

ExtremeSwitching™

Open Networking Adapter 1101GT Installation Job Aid

Release 3.0
December 2017

This *Installation Job Aid* provides an overview of your Open Networking Adapter (ONA).



Training

Ongoing product training is available. For more information or to register, you can access the Web site at www.extremenetworks.com/education/.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at internalinfodev@extremenetworks.com

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- [GTAC \(Global Technical Assistance Center\) for Immediate Support](#)
 - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
 - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- [GTAC Knowledge](#) – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- [The Hub](#) – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- [Support Portal](#) – Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)

- Any related RMA (Return Material Authorization) numbers

Extreme Networks Documentation

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for previous versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing.

Subscribing to Service Notifications

Subscribe to receive an email notification for product and software release announcements, Vulnerability Notices, and Service Notifications.

About this task

You can modify your product selections at any time.

Procedure

1. In an Internet browser, go to <http://www.extremenetworks.com/support/service-notification-form/>.
2. Type your first and last name.
3. Type the name of your company.
4. Type your email address.
5. Type your job title.
6. Select the industry in which your company operates.
7. Confirm your geographic information is correct.
8. Select the products for which you would like to receive notifications.
9. Click **Submit**.

© 2017 Extreme Networks

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Extreme Networks assumes no liability for any errors. Extreme Networks reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes. For the most current versions of Documentation, see the Extreme Networks Documentation website: www.extremenetworks.com/documentation/ or such successor site as designated by Extreme Networks. For a list of support telephone numbers and contact addresses, see the Extreme Networks support website: <http://www.extremenetworks.com/support/contact/>.

Warranty for Extreme Products

Extreme Networks provides a limited warranty on Extreme Networks hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Extreme Networks' standard warranty language, as well as information regarding support for this product while under warranty is available to Extreme Networks customers and other parties through the Extreme Networks Support website: <http://www.extremenetworks.com/support> under the link "Policies" or such successor site as designated by Extreme Networks. Please note that if You acquired the product(s) from an authorized Extreme Networks Channel Partner outside of the United States and Canada, the warranty is provided to You by said Extreme Networks Channel Partner and not by Extreme Networks.

International Regulatory Statements of Conformity

This is to certify that the device was evaluated to the international regulatory standards for electromagnetic compliance (EMC) and safety and were found to have met the requirements for the following international standards:

- EMC—Electromagnetic Emissions—CISPR 22, Class B
- EMC—Electromagnetic Immunity—CISPR 24
- Electrical Safety—IEC 60950-1, with CB member national deviations

Further, the equipment has been certified as compliant with the national EMC standards as detailed in the following sections.

FCC Statement (USA only)

This device complies with Part 15 of the Federal Communications Commission (FCC) rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

ICES Statement (Canada only)

Canadian Department of Communications Radio Interference Regulations:

Complies with the Canadian ICES-003 Class B specifications.

Cet appareil numérique de la Classe B est conforme a la norme NMB-003 du Canada.

This device complies with RSS 210 of Industry Canada. This Class B device meets all the requirements of the Canadian interference-causing equipment regulations.

Cet appareil numérique de la Classe B respecte toutes les exigences du Règlement sur le matériel brouiller du Canada.

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil est conforme aux normes CNR exemptes de licence d'Industrie Canada. Le fonctionnement est soumis aux deux conditions suivantes: (1) cet appareil ne doit pas provoquer d'interférences et (2) cet appareil doit accepter toute interference, y compris celles susceptibles de provoquer un fonctionnement non souhaité de l'appareil

Restriction on Hazardous Substances Directive Compliance Statement

The Restriction on Hazardous Substances (RoHS) Directive (2011/65/EU), which accompanies the WEEE Directive, bans the use of heavy metals and brominated flame-retardants in the manufacture of electrical and electronic equipment. Specifically, restricted materials under the RoHS Directive are Lead (including solder used in PCBs), Cadmium, Mercury, Hexavalent Chromium, and Bromine.

Extreme Networks declares compliance with the European Union (EU) RoHS Directive (2011/65/EU) in that Lead, which is a restricted hazardous substance, is used only in accordance to the exemption(s) to Article 4(1), item 7 granted by the European Union.

