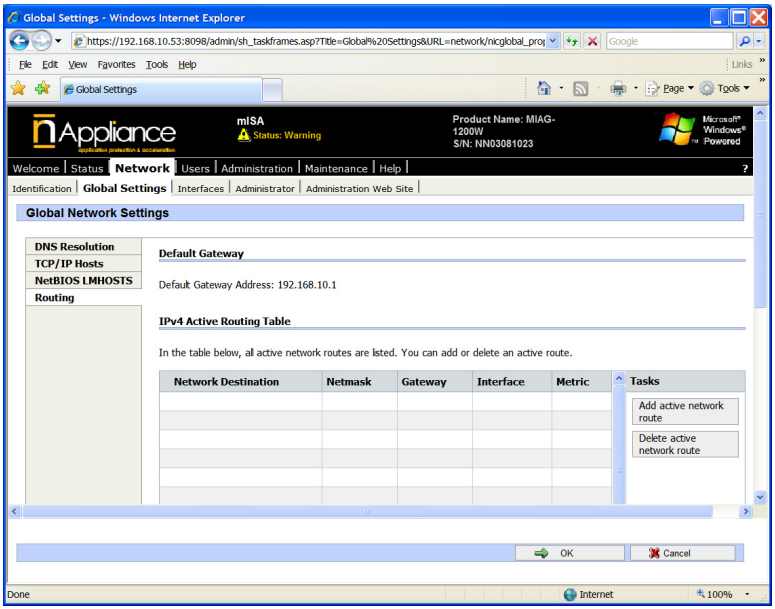
The TCP/IP Hosts screen manages the IP Hosts File.

Global Settings – NetBIOS Lmhosts



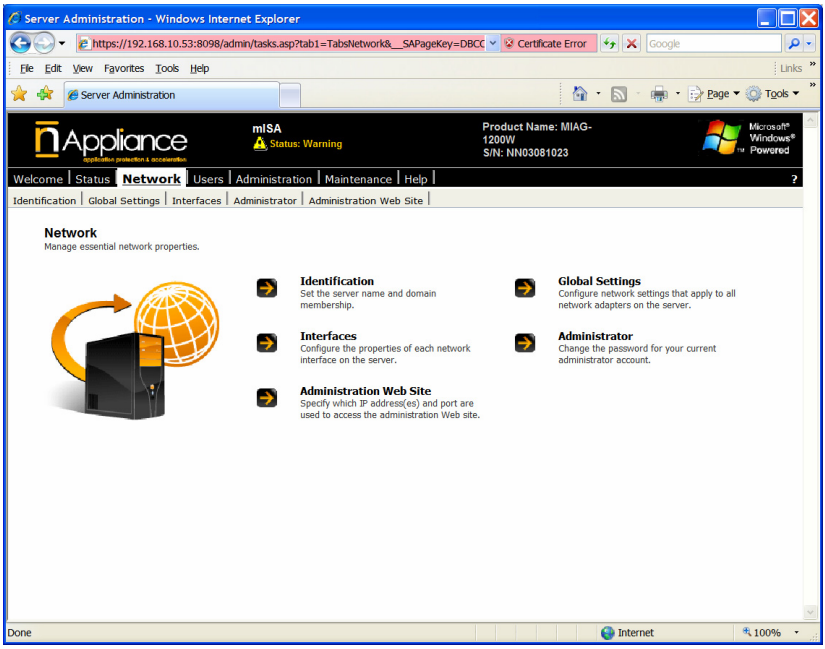
The NetBIOS Lmhosts management screen manages the Windows LMHOSTS file. This is a Windows version of a HOSTS file which overrides the Windows Master Browser and WINS for Windows Name Resolution.

Global Settings – Routing



The Routing function allows the administrator to manage static IP routes.

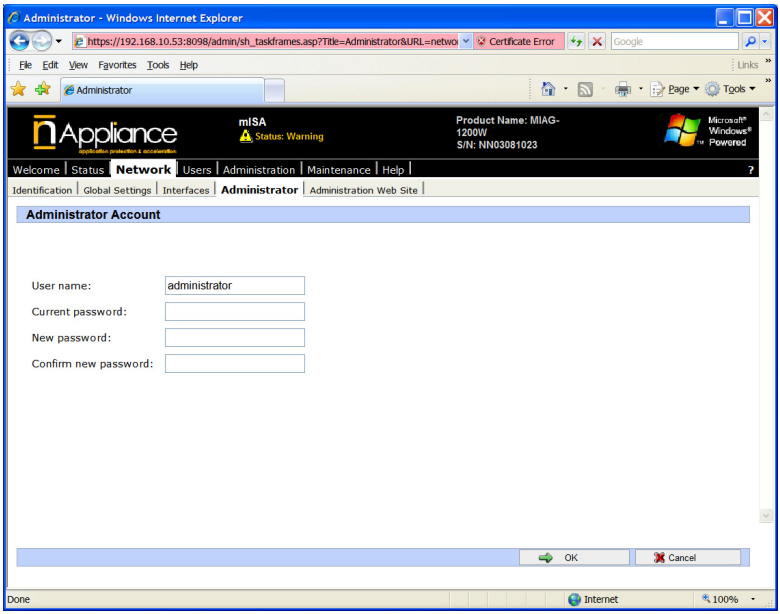
Network



The Interfaces function manage the Windows network interfaces.

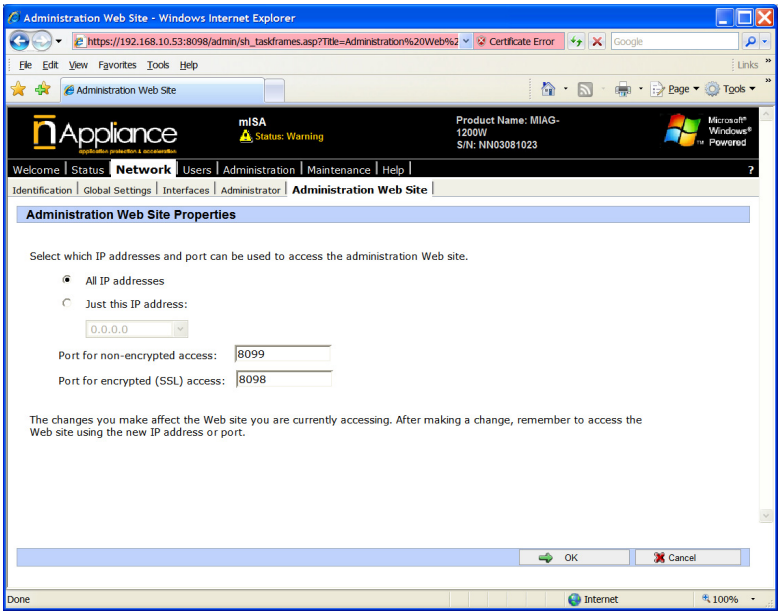
See Welcome – Interfaces described above.

Administrator



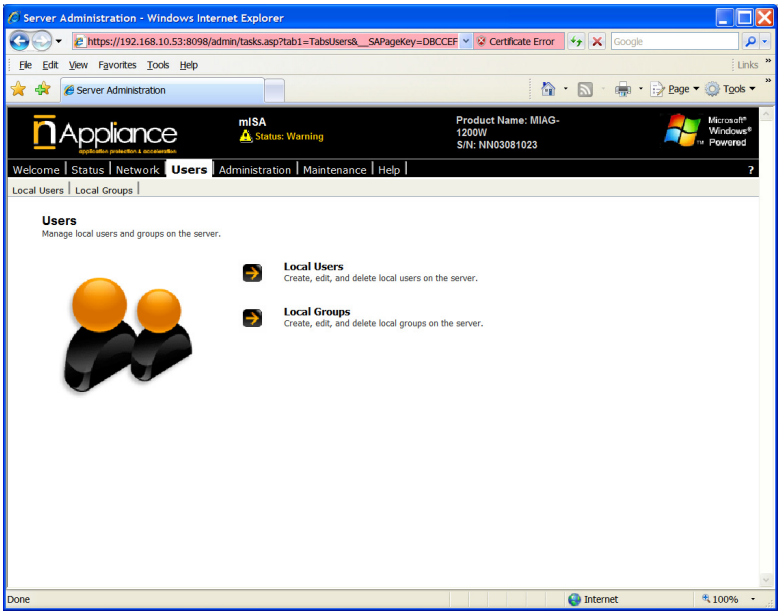
The Administrator function manages user passwords.

Administrator Web Site



The Administrator Web Site manages the security access for the Web Console interface, and the ports used for this access.

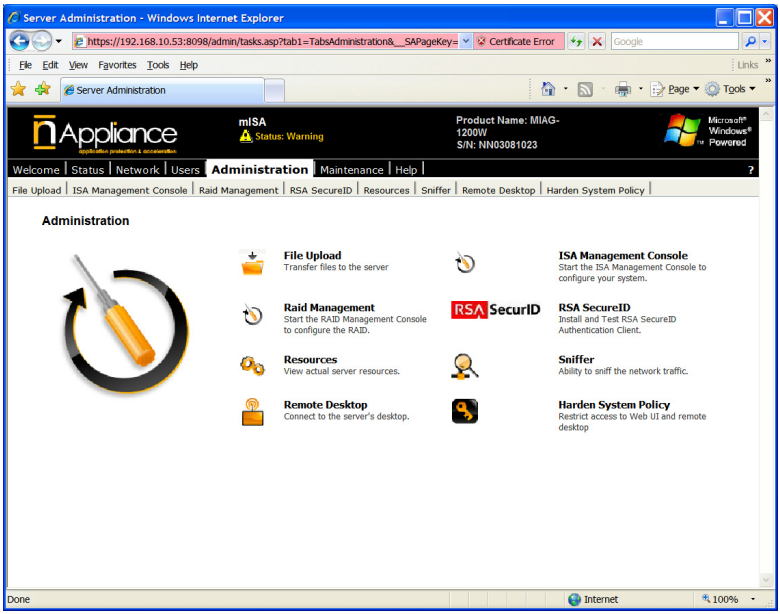
Users



The users functions manage users and user groups.

The local user and group management opens a Windows Terminal Services screen to the appliance.

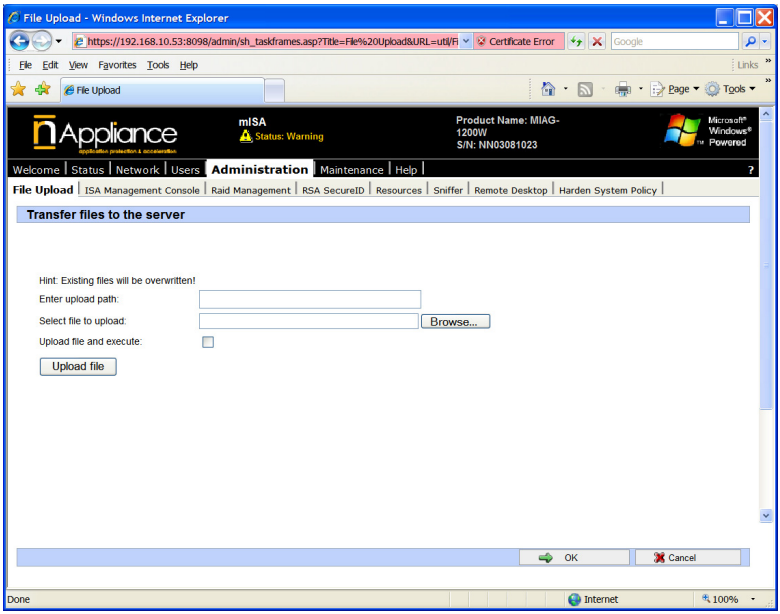
Administration



Most of the Administration functions open Windows Terminal Services to the appliance. The exceptions are:

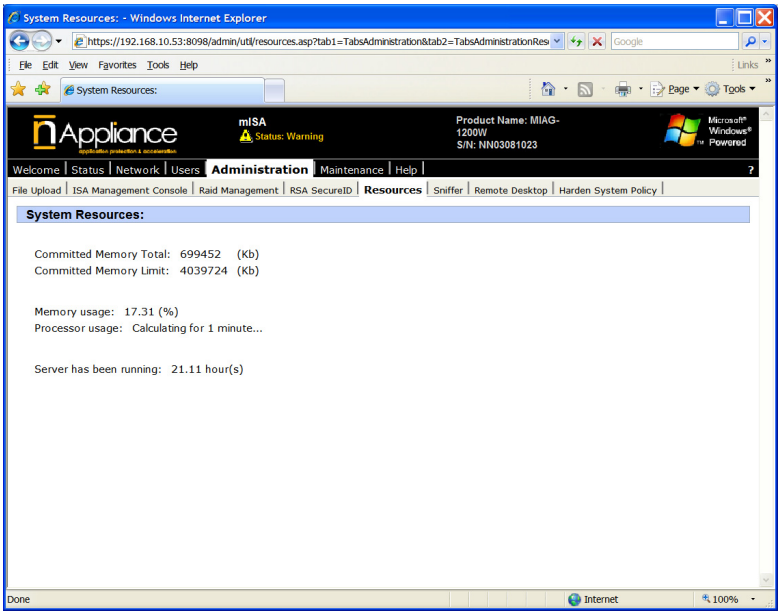
- File Upload
- Resources
- Harden System Policy

File Upload



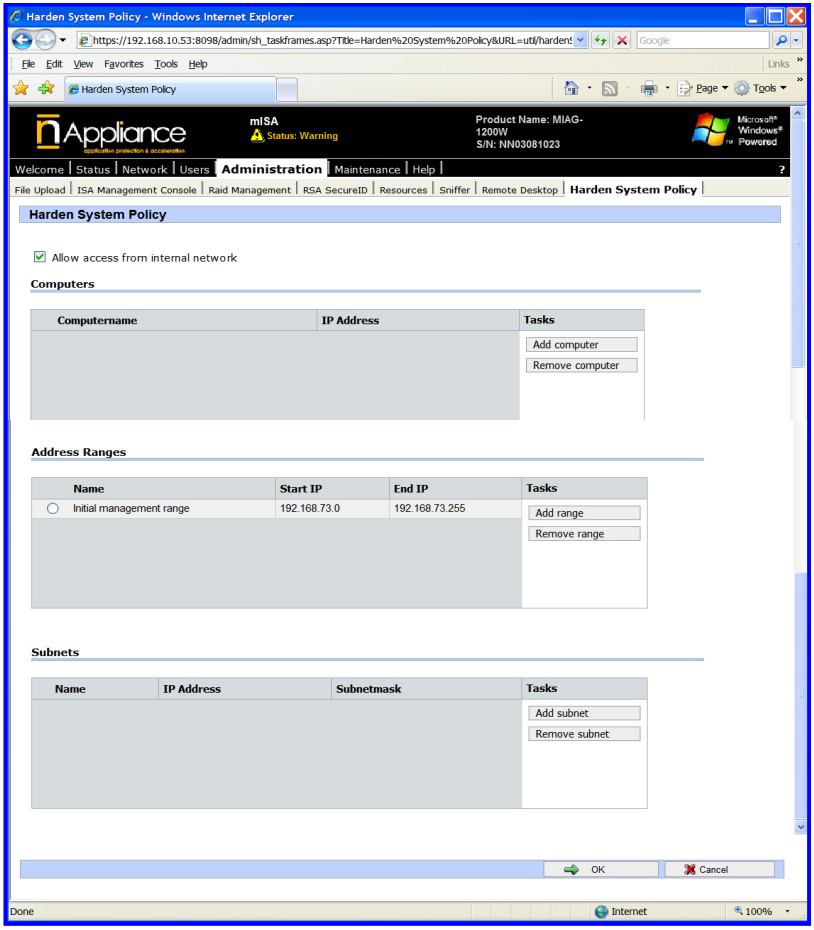
The File Upload function allows uploading files to specified locations on the appliance, and optionally executing this uploaded file. This provides a simple method of updating or patching remotely one or many appliances.

Resources



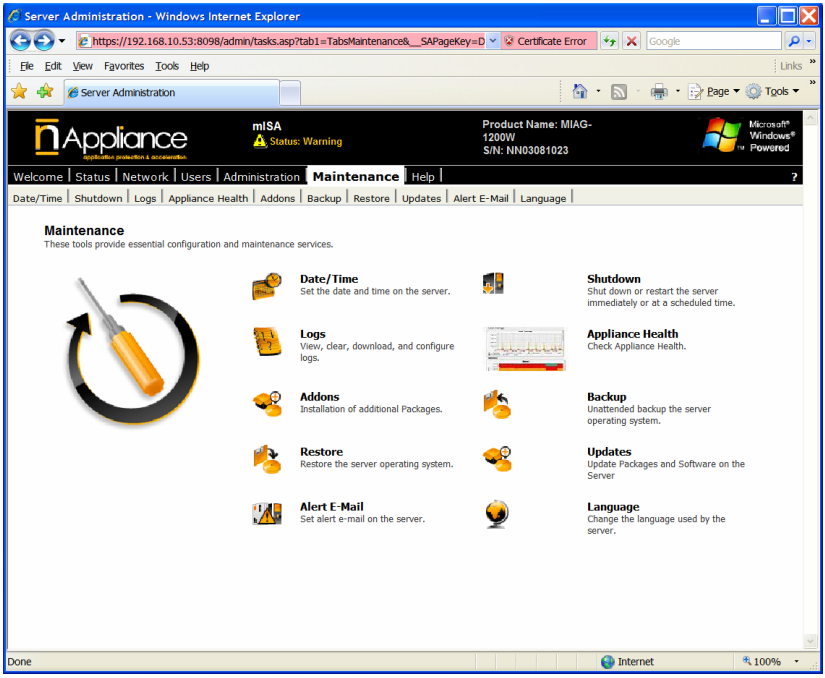
The Resources screen displays memory and CPU resources.

Harden System Policy



The Harden System Policy allows the administrator to restrict access to the Web Console by IP address or IP range.

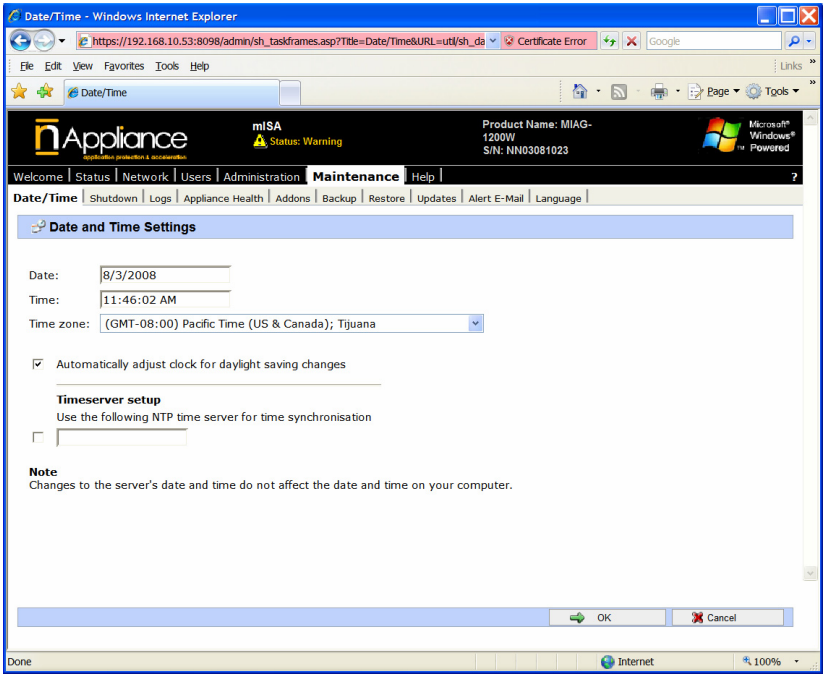
Maintenance Screen



The Maintenance functions allow the administrator to manage various general functions including:

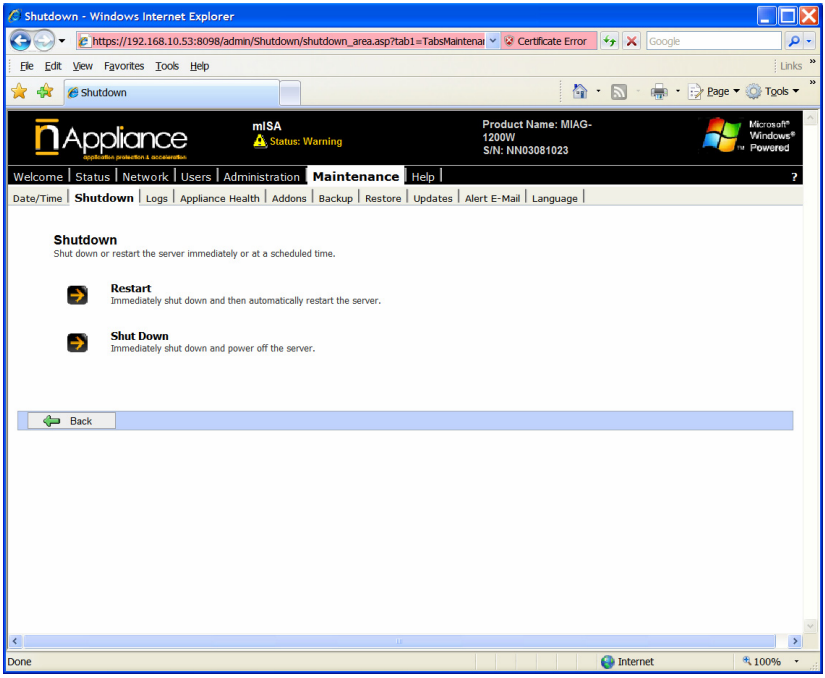
- Setting the appliance time/date
- Shutdown and reboot the appliance
- Reviewing the Windows Event Viewer logs
- Install addon 3rd party packages supported by nAppliance
- Create a backup image of the appliance image
- Set the alert administrator email address

Date/Time



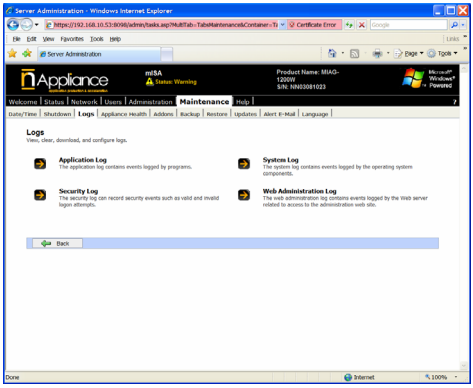
The Time/Date function allows the administrator to set the system time and date, and to specify an NTP time server to receive time updates over the Internet.

Shutdown

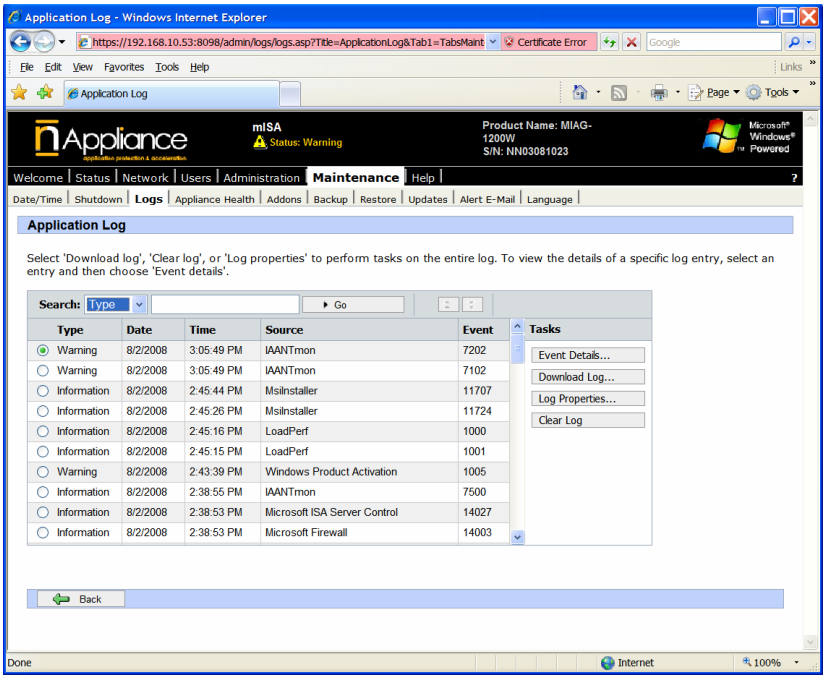


The Shutdown function allows the administrator to shutdown and power off the appliance, or to reboot the appliance.

Logs

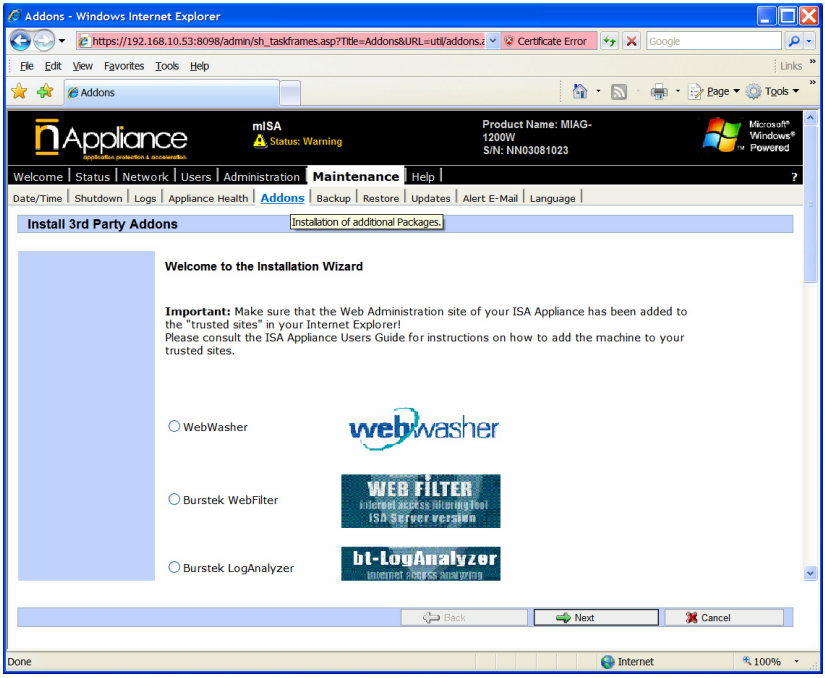


The Logs function allows the administrator to view the Windows Event Viewer logs.



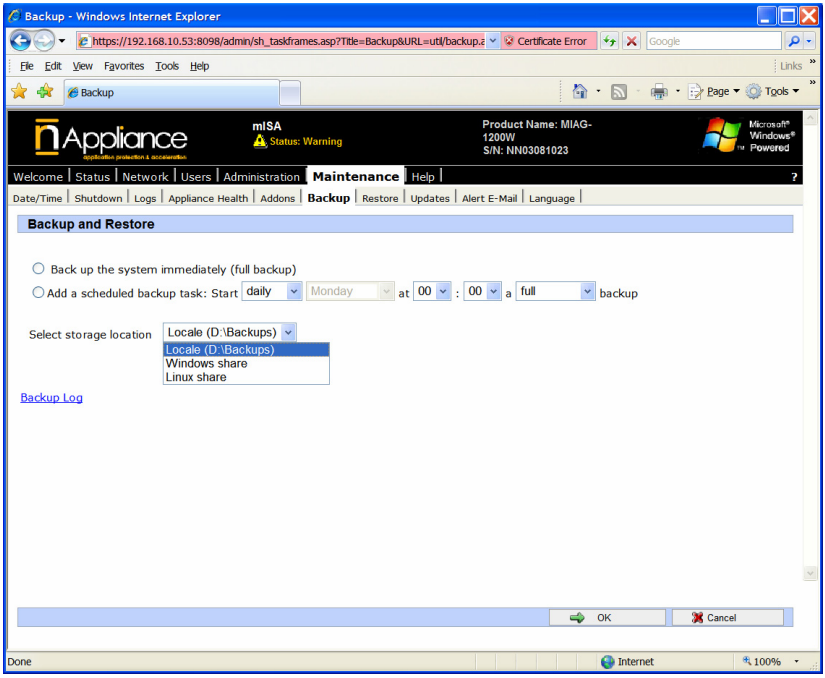
Type	Date	Time	Source	Event
Warning	8/2/2008	3:05:49 PM	IAANTmon	7202
Warning	8/2/2008	3:05:49 PM	IAANTmon	7102
Information	8/2/2008	2:45:44 PM	MsiInstaller	11707
Information	8/2/2008	2:45:26 PM	MsiInstaller	11724
Information	8/2/2008	2:45:16 PM	LoadPerf	1000
Information	8/2/2008	2:45:15 PM	LoadPerf	1001
Warning	8/2/2008	2:43:39 PM	Windows Product Activation	1005
Information	8/2/2008	2:38:55 PM	IAANTmon	7500
Information	8/2/2008	2:38:53 PM	Microsoft ISA Server Control	14027
Information	8/2/2008	2:38:53 PM	Microsoft Firewall	14003

Addons



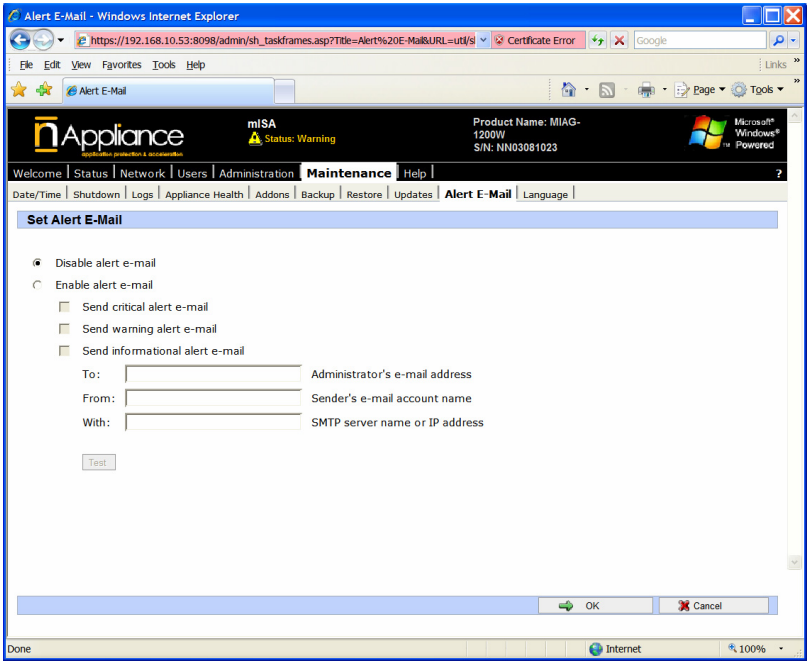
The Addons function allows the administrator to download and install nAppliance supported applications.