Extreme Networks declares compliance with the European Union (EU) RoHS Directive (2011/65/EU) in that Lead, which is a restricted hazardous substance, is used only in accordance to the exemption(s) to Article 4(1), item 7 granted by the European Union (EU) RoHS Directive (2011/65/EU) in the Annex —"lead in solders for network infrastructure equipment for switching, signalling, transmission as well as network management for telecommunication".

Notices and Safety Messages

*** Note:**

This device is not intended for use in the direct field of view at visual display workplaces. To avoid incommoding reflections at visual display workplaces this device must not be placed in the direct field of view.

*** Note:**

The device has no essential performance per IEC 60601-1-2.

⚠ Caution:

Take special precautions with MEDICAL ELECTRICAL EQUIPMENT regarding EMC. It must be installed and put in service according to the EMC information provided above in International Regulatory Statements of Conformity.

⚠ Caution:

Portable and mobile RF communications equipment can affect MEDICAL ELECTRICAL EQUIPMENT.

⚠ Caution:

The use of accessories other than those specified may result in increased emissions or decreased immunity of the device.

⚠ Warning:

The equipment should not be used adjacent to or stacked with other equipment. If adjacent or stacked use is necessary, you must observe the equipment to verify normal operation in the configuration in which it is to be used.

Declarations and Specifications

Guidance and manufacturer's declaration – electromagnetic immunity			
The ONA 1101GT is intended for use in the electromagnetic environment specified below. The customer or the user of the ONA 1101GT should assure that it is used in such an environment.			
Immunity test	IEC 60601 test level	Compliance level	Electromagnetic environment - guidance
Electrostatic Discharge (ESD) IEC 61000-4-2	± 6 kV contact ± 8 kV air	± 6 kV contact ± 8 kV air	Floors should be wood, concrete or ceramic tile. If floors are covered with synthetic material, the relative humidity should be at least 30 %.
Electrical fast transient/burst IEC 61000-4-4	± 2 kV for power supply lines ± 1 kV for input/output lines	± 2 kV for power supply lines ± 1 kV for input/output lines	
Surge IEC 61000-4-5	± 1 kV line(s) to line(s) ± 2 kV line(s) to earth	± 1 kV line(s) to line(s) ± 2 kV line(s) to earth	
Voltage dips, short interruptions and voltage variations on power supply input lines IEC 61000-4-11	<5 % U_t (>95 % dip in U_t) for 0.5 cycle 40 % U_t (60 % dip in U_t) for 5 cycles	<5 % U_t (>95 % dip in U_t) for 0.5 cycle 40 % U_t (60 % dip in U_t) for 5 cycles	


Table continues...

Guidance and manufacturer's declaration – electromagnetic immunity			
	70 % U_t (30 % dip in U_t) for 25 cycles <5 % U_t (>95 % dip in U_t) for 5 s	70 % U_t (30 % dip in U_t) for 25 cycles <5 % U_t (>95 % dip in U_t) for 5 s	
Power frequency (50/60 Hz) magnetic field IEC 61000-4-8	3 A/m	3 A/m	Power frequency magnetic fields should be at levels characteristic of a typical location in a typical commercial or hospital environment.
NOTE U_t is the a.c. mains voltage prior to application of the test level.			

Guidance and manufacturer's declaration – electromagnetic immunity			
The ONA 1101GT is intended for use in the electromagnetic environment specified below. The customer or the user of the ONA 1101GT should assure that it is used in such an environment.			
Immunity test	IEC 60601 test level	Compliance level	Electromagnetic environment - guidance
Conducted RF IEC 61000-4-6 Radiated RF IEC61000-4-3	3 Vrms 150 kHz to 80 MHz 3 V/m 80 MHz to 2.5 GHz	3 V 3 V/m	Portable and mobile RF communication equipment should be no closer to any part of the ONA 1101GT, including cables, than the recommended separation distance calculated from the equation applicable to the frequency of the transmitter. Recommended separation distance $d = 1.17 \cdot \sqrt{P}$ $d = 1.17 \cdot \sqrt{P}$ 80 MHz to 800 MHz $d = 2.33 \cdot \sqrt{P}$ 800 MHz to 2.5 GHz Where P is the maximum output power rating of the

Table continues...