Backup



The Backup function allows the adminstrator to create a backup image of the appliance image and restore this image back to the appliance using the Restore function.

Alert Email



The Alert Email assigns the appliance monitoring system's administrator email address. When there is a critical event within the appliance, this function will define where to send the alerts. This function is disabled by default and should be enabled.

Chapter 4: IPMI – Network Based Management Interface

IPMI is a network based system management interface which runs on a hardware component on nAppliance systems. This is a Lights Out Management interface (LOM). This hardware component is called a BMC (Base Management Card). System management communications between the administrator and the BMC runs through an IP network.

The nAppliance BMC is based on the IPMI specification version 2.0. The network protocols supported are RMCP version 1, and also HTTP via a web interface.

The IPMI BMC supports network access to a system at the hardware level, where the administrator can access a system regardless of the OS type or functionality. Since the BMC runs independently of the motherboard and CPU, the system can be accessed, powered off and on, and monitored during all modes of the operating system during the boot process.

The IPMI hardware system supports a direct RMCP access via a java client (IPMIView) available on the nAppliance website. This client is available at:

http://support.nAppliance.com

under the downloads section.

The nAppliance IPMI card has a builtin web server and includes a web application where the administrator can access all management features of IPMI 2.0. This document describes the operation of the IPMI using the HTML interace.

There are two hardware implementations of IPMI on the nAppliance systems. One implementation has a dedicated NIC port. The other implementation uses a shared NIC configuration. The shared NIC configuration uses the same network port for traffic on LAN 1 and for IPMI network traffic. The IPMI traffic is separated by the IPMI hardware so that the operating system supporting traffic on LAN 1 can be inoperable but the IPMI system will still have full functionality. This allows the administrator to power down the system and watch the system boot as if the adminstrator was physically at the local console.

Setup

On systems with a dedicated IPMI NIC port, this dedicated port will be a single port and is identified by the appliance quick start guide, and typically documented somewhere on the appliance.

On shared port systems which do not have a dedicated IPMI NIC port, the IPMI functions are multiplexed onto the first port or LAN 1. This port will be the uppermost port closest to the mouse and keyboard ports (see Appendix 1). Systems with shared ports do not have the KVM over IP capability, but have the hardware sensor monitoring capabilities.

The IPMI BMC must have an IP address to be accessed. This port can be set by one of two methods.

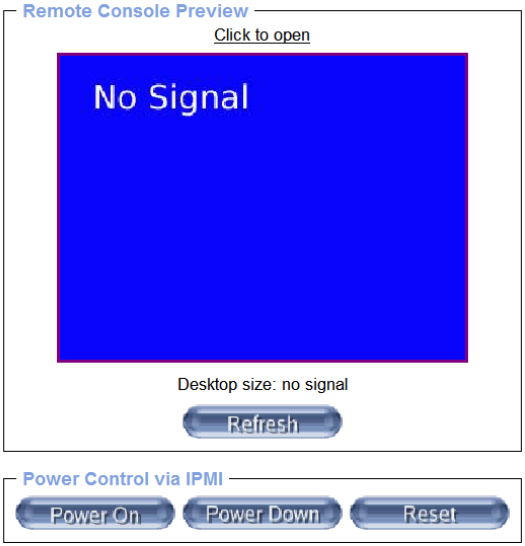
1. The port comes from the factory preset with the address 10.10.10.201. If you assign a computer with an IP address on this network, you will be able to access the IPMI web server by pointing a web browser at: http://10.10.10.201/
    i. Once accessing the IPMI web application, there is a screen which will allow the administrator to change the IP network settings to match the correct network configuration.
2. When booting the nAppliance systems, there is a boot system called FFRS which is documented elsewhere in this document. This system has the capability of accressing the IPMI BMC card and setting the IP addresses directly.

Once the IPMI card has an IP address, it can be accessed similarily to any other computer on the network.

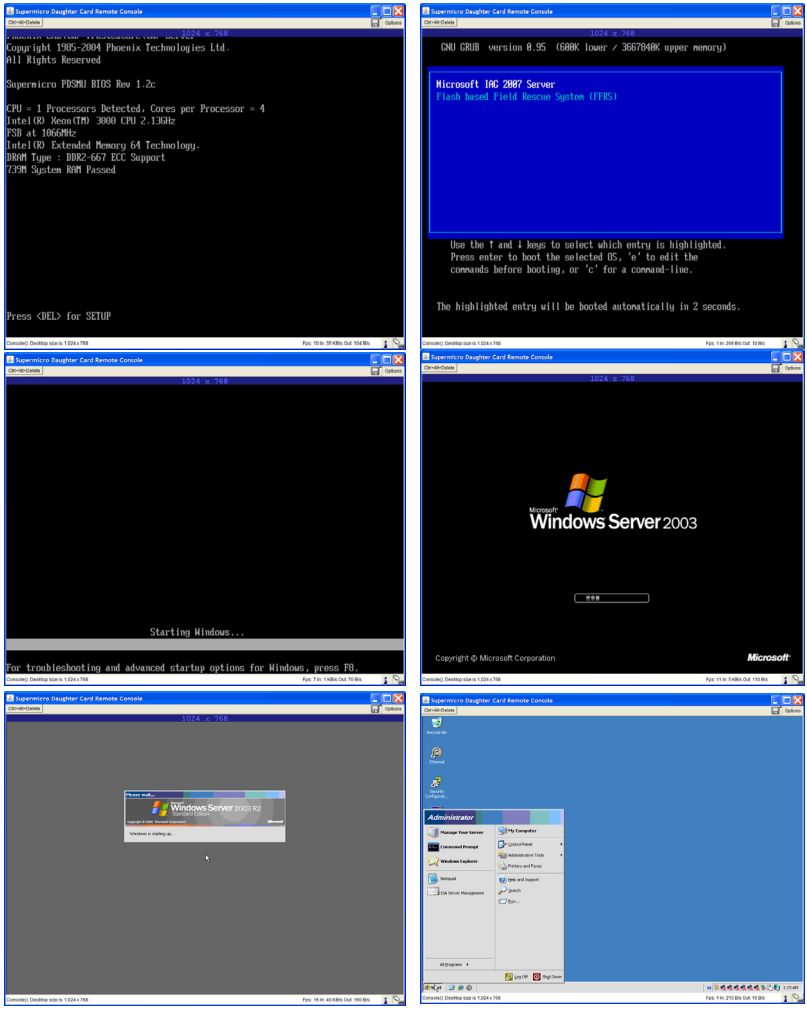
KVM over IP

KVM over IP is a feature available only with the hardware models with a dedicated IPMI NIC port, or on 3200 models, which provide dual KVM and network functionality on the first NIC port.

KVM (Keyboard, Video, Mouse) over IP allows the administrator to connect and manage systems remotely. This is equivalent functionality to physical KVM systems which directly connect computer systems. KVM over IP allow the administrator to manage the keyboard and mouse movements over the network, and view the actual video signal from a remote location. Additionally the system can be powered on and off remotely

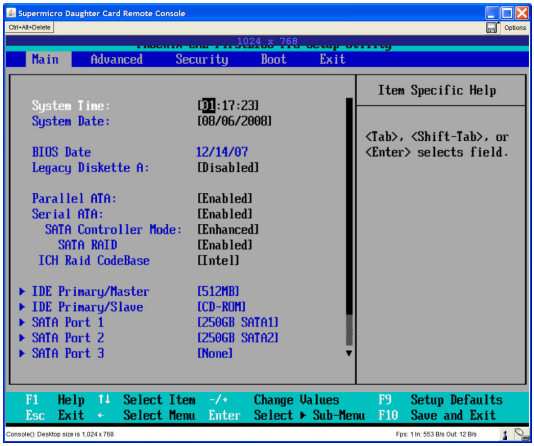


This is an IPMI KVM over IP screen connected to a system which is powered down.



The above screens show a boot-up as seen on the IPMI KVM web interface.

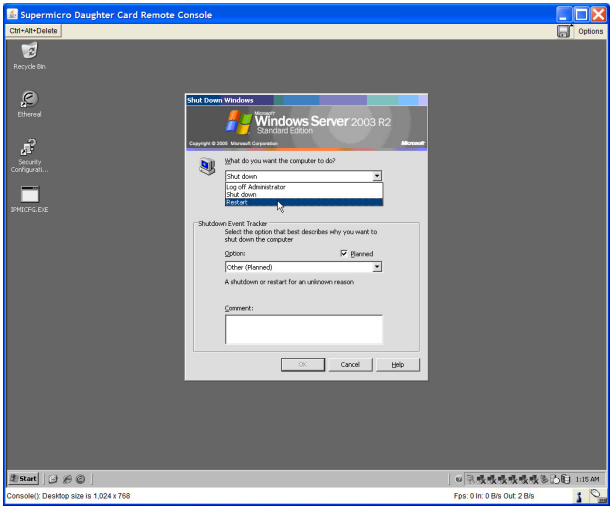
The system is powered up by pressing the power on button on the KVM over IP screen (or physically powering up the server) and the above screens show the booting process on the web browser screen remotely.

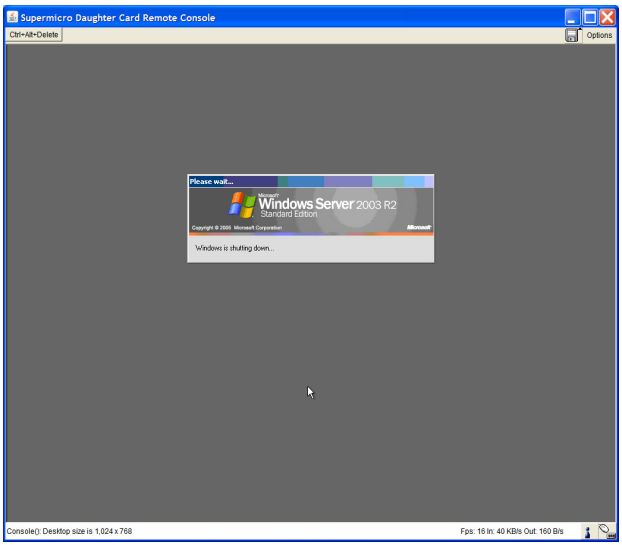


The BIOS can be managed remotely as well.

The following show the system being shutdown remotely.

The Control Alt Delete command is sent by pressing the Cntl-Alt-Del button at the top of the web application.



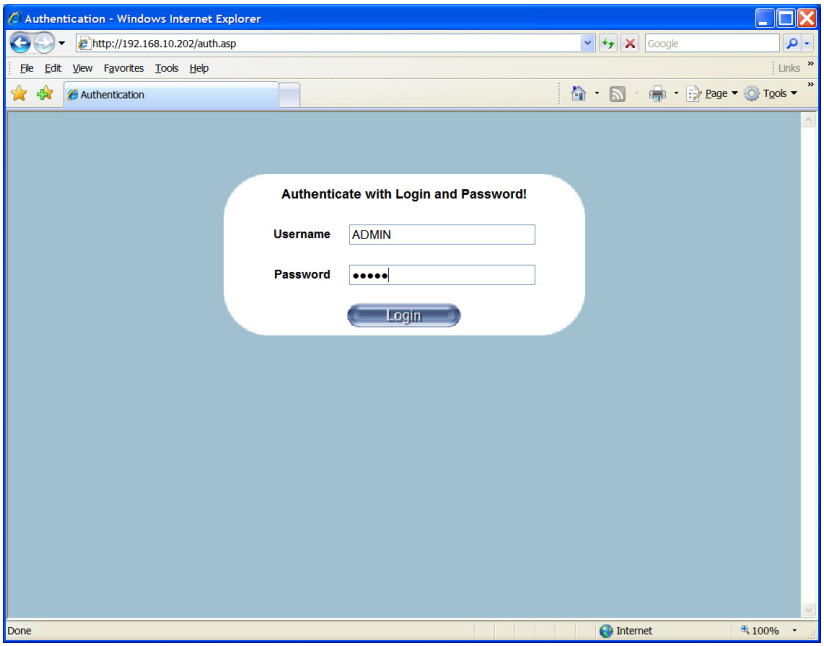


And the server is shutdown normally.

The systems powers off during a complete shutdown.

Using the IPMI Web Console

Login

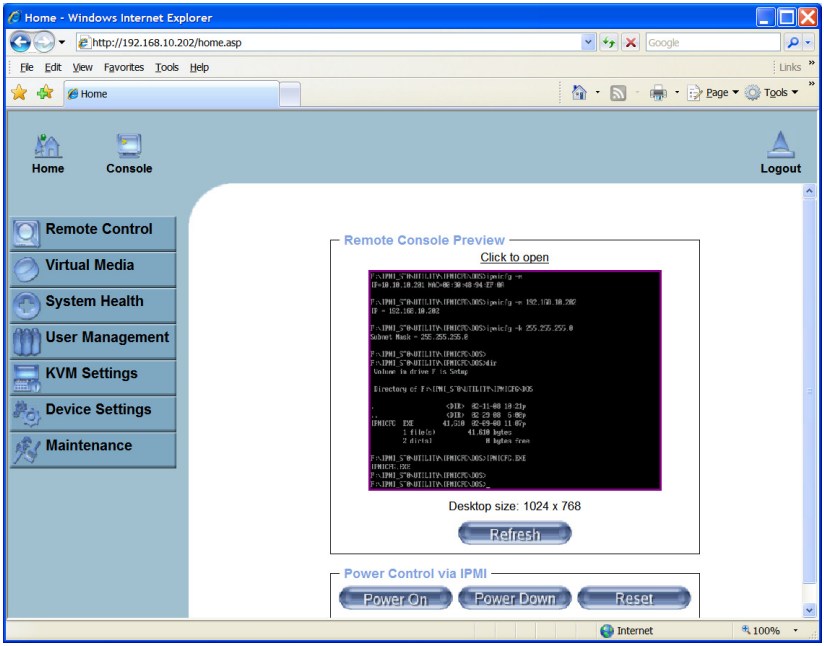


The first screen on the application is the login screen. The default username and password is (uppercase):

Username: ADMIN
Password: ADMIN

Main Screen

Once logged in, the main management screen is displayed.



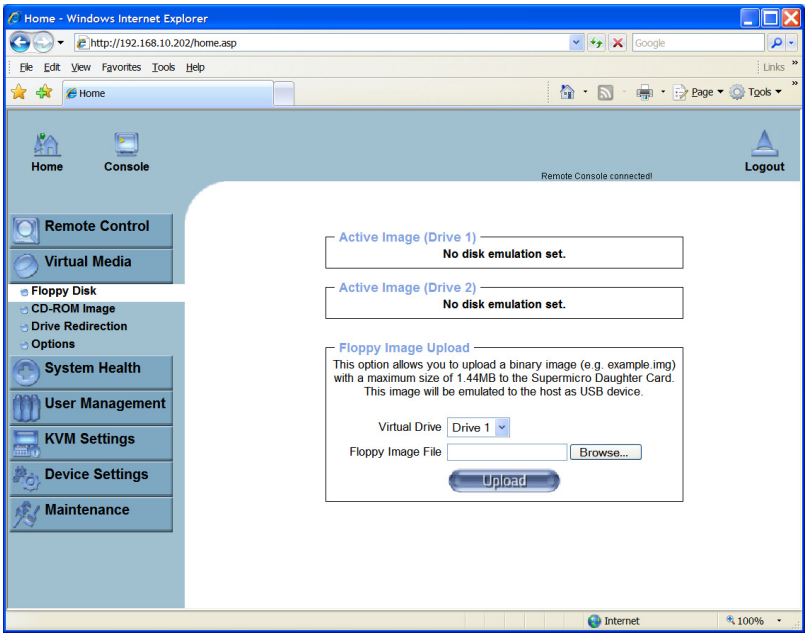
The usage of each function is described below.

The screen in the center is a remote KVM over IP console view. Clicking on this screen spawns a larger screen view.

Power On: Power up the remote system
Power Down: Power down the remote system
Reset: Power down then power up the remote system

Virtual Media

The IPMI system has the ability to attach virtual peripherals.



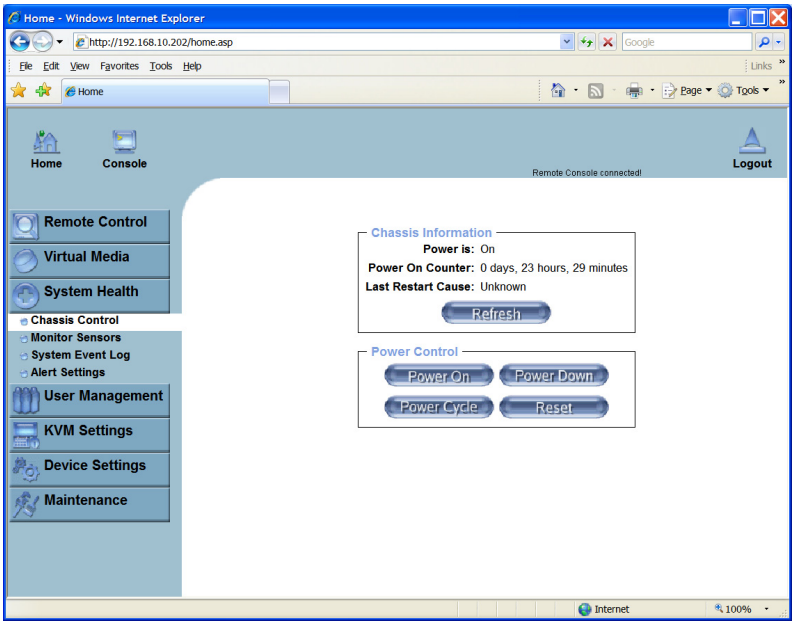
Virtual disk drives such as CD ROM drives and Floppy drives can be emulated by mounting ISO file images or attaching to Windows Shares.

System Health

Several functions for monitoring the remote system's health include:

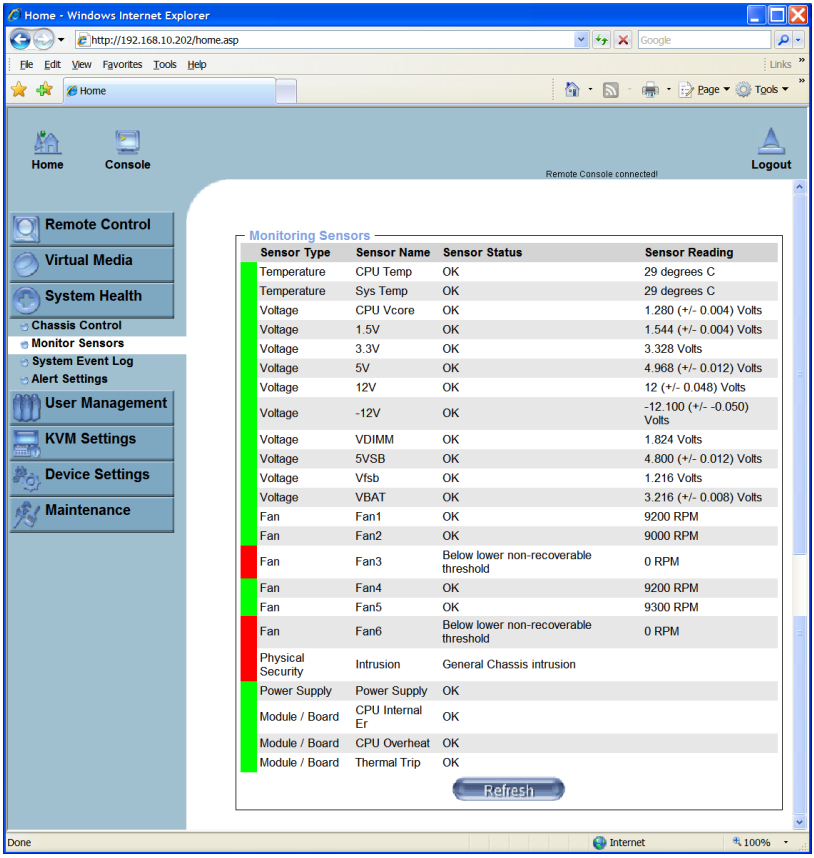
- Chassis control for displaying system uptime statistics
- Monitor for sensors, displaying temperatures, and other data points
- Displaying the IPMI hardware event log
- And creating events which are logged and sent out as emails or SNMP traps

Chassis Control



The chassis control also provides functions to power cycle and reset the hardware system.

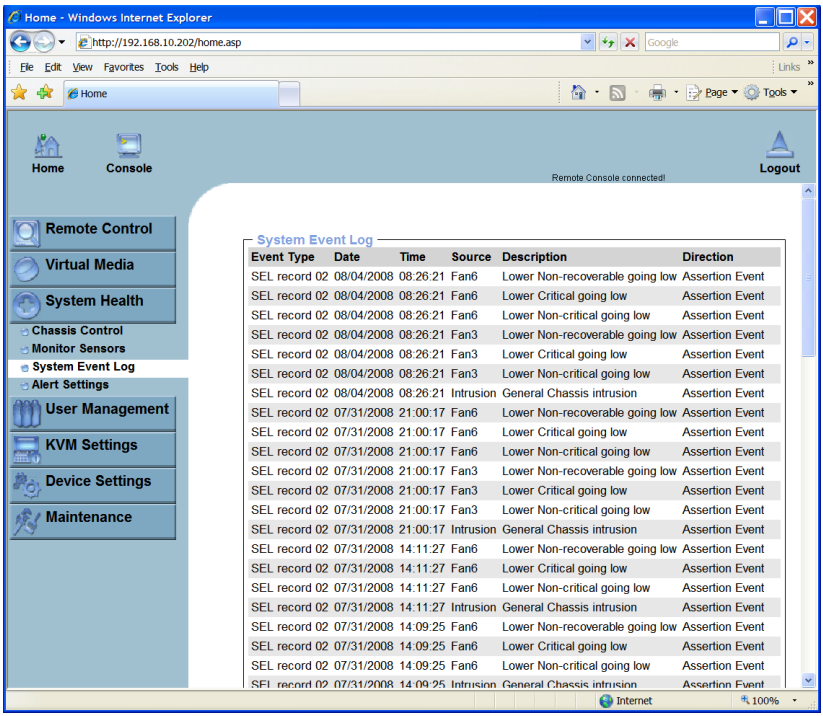
Monitor Sensors



Sensor Type	Sensor Name	Sensor Status	Sensor Reading
Temperature	CPU Temp	OK	29 degrees C
Temperature	Sys Temp	OK	29 degrees C
Voltage	CPU Vcore	OK	1.280 (+/- 0.004) Volts
Voltage	1.5V	OK	1.544 (+/- 0.004) Volts
Voltage	3.3V	OK	3.328 Volts
Voltage	5V	OK	4.968 (+/- 0.012) Volts
Voltage	12V	OK	12 (+/- 0.048) Volts
Voltage	-12V	OK	-12.100 (+/- -0.050) Volts
Voltage	VDIMM	OK	1.824 Volts
Voltage	5VSB	OK	4.800 (+/- 0.012) Volts
Voltage	Vfsb	OK	1.216 Volts
Voltage	VBAT	OK	3.216 (+/- 0.008) Volts
Fan	Fan1	OK	9200 RPM
Fan	Fan2	OK	9000 RPM
Fan	Fan3	Below lower non-recoverable threshold	0 RPM
Fan	Fan4	OK	9200 RPM
Fan	Fan5	OK	9300 RPM
Fan	Fan6	Below lower non-recoverable threshold	0 RPM
Physical Security	Intrusion	General Chassis intrusion	
Power Supply	Power Supply	OK	
Module / Board	CPU Internal Er	OK	
Module / Board	CPU Overheat	OK	
Module / Board	Thermal Trip	OK	

The Monitor Sensor displays the IPMI statistics for CPU and Motherboard temperatures, fan speeds, power voltages and other sensor readings.

System Event Log



Event Type	Date	Time	Source	Description	Direction
SEL record 02	08/04/2008	08:26:21	Fan6	Lower Non-recoverable going low	Assertion Event
SEL record 02	08/04/2008	08:26:21	Fan6	Lower Critical going low	Assertion Event
SEL record 02	08/04/2008	08:26:21	Fan6	Lower Non-critical going low	Assertion Event
SEL record 02	08/04/2008	08:26:21	Fan3	Lower Non-recoverable going low	Assertion Event
SEL record 02	08/04/2008	08:26:21	Fan3	Lower Critical going low	Assertion Event
SEL record 02	08/04/2008	08:26:21	Fan3	Lower Non-critical going low	Assertion Event
SEL record 02	08/04/2008	08:26:21	Intrusion	General Chassis intrusion	Assertion Event
SEL record 02	07/31/2008	21:00:17	Fan6	Lower Non-recoverable going low	Assertion Event
SEL record 02	07/31/2008	21:00:17	Fan6	Lower Critical going low	Assertion Event
SEL record 02	07/31/2008	21:00:17	Fan6	Lower Non-critical going low	Assertion Event
SEL record 02	07/31/2008	21:00:17	Fan3	Lower Non-recoverable going low	Assertion Event
SEL record 02	07/31/2008	21:00:17	Fan3	Lower Critical going low	Assertion Event
SEL record 02	07/31/2008	21:00:17	Fan3	Lower Non-critical going low	Assertion Event
SEL record 02	07/31/2008	21:00:17	Intrusion	General Chassis intrusion	Assertion Event
SEL record 02	07/31/2008	14:11:27	Fan6	Lower Non-recoverable going low	Assertion Event
SEL record 02	07/31/2008	14:11:27	Fan6	Lower Critical going low	Assertion Event
SEL record 02	07/31/2008	14:11:27	Fan6	Lower Non-critical going low	Assertion Event
SEL record 02	07/31/2008	14:11:27	Intrusion	General Chassis intrusion	Assertion Event
SEL record 02	07/31/2008	14:09:25	Fan6	Lower Non-recoverable going low	Assertion Event
SEL record 02	07/31/2008	14:09:25	Fan6	Lower Critical going low	Assertion Event
SEL record 02	07/31/2008	14:09:25	Fan6	Lower Non-critical going low	Assertion Event
SEL record 02	07/31/2008	14:09:25	Intrusion	General Chassis intrusion	Assertion Event

The IPMI system records system events such as low fan speeds and voltages. These records are saved and can be reviewed for later analysis.

Alert Settings

The IPMI system can be configured with a set of alerts. These alerts can be discretely defined to watch for specific events, to set a policy for the type of event for the specific sensor or device, and to define how to send the alert message for the specific alert. Message options are email and SNMP traps.

Filter Lists

Each alert is selected by filtering on events. The filter list record is defined by the filter list screen.

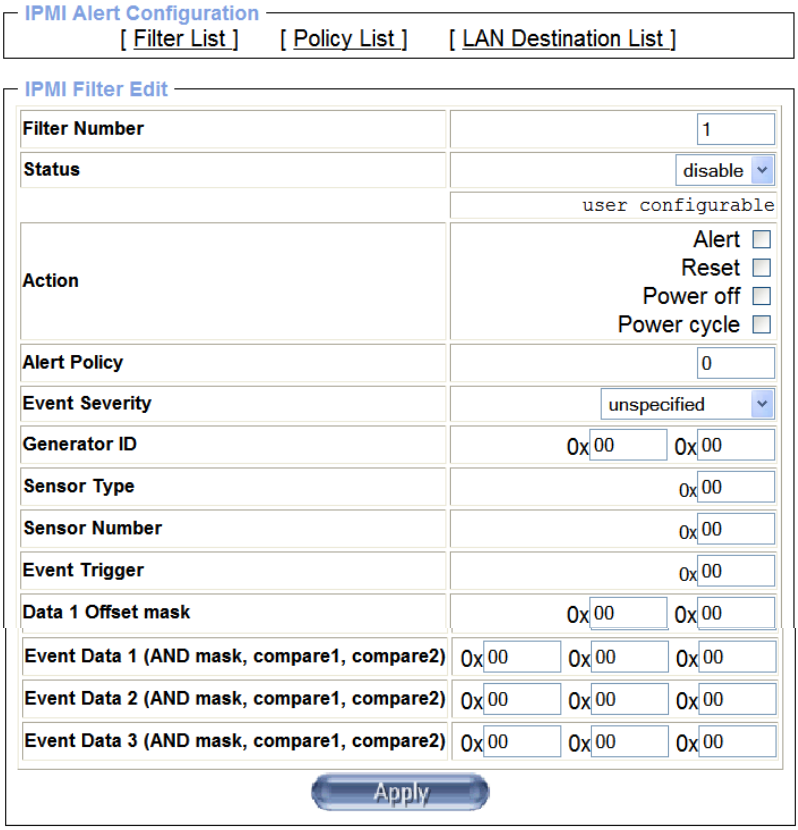
IPMI Alert Configuration

[Filter List] [Policy List] [LAN Destination List]

IPMI Filter List

Index	Status	Filter Type	Action	Policy#	Severity	Generator ID		Sensor Type	Sensor No	Trigger	Offset Mask	Data 1		Data 2		Data 3		
1	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	[edit]
2	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	[edit]
3	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	[edit]
4	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	[edit]
5	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	[edit]

Each filter can be created by pressing the [edit] link.