Guidance and manufacturer's declaration – electromagnetic immunity

			<p>transmitter in watts (W) according to the transmitter manufacturer and d is the recommended separation distance in metres (m).</p> <p>Field strengths from fixed RF transmitters, as determined by an electromagnetic site survey^a, should be less than the compliance level in each frequency range^b.</p> <p>Interference may occur in the vicinity of equipment marked with the following symbol:</p> 
--	--	--	--

NOTE 1 At 80 MHz and 800 MHz, the higher frequency range applies.

NOTE 2 These guidelines may not apply in all situations. Electromagnetic propagation is affected by absorption and reflection from structures, objects and people.

^a Field strengths from fixed transmitters, such as base stations for radio (cellular/cordless) telephones and land mobile radios, amateur radio, AM and FM radio broadcast and TV broadcast cannot be predicted theoretically with accuracy. To assess the electromagnetic environment due to fixed RF transmitters, an electromagnetic site survey should be considered. If the measured field strength in the location in which the ONA 1101GT is used exceeds the applicable RF compliance level above, the ONA 1101GT should be observed to verify normal operation. If abnormal performance is observed, additional measures may be necessary, such as re-orienting or relocating the ONA 1101GT.

^b Over the frequency range 150 kHz to 80 MHz, field strengths should be less than 3 V/m.

Recommended separation distances between portable and mobile RF communication equipment and the ONA 1101GT

The ONA 1101GT is intended for use in an electromagnetic environment in which radiated RF disturbances are controlled. The customer or the user of the ONA 1101GT can help prevent electromagnetic interference by maintaining a minimum distance between portable and mobile RF communications equipment (transmitters) and the ONA 1101GT as recommended below, according to the maximum output power of the communications equipment.

Table continues...

Recommended separation distances between portable and mobile RF communication equipment and the ONA 1101GT

Rated maximum output power of transmitter W	Separation distance according to frequency of transmitter m		
	150 kHz to 80 MHz $d = 1.17 * \sqrt{P}$	80 MHz to 800 MHz $d = 1.17 * \sqrt{P}$	800 MHz to 2.5 GHz $d = 2.33 * \sqrt{P}$
0.01	0.12	0.12	0.23
0.1	0.37	0.37	0.74
1	1.17	1.17	2.33
10	3.7	3.7	7.37
100	11.7	11.7	23.3

For transmitters rated a maximum output power not listed above, the recommended separation distance d in metres (m) can be estimated using the equation applicable to the frequency of the transmitter, where P is the maximum output power rating of the transmitter in watts (W) according to the transmitter manufacturer.

NOTE 1 At 80 MHz and 800 MHz, the separation distance for the higher frequency range applies.

NOTE 2 These guidelines may not apply in all situations. Electromagnetic propagation is affected by absorption and reflection for structures, objects and people.

Compliant Accessories

This table lists the manufacturer compliant accessories for the ONA 1101GT.

Accessory	Description	Part Number
AC/DC Adapter	ASIAN POWER DEVICES INC; LITE ON TECHNOLOGY CORP WB-10E05R	EC1105E11-E6

Regulatory label for Brazil



Starting the ONA

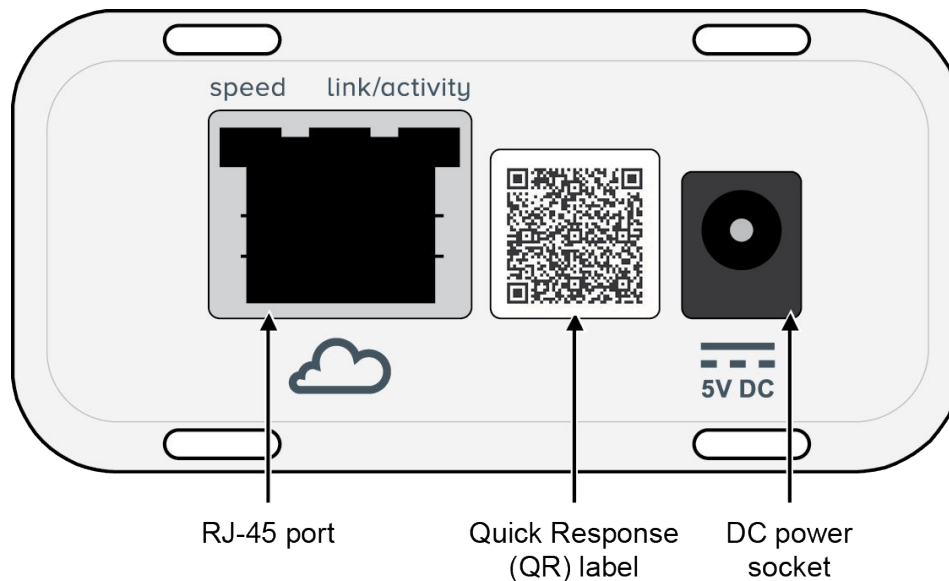
There are two ways to power the ONA, but you CANNOT use both ways at the same time:

- Connect a cable from a POE, POE+, or uPOE port on an Ethernet switch to the RJ-45 port with the cloud symbol on the ONA.
- Use the optional external power adapter. This adapter can supply power to the ONA if there is no PoE port available or, as a backup, if the PoE port fails.

*** Note:**

The Status LED flashes slow blinking blue as the ONA starts diagnostic tests. If you did not start any tests, the ONA bypasses the Diagnostics and slow blinks amber during boot up. This is normal and does not indicate any error.

Connecting the ONA to the network



Procedure

1. Use a QR code reader application to get information about your ONA. The following is a sample of the information in the QR code. QR code information is subject to change.
 - SERIAL:xxxxxxxxxxxxxxxx (Serial number of this ONA)
 - MAC:xx:xx:xx:xx:xx:xx (MAC address)
 - MACNUM:16 (This ONA can have one of 16 MAC addresses. The 16 total MAC addresses available start with the address reported above in the MAC field and includes the next consecutive 15 addresses.)
 - PEC:EC1100010-E6 (Extreme Networks part number)
 - MAN:EXTREME (Manufacturer's name — Extreme Networks)
 - MOD:ONA 1101GT (Model number)
 - REV:xxx (Revision number of this ONA)
2. Use the 10/100/1000 BASE-T RJ-45 port with the cloud symbol to connect the ONA to the network. If the upstream switch port is POE, POE+, or uPOE capable, it will also power on the ONA.

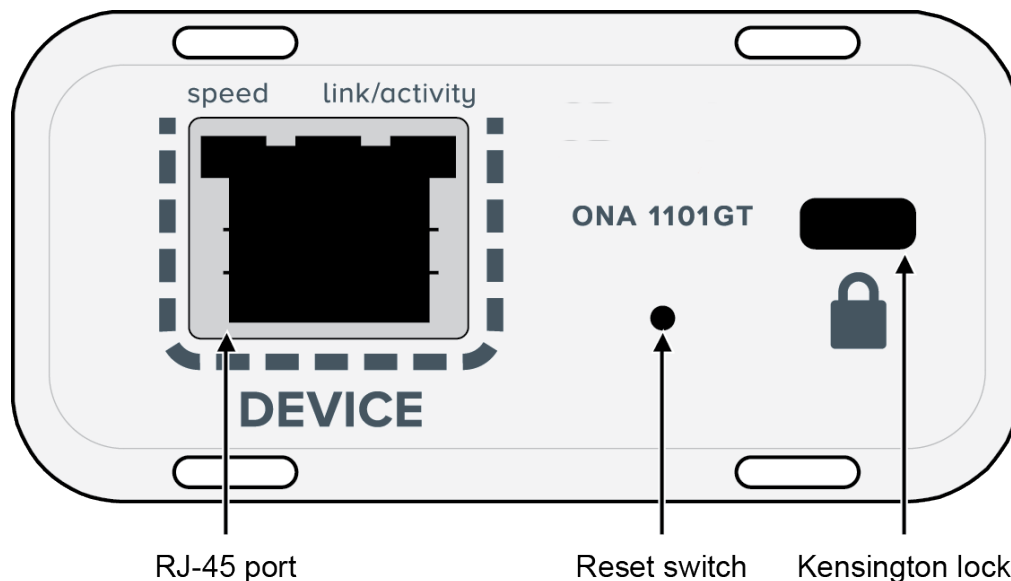
3. If PoE power is unavailable, connect the wall unit power adapter into the DC socket to provide direct power.

The 10W 100–240 AC power adapter is sold separately and comes with four snap-in plug adapters: Type A (U.S. and Japan), Type B (EU), Type G (UK), and Type I (AUS and China). The part number is EC1105E11-E6.

4. (Optional) The ONA comes with zip ties that you can use to mount the ONA near the wall unit power adapter, the device connected to the ONA, or any location you desire. There are four slots on the top of the ONA and four slots on the bottom to give you multiple options for securing the ONA.