Policy List

IPMI Alert Configuration

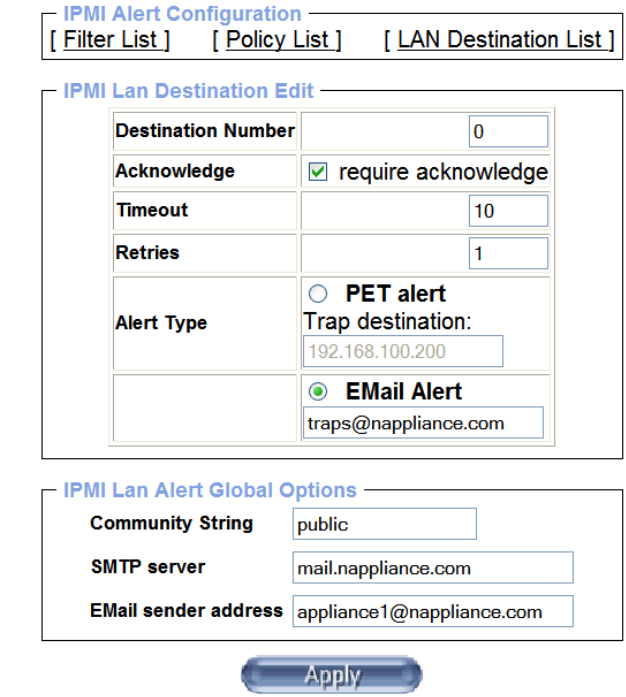
[Filter List] [Policy List] [LAN Destination List]

IPMI Policy List

Index	Status	Policy Set	Policy	Channel No.	Destination	Alert String
1	enable	0	always	1	1	1
2	disabled	0	always	0	0	0
3	disabled	0	always	0	0	0
4	disabled	0	always	0	0	0
5	disabled	0	always	0	0	0
6	disabled	0	always	0	0	0
7	disabled	0	always	0	0	0
8	disabled	0	always	0	0	0
9	disabled	0	always	0	0	0
10	disabled	0	always	0	0	0
11	disabled	0	always	0	0	0
12	disabled	0	always	0	0	0
13	disabled	0	always	0	0	0
14	disabled	0	always	0	0	0
15	disabled	0	always	0	0	0

The policy describes how and whether to process an alert. The policy links the event to the LAN Destination List (Alert message processing).

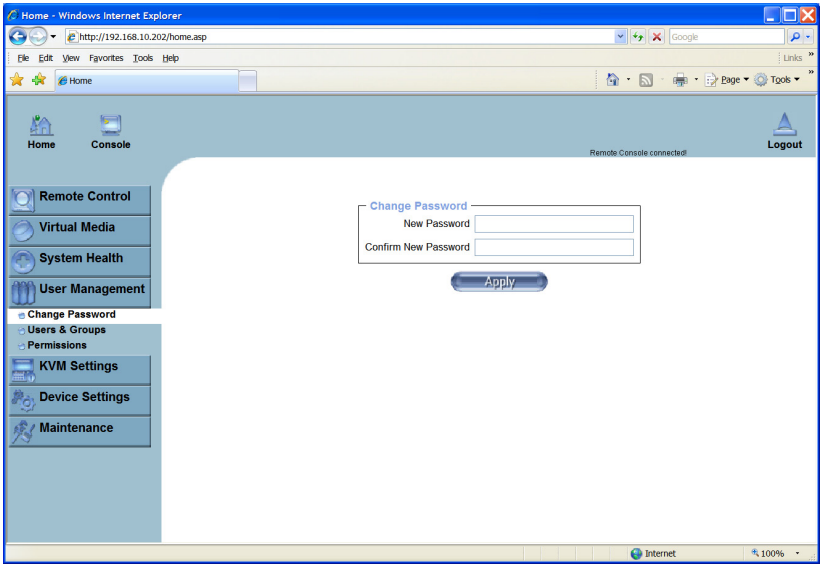
LAN Destination List



The LAN Destination defines how to send out an alert message, either via Email or via an SNMP Trap message.

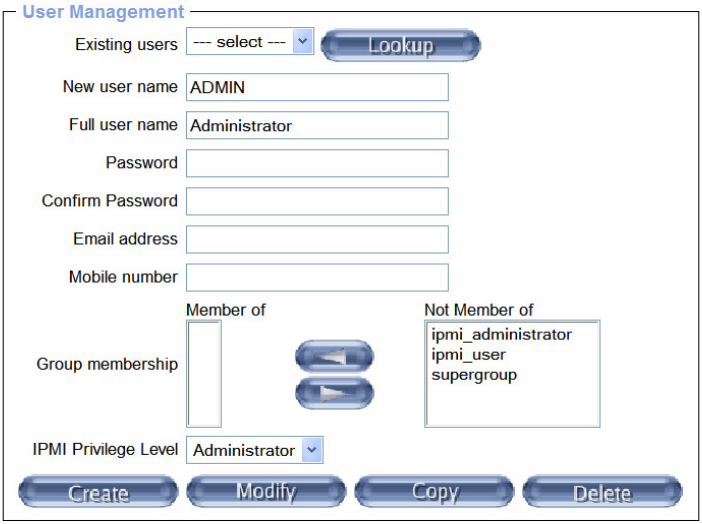
User Management

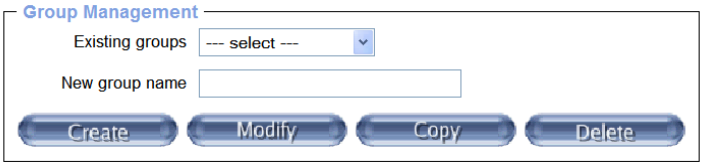
Change Password



The Change Password function allows the administrator to change the ADMIN account password.

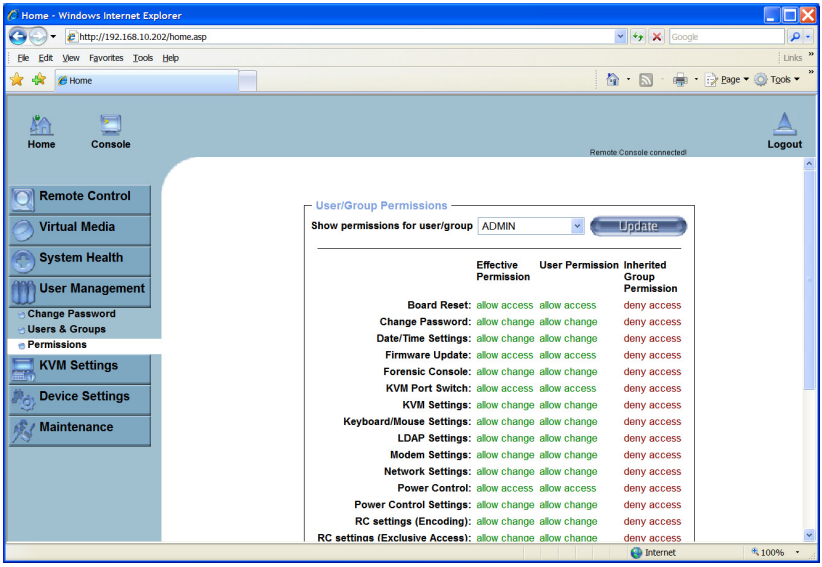
Group Management





Group management allows the adminstrator to define specifics about each user as well as define groups of users.

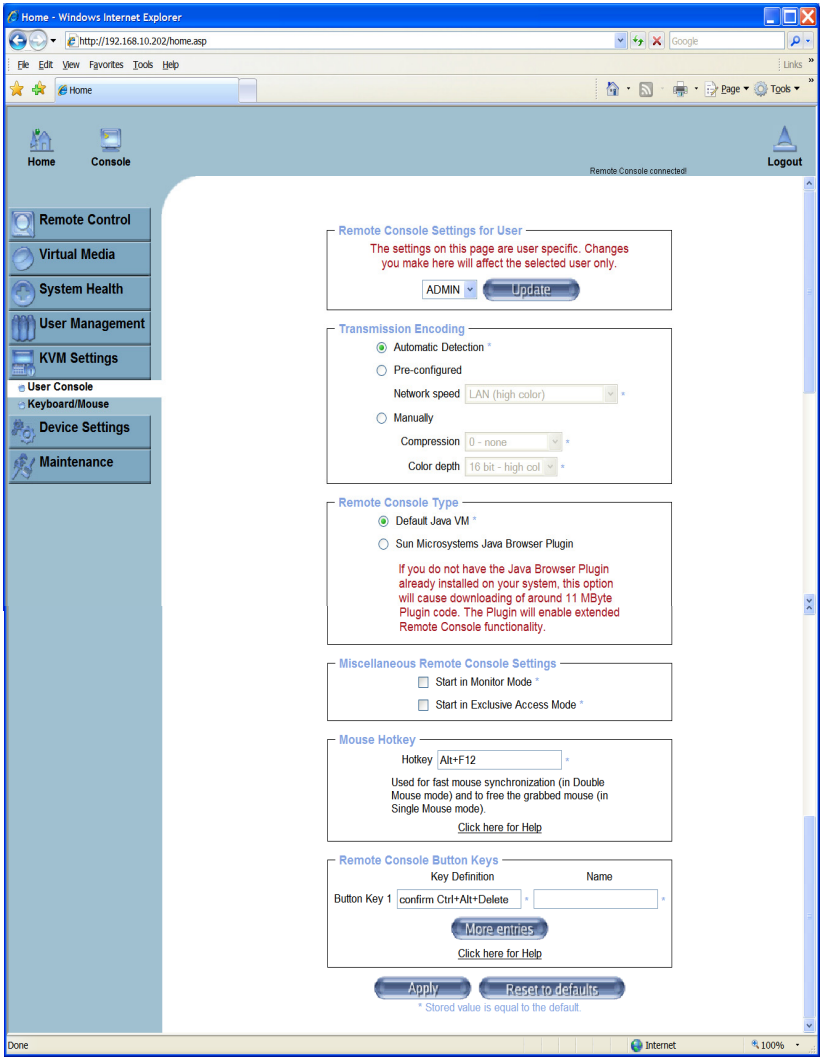
Permissions



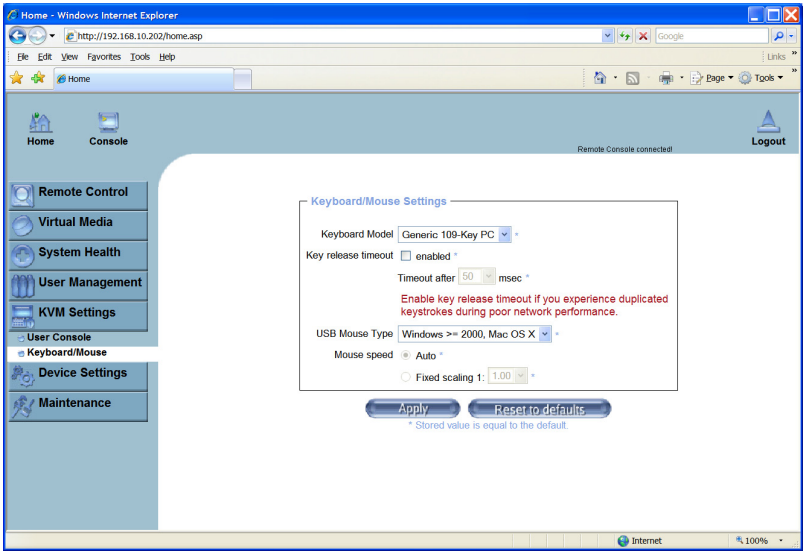
Each IPMI user has highly defined permissions which define which permission or capability is allowed. Users or groups can be created for monitoring, or defining each setting.

KVM Settings

The remote network console can be configured for different behaviors and functinoality. Some of the configurations include the button hot key functions and the screen sizes.


Home - Windows Internet Explorer
http://192.168.10.202/home.asp
File Edit View Favorites Tools Help
Home
Console
Logout
Remote Console connected!
Remote Control
Virtual Media
System Health
User Management
KVM Settings
User Console
Keyboard/Mouse
Device Settings
Maintenance
Remote Console Settings for User
The settings on this page are user specific. Changes you make here will affect the selected user only.
ADMIN
Update
Transmission Encoding
Automatic Detection *
Pre-configured
Network speed LAN (high color) *
Manually
Compression 0 - none *
Color depth 16 bit - high col *
Remote Console Type
Default Java VM *
Sun Microsystems Java Browser Plugin
If you do not have the Java Browser Plugin already installed on your system, this option will cause downloading of around 11 MByte Plugin code. The Plugin will enable extended Remote Console functionality.
Miscellaneous Remote Console Settings
Start in Monitor Mode *
Start in Exclusive Access Mode *
Mouse Hotkey
Hotkey Alt+F12 *
Used for fast mouse synchronization (in Double Mouse mode) and to free the grabbed mouse (in Single Mouse mode).
Click here for Help
Remote Console Button Keys
Key Definition
Name
Button Key 1 confirm Ctrl+Alt+Delete *
More entries
Click here for Help
Apply
Reset to defaults
* Stored value is equal to the default.
Done
Internet
100%

Keyboard/Mouse Settings

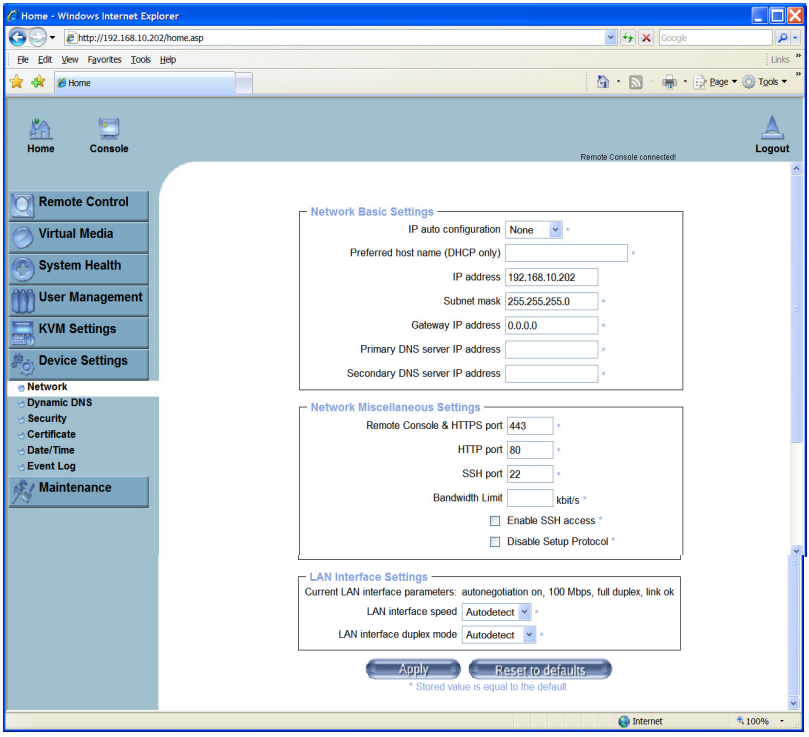


Several setttings for controlling the keyboard and mouse functionality are settable.

Device Settings

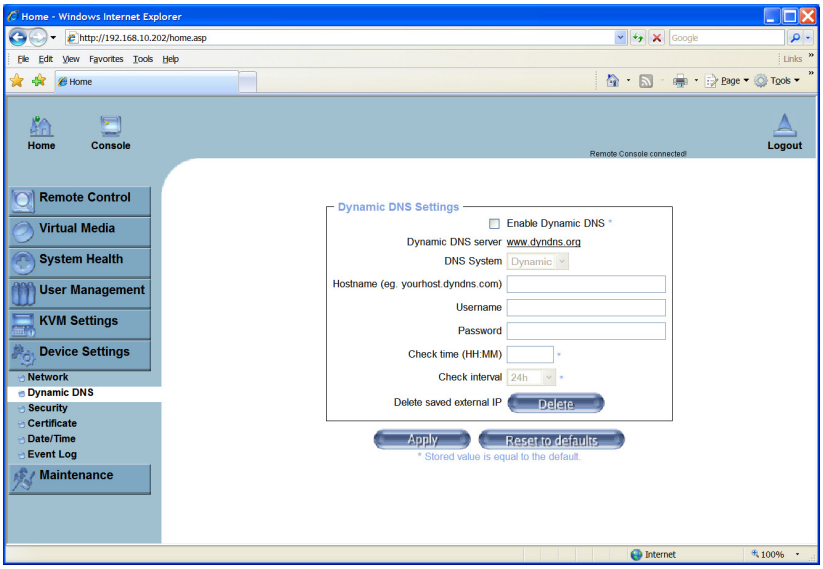
Network

The IP Network and LAN settings are configurable via the web interface.



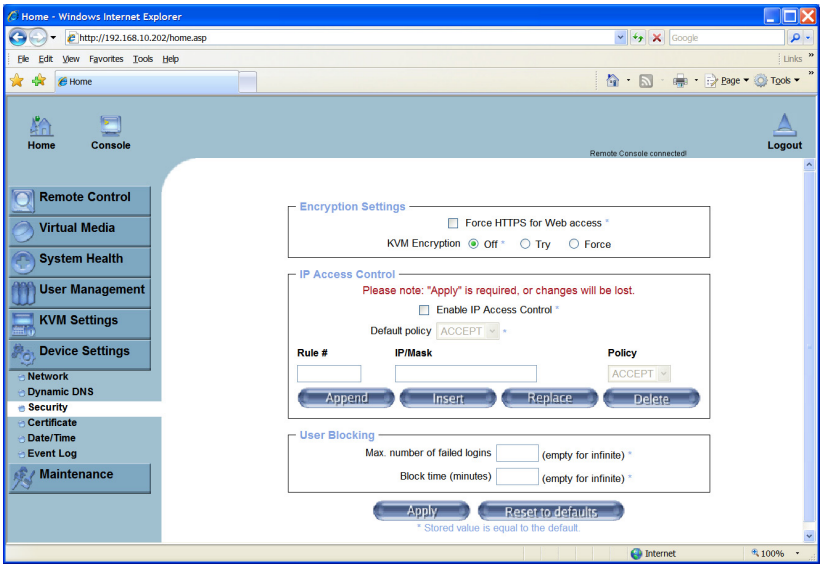
Dynamic DNS

The IPMI system supports dynamic DNS, especially useful for DHCP network implementations.



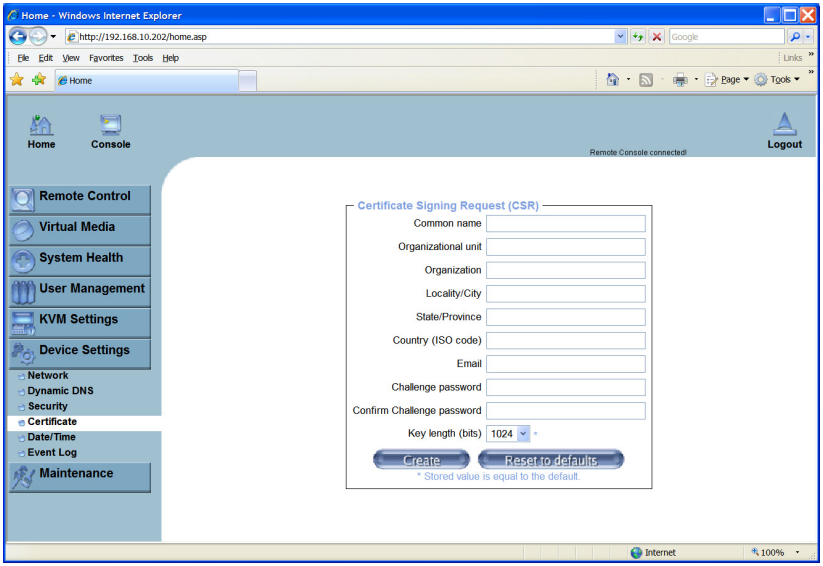
Security Settings

Security settings include login breakin detection for blocking out users after failed login attempts, firewall access lists for access control, and forcing SSL access for the KVM and web management.



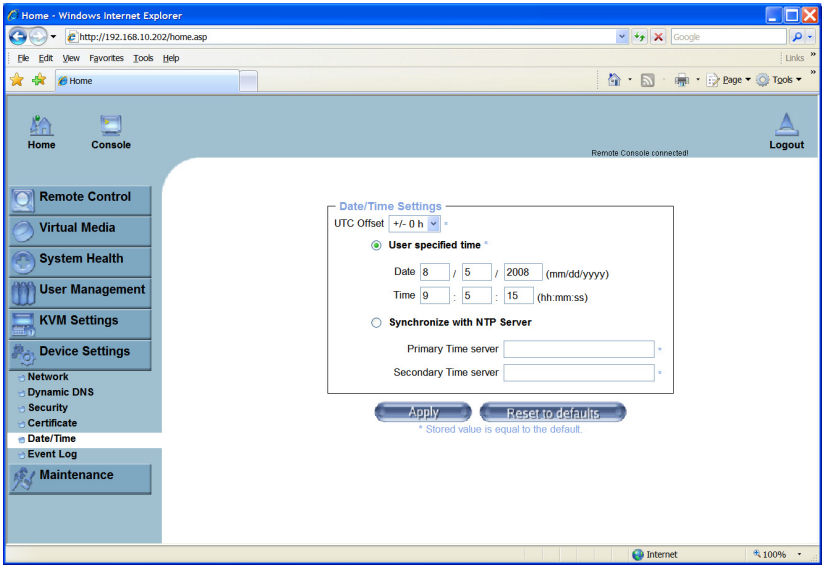
Certificate

An end point certificate can be defined.



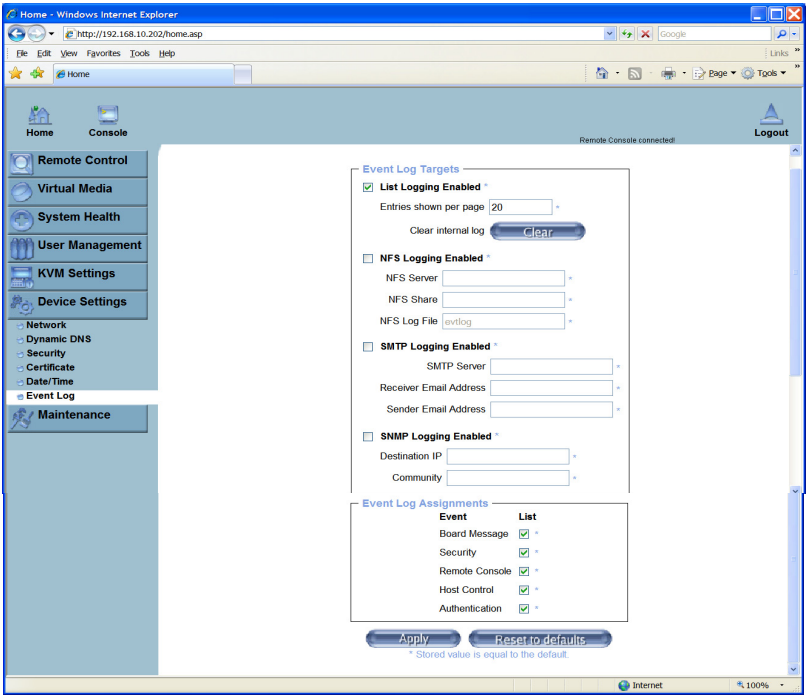
Date/Time

The system time and date can be defined as well as NTP settings for automatic time updates.



Event Log Settings

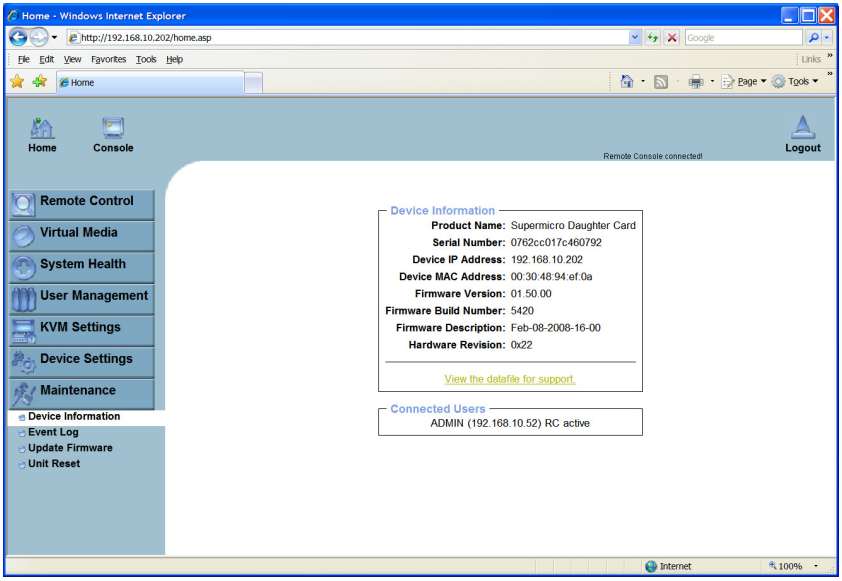
The events which occur can be redirected to remote file systems, remote logging systems, SNMP traps, etc.



Maintenance

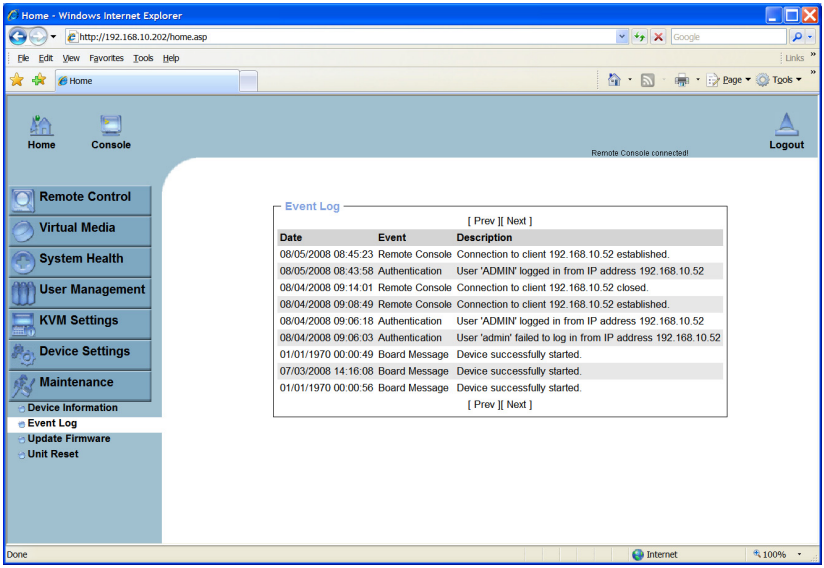
Specific system reports and upgrades are available.

Device Information



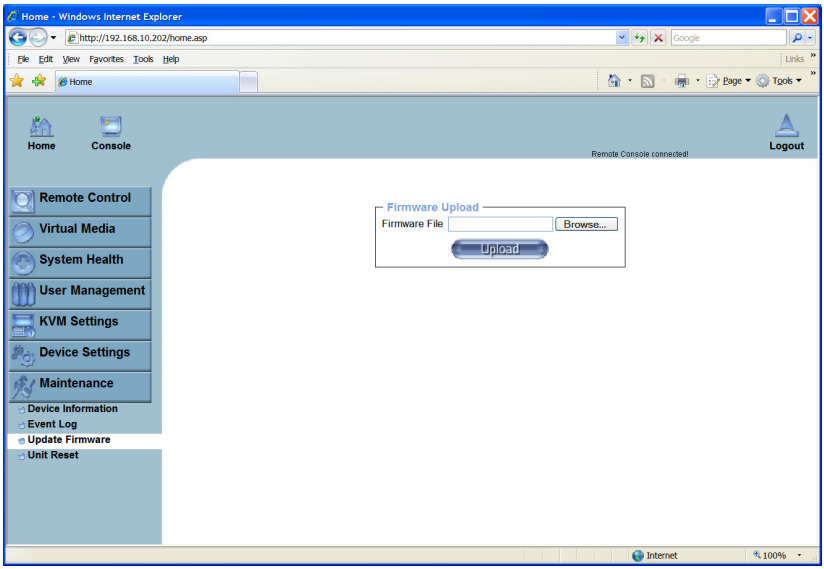
Event Log

Report listing of system events.