Connecting your device to the ONA

Use the following figure and steps to connect your device to the ONA.



Procedure

1. Connect your device to the ONA using the 10/100/1000 BASE-T RJ-45 DEVICE port.
2. (Optional) Secure your ONA by attaching a Kensington lock to the slot above the lock icon.
3. If necessary, you can reset your ONA by inserting a paper clip into the reset switch pin hole and pressing the switch for more than 1 second but less than 5 seconds.

Setting the ONA to factory defaults

The following parameters are the ONA factory defaults:

- Management IP Address :

- Management IP Subnet Mask :
- Default Gateway IP Address :
- Primary DNS Server IP Address :
- Secondary DNS Server IP Address :
- DNS Domain Name :
- SDN Controller IP Address or Name :
- Syslog Server IP Address :
- Operational Mode : 0
- Password :

*** Note:**

All the fields are empty except the Operational Mode, which is 0 for the SDN Controller Mode.

Use the following procedure if you want to reset the ONA to the factory default parameters:

Procedure

1. Wait until the ONA starts and the Status LED flashes green. (You can enter this mode anytime after the ONA starts.)
2. On the Device side of the ONA, insert a paper clip into the reset switch and depress it for at least five seconds. This action clears the parameters so they are all empty fields (except for Operating Mode) and then resets the ONA.

ONA Operational Modes

The ONA has two operational modes:

- SDN Controller Mode (Mode 0, the default mode)
- Fabric Extend Mode (Mode 1)

During reboot, the system checks the Mode parameter and proceeds accordingly. The ONA stays in the mode you select unless you depress the reset button for at least five seconds. This causes the ONA to revert back to the factory default parameters.

To change operational modes, use the Manual Configuration menu as described in the next section [Modifying Manual Configuration parameters](#) on page 14.

You can also use the Manual Configuration menu to modify any of the other factory default parameters. After you modify the parameters and save the configuration, the ONA stores your changes in persistent memory and reboots.

*** Note:**

Manual Configuration menu changes for default parameters are not required for SDN Controller Mode 0 operation.

ONA can be configured with a Management IP address using DHCP. If no DHCP server is available to provide the IP address to the ONA, use the Manual Configuration menu to configure the following:

- IP address in the "Management IP Address" field
- Subnet mask in the "Management IP Subnet Mask" field
- Default gateway in the "Default Gateway IP Address" field
- (For Mode 0 only) IP address of the controller in the "SDN Controller IP Address or Name" field

Setting the ONA to SDN Controller Mode 0

The SDN Controller Mode (Mode 0) enables the ONA to use the Fabric Attach feature, and establish control plane communication with the SDN Controller. In Mode 0, the ONA must communicate with an Extreme Networks SDN Controller to operate correctly.

The ONA ships in Mode 0. If the mode changed and you want to use Mode 0, use one of the following methods:

- Use the Manual Configuration menu to configure the "SDN Controller IP Address or Name" and set the "Operational Mode" to 0.
- Depress the reset button for at least five seconds to reset the ONA back to the factory default settings. This method clears all the parameters in persistent memory (including the controller's IP address) and sets the Operational Mode to 0. Because the "SDN Controller IP Address or Name" is not configured when the ONA boots up, it uses a DNS query to get the SDN Controller's IP address and initiates a connection to the controller.

Setting the ONA to Fabric Extend Mode 1

The Fabric Extend Mode (Mode 1) enables the ONA to use the Fabric Extend feature. After you select this mode, the ONA reboots and stays in Mode 1 unless you depress the reset button for at least five seconds to enter SDN Controller Mode.

Modifying Manual Configuration parameters

To access the Manual Configuration menu to modify the parameters, press and hold the reset button during a power on sequence.

Use the following procedure:

Procedure

1. Connect a PC to the RJ-45 port on the Device side of the ONA.
2. Insert a paper clip into the reset switch. Press and hold the reset button before applying power to the ONA.
3. Connect the cable from the network switch to the Network side of the ONA for PoE power. If PoE power is unavailable, connect an external power adapter.
4. Continue pressing and holding the reset button until the Status LED cycles through a red/green/blue pattern. Then release the reset button. The Status LED will flash a steady amber, which indicates that the Manual Configuration menu is running.

5. On the PC, use a browser to connect to the ONA configuration menu with the address <http://192.168.100.1>.
6. Click Edit Parameters.
7. Modify the configuration parameters that you want to change.
8. Click "Save" to store the parameters in persistent memory.
9. Click "Return to Configuration page."
10. Click "Reboot into Operational Mode."
11. Disconnect the PC.

System Status LED

The System Status LED is visible from either side of the unit.

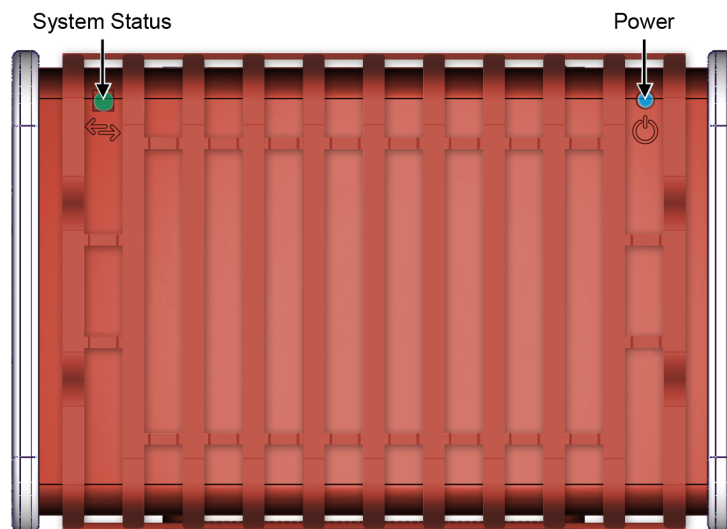


Table 1: System Status LED

Color and Status	Description
Amber (slow blinking)	Booting OS (both modes)
Amber (steady)	Manual Configuration menu running (both modes)
Green (slow blinking)	Application starting (both modes)
Green (fast blinking)	IP address is acquired by DHCP (both modes)
Green (steady)	Application initialization completed. Connectivity is established and operating (both modes)

Table continues...

Color and Status	Description
SDN Controller mode status (in Mode 0 only)	
Red (fast blinking)	Failure to obtain time of day from NTP server, rebooting in 5 seconds.
Amber (fast blinking)	Failure to obtain SDN Controller IP address by DNS lookup, 3 lookup retries, 2 second interval
Green (fast blinking)	DNS lookup retry succeeded after DNS lookup failure condition
Green (steady, then fast blinking)	TCP connections to SDN Controller is lost
Diagnostics tests (in Mode 0 only)	
Blue (slow blinking)	Diagnostics tests starting, or no Ethernet loopback detected
Red (fast blinking)	Diagnostics Ethernet loopback test failed
Red (slow blinking)	Diagnostics unknown error condition
Magenta (fast blinking)	Diagnostics Ethernet loopback test succeeded after a previous failure condition

Power LED

The Power LED is visible from either side of the unit.

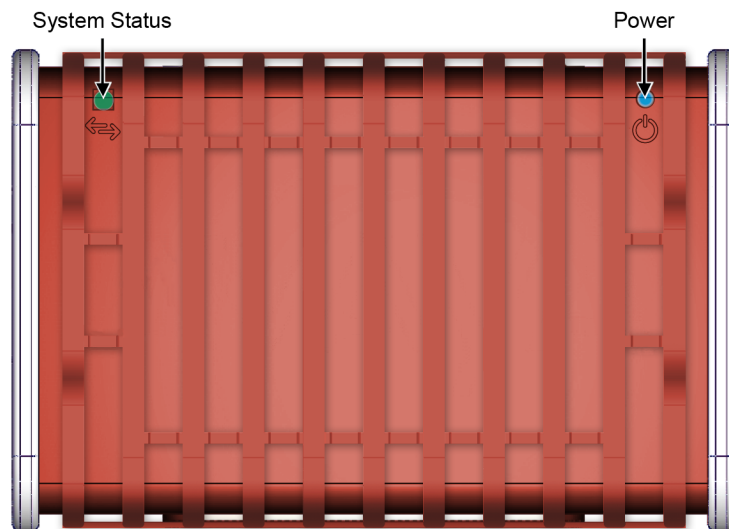


Table 2: Power LEDs

Label	Color and Status	Description
Power	Blue (steady)	Operating normally

Table continues