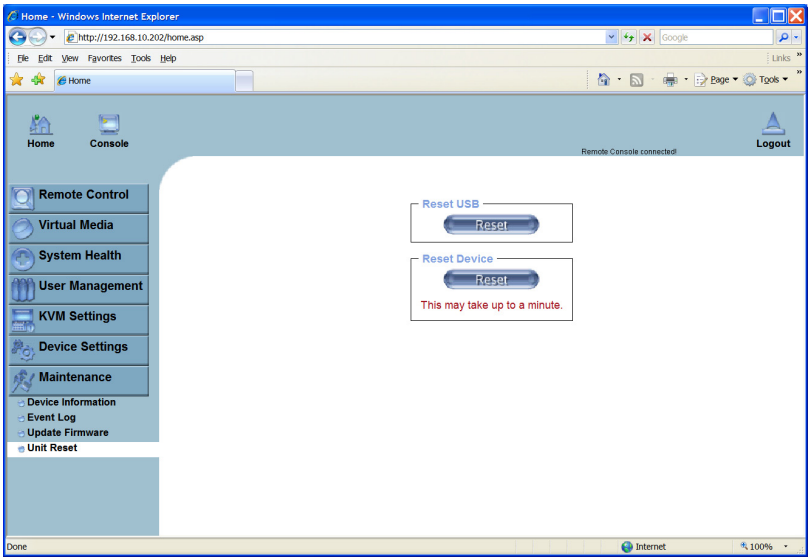
Update Firmware

A firmware file supplied by nAppliance can be applied to upgrade the IPMI software system.



Unit Reset

The USB interface, and the IPMI card can be hard rebooted with this screen.



Chapter 5: FFRS – Appliance Management Functions

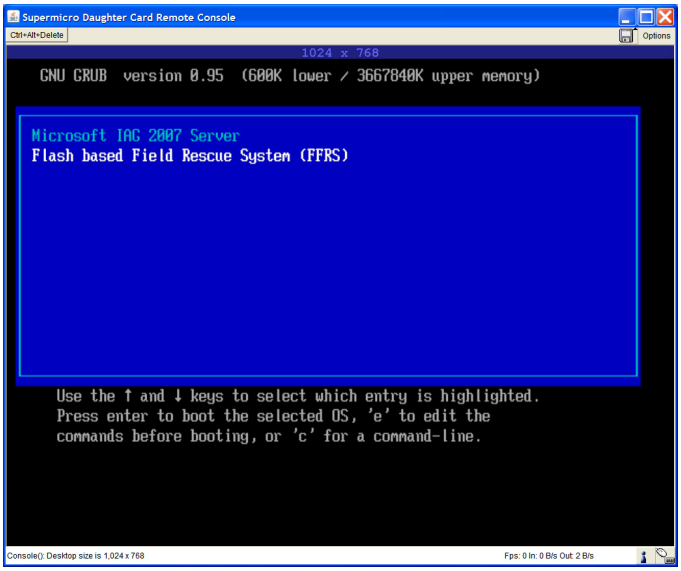
FFRS is the Flash based Field Recovery System, which is embedded on every nAppliance system within a DOM Flash drive. This system provides a set of management functions which can:

- Backup or Restore the complete system image of the appliance including the embedded applications
- Restore the appliance to it's factory default software configuration
- Manage the IPMI hardware interface and lights out console access system
- Provide other hardware or disk management functions performed during recovery or pre-boot

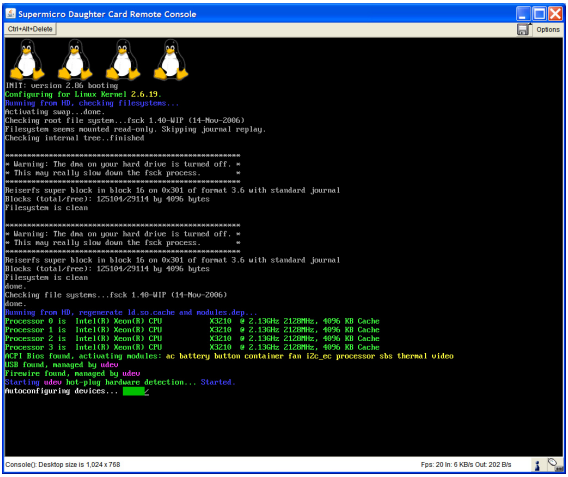
The FFRS is stored on a Flash Drive and can be booted independently of any operating environment running on the appliance. When combined with the IPMI remote console functionality and the OneFace Web Console, the nAppliance environment can be completely managed remotely over a network connection.

Running FFRS

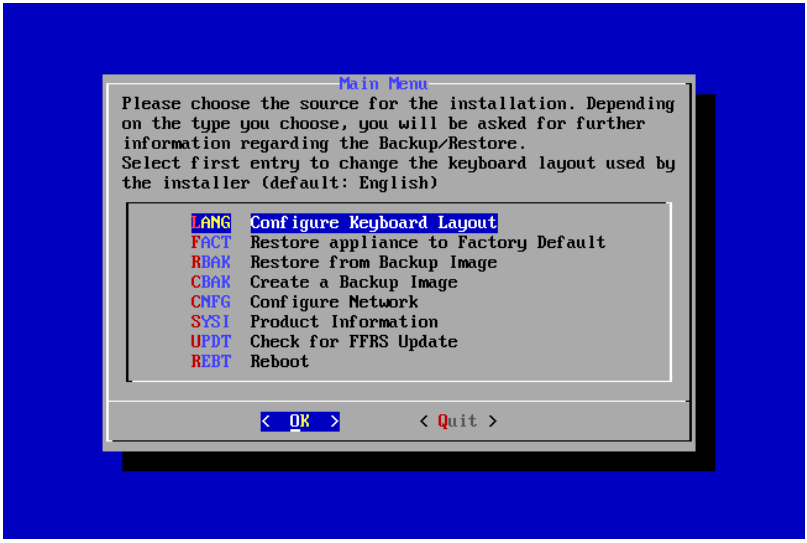
FFRS can be selected to boot during the appliance booting sequence. During the boot, the following screen will appear.



Select the FFRS option and the system will boot into a Linux environment.



Once FFRS is booted, the administrator will be presented with a menu of options. These menu items can be navigated through using the Up/Down arrow buttons, and an item can be selected by pressing the Enter key.



Configure Keyboard Layout

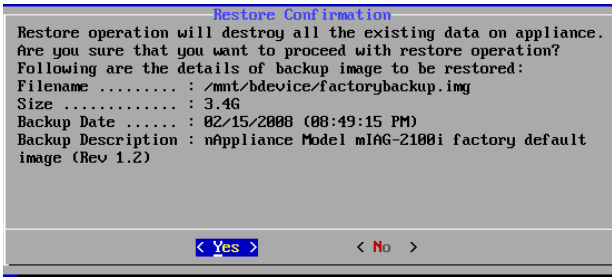
Currently there are two keyboard layouts available, German and English.

Restore Appliance to Factory Defaults

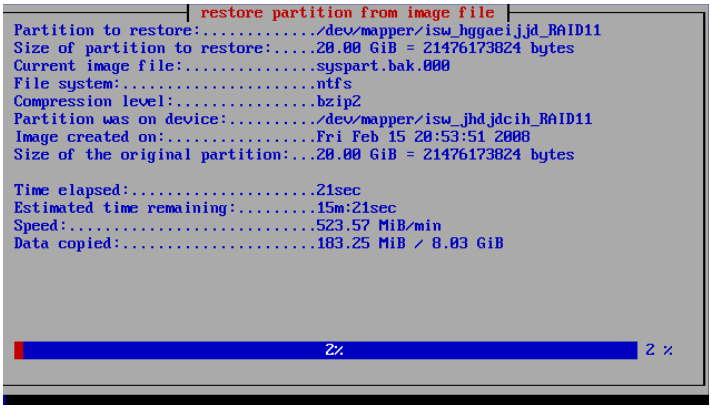
The appliance can be restored to factory defaults. This will completely replace the running operating system with a clean factory default version. This version will not have any user customizations.

The process will reload an operating system image, and in the case of Windows environments, will run through a set of installation and booting processes to recreate the environment.

Once this option is selected, the system will prompt to start the rebuild process.



When the restore is selected, a progress screen will appear. This will take at least 30 minutes depending on the system.



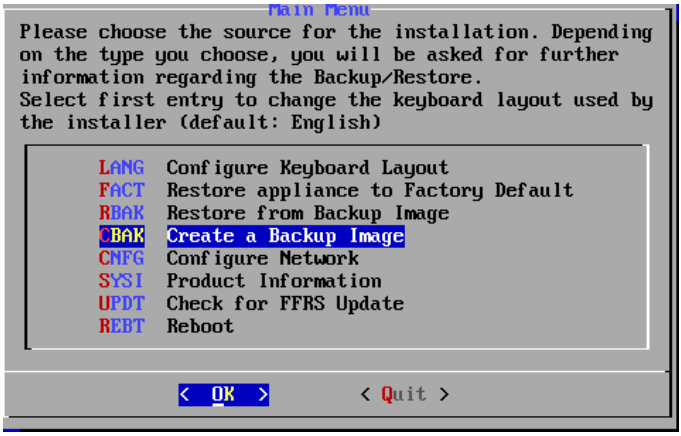
Once complete, the system will be booted into the environment state as it was shipped from nAppliance Networks.

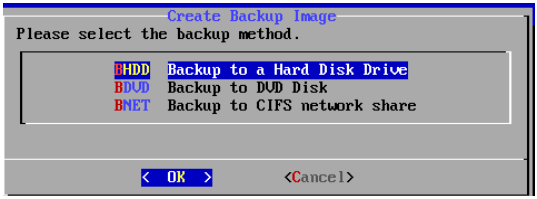
On Windows systems, the operating system license key will have to be manually entered. This license key is located on a decal on the outside of the appliance.

The system will also need to be reactivated using the Microsoft reactivation system.

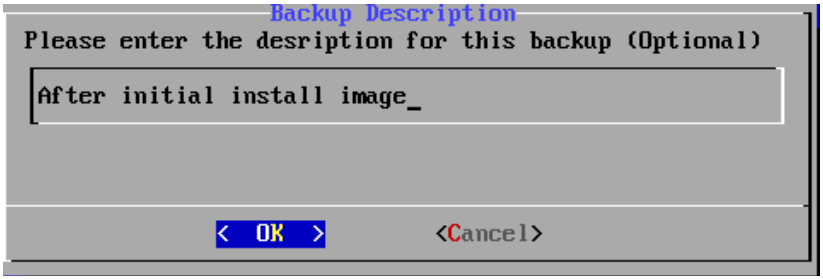
Backup Appliance Image

The FFRS system includes an option to backup the appliance image. The backup image can be saved to an external Windows Share, written to a DVD, or saved within another partition on the appliance.

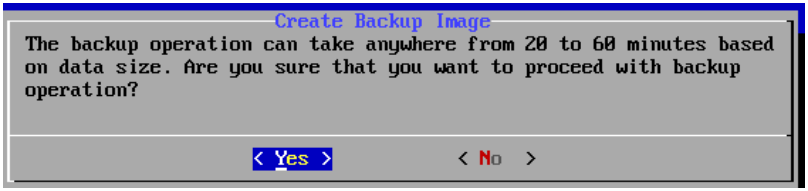




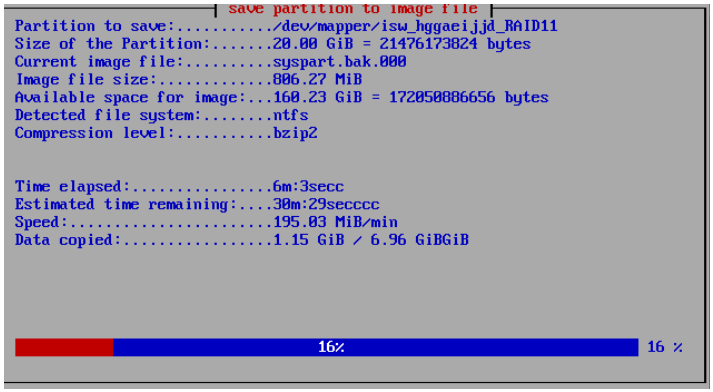
When selecting backup to a Hard Disk Drive (internal partition), the system will prompt for the backup image description. This description is used to select the backup image for restoration later.



The backup will prompt to continue backup.

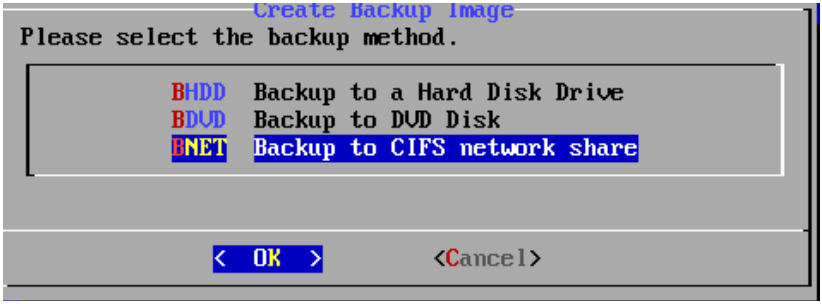


During the backup, the system will display a progress message box. Once complete the backup will reside on a partition and can be retrieved by the Restore process. This image can also be removed later if desired.

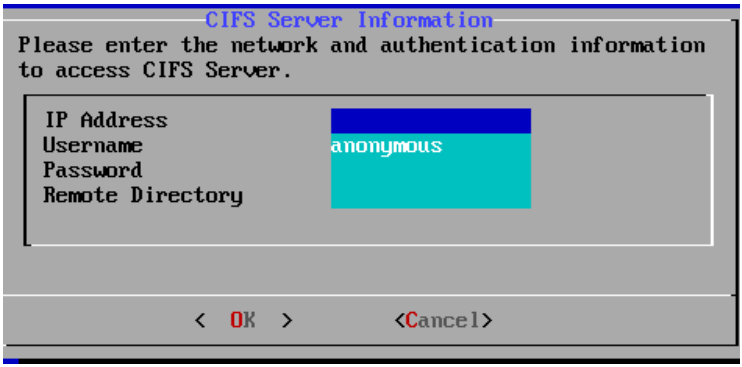


Backup to Network Share

An appliance image backup can be written to a Windows network share.



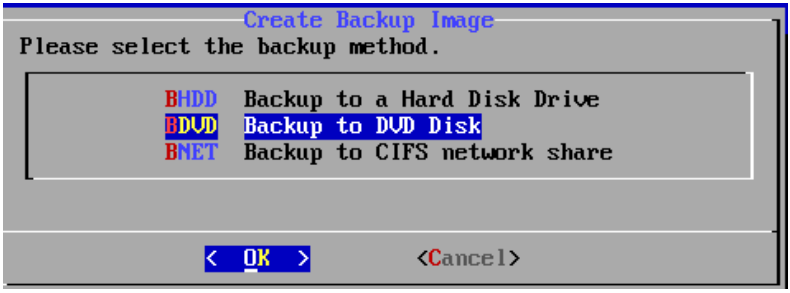
This backup option will prompt you for the credentials of the remote share.



After entering the credentials, the backup will continue as before.

Backup to DVD drive

An appliance image backup can be wrtten to an attached DVD drive. If the appliance does not have a writable DVD drive installed, attach an extenral USB DVD writable drive.

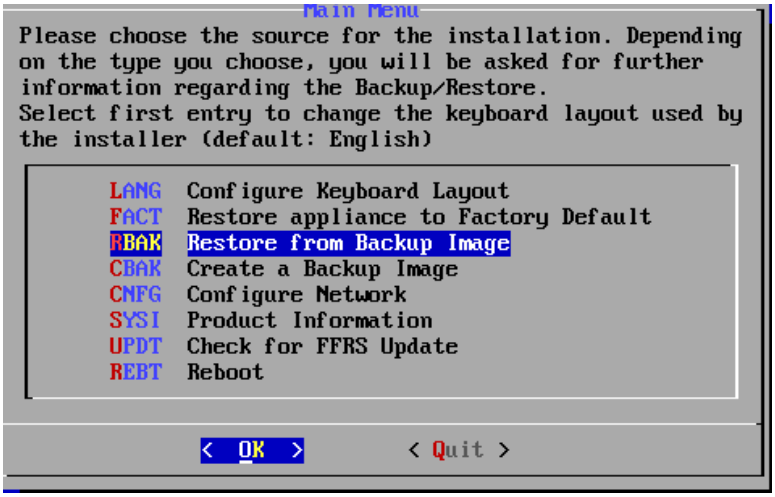


Once this option is selected, the system will attempt to mount the DVD.

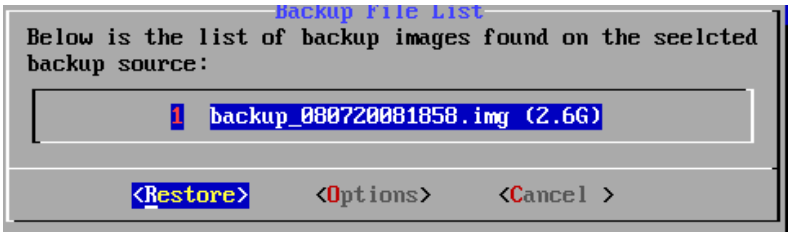
Once sucessful in accessing the drive, the backup will continue as normal.

Restore from Backup

The appliance image can be restored from prior appliance backups made by FFRS. These backups can be stored on DVD disks, on remote Wndows shares, or stored locally on the appliance on a special partition.



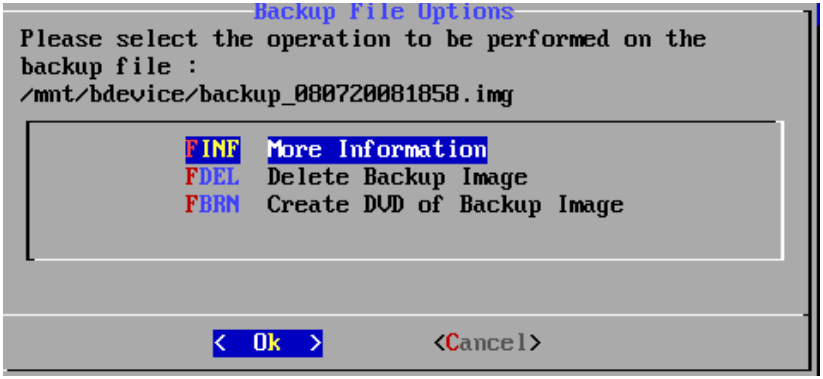
When restoring from a local partition image, the system will allow you to select the backup image.



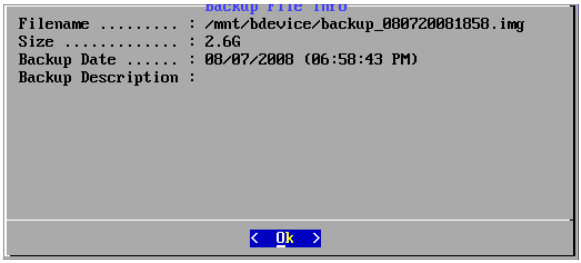
After selecting the backup image, the restore will continue.

Restore Options Tab

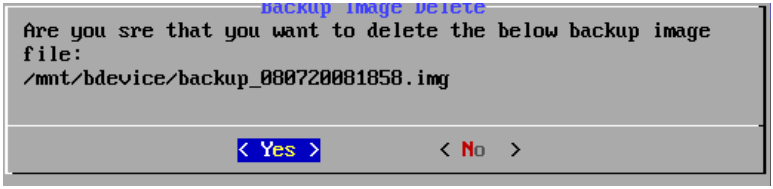
Under the options tab, there are several options available to allow you to review the backups and select the correct version.



More Information – Display the details of the backup image file.

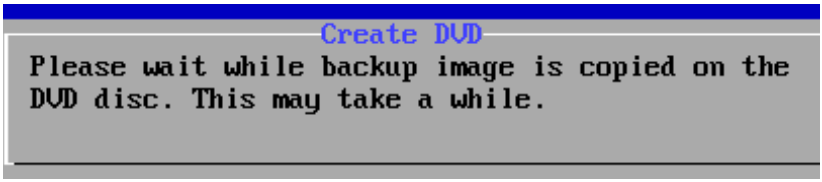


Delete Backup Image – Select the image from the list for deletion.


Backup Image Delete
Are you sre that you want to delete the below backup image file:
/mnt/bdevice/backup_080720081858.img
< Yes >
< No >

Create DVD of Backup Image

A copy of the backup image stored on the local partition can be written to a DVD. Select this option to write to an embedded DVD drive or attach an external USB DVD drive.



Product Information

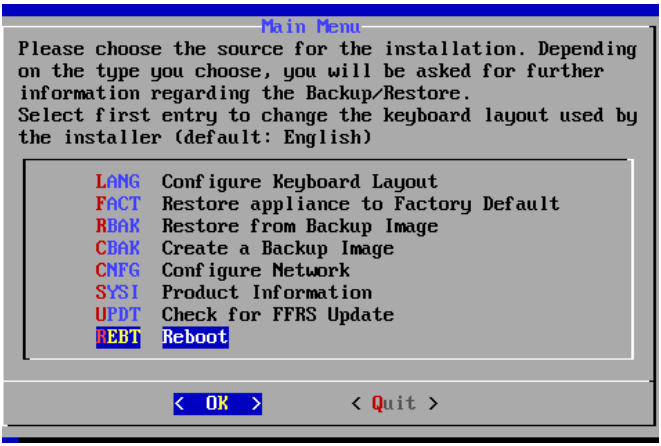
```
Main Menu
Please choose the source for the installation. Depending
on the type you choose, you will be asked for further
information regarding the Backup/Restore.
Select first entry to change the keyboard layout used by
the installer (default: English)

        LANG  Configure Keyboard Layout
        FACT  Restore appliance to Factory Default
        RBAK  Restore from Backup Image
        CBAK  Create a Backup Image
        CNFG  Configure Network
        SYSI  Product Information
        UPDT  Check for FFRS Update
        REBT  Reboot

                < OK >          < Quit >
```

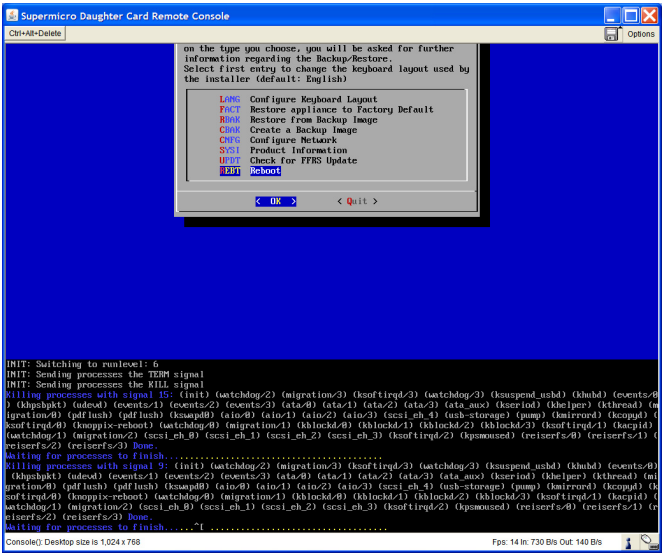
The Product Information function will list product details such as hardware and software models and versions.

```
Appliance Information
Product Name... : mIAG-2100I.
Serial Number.. : NN03081064
BIOS Rev....... : 6.00 (12/14/2007)
Processor Model : Intel(R) Xeon(R) CPU X3210 @ 2.13GHz
Processor Speed : 2.08GHz
Windows License : KM8FW-3TRWM-DXBXP-FRHBR-TVCTM
FFRS Version... : 1.07 (04/16/2008)

For product support, please call 1-800-921-nAPP (6277) Ext. 400
or send an email to support@nappliance.com.

                < OK >
```

Reboot Appliance

The reboot function will reboot the appliance. This is used to exit FFRS and return to the default running image on the appliance.

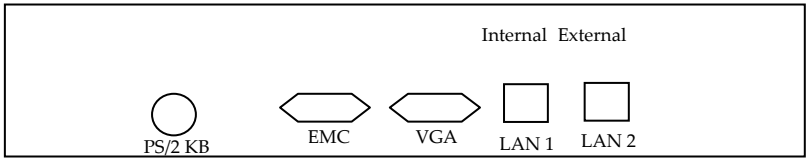




Appendix 1 – Hardware Port Configurations

mIAG-500i
iIAG-1100i

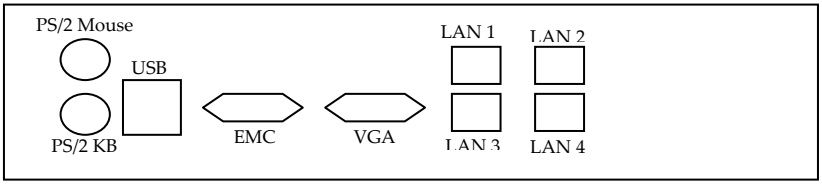
I/O Ports



IPMI (Optional): Internal will also be used as IPMI port

mISA-500w
mISA-1100B
mISA-1100W

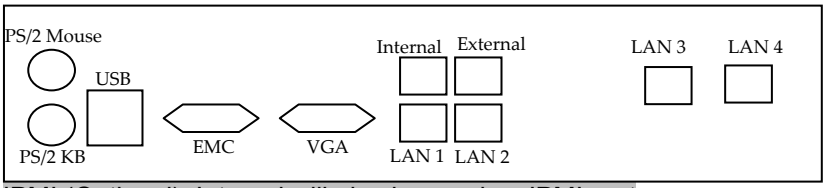
I/O Ports



IPMI (Optional): LAN 1 will also be used as IPMI port

mIAG-1200i

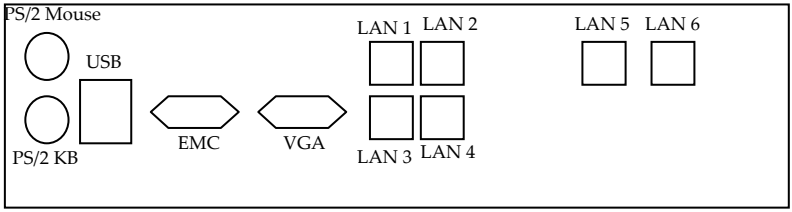
I/O Ports



IPMI (Optional): Internal will also be used as IPMI port

mISA-1200W
mISA-1200B
mISAE-1500E

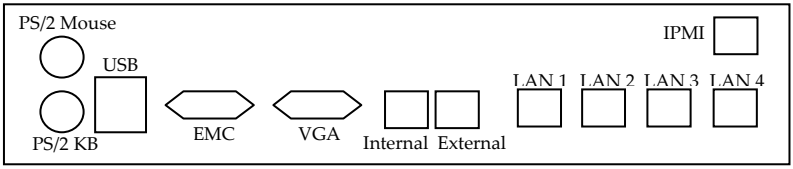
I/O Ports



IPMI (Optional): LAN 1 will also be used as IPMI port

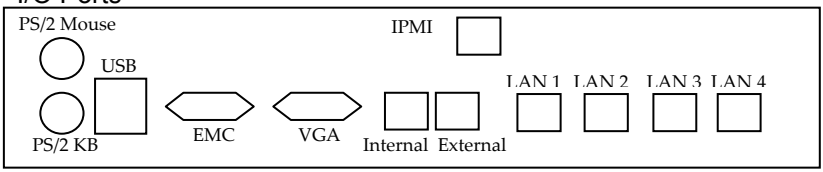
mIAG-2100i

I/O Ports



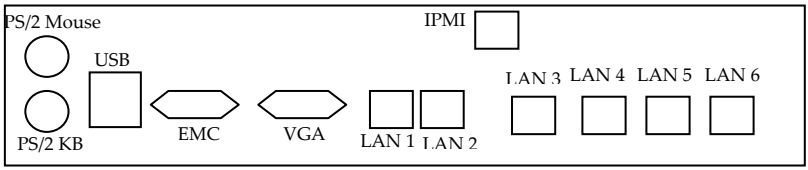
mIAG-2200i

I/O Ports



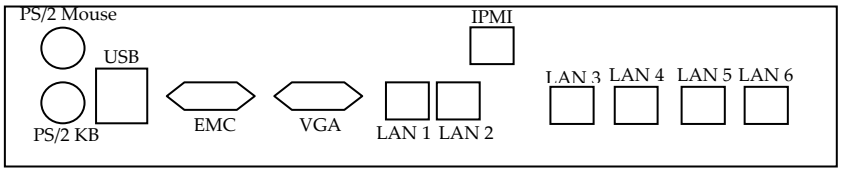
mISAE-2100E/B
mISA-2100S

I/O Ports



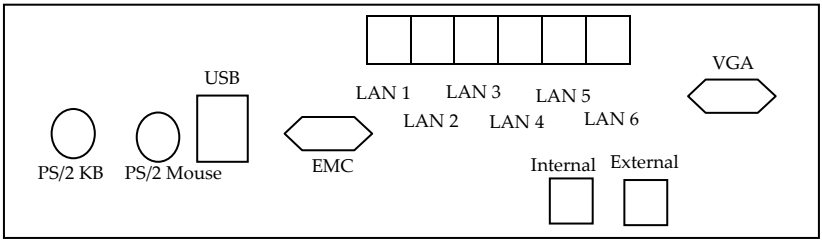
mISAE-2200E/B
mISA-2200S

I/O Ports



mIAG-3200i

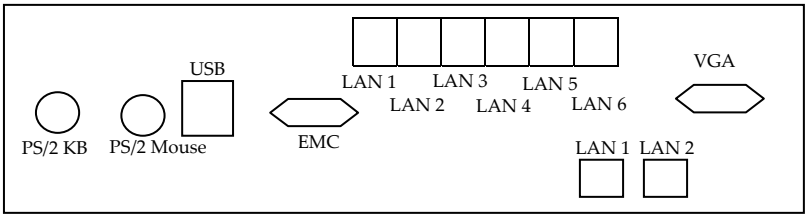
I/O Ports



IPMI: Internal will also be used as IPMI port

mISAE-3200E/B
mISA-3200S

I/O Ports



IPMI: LAN 1 will also be used as IPMI port

Index

L

M

N

O

P

R

S

T

U

V

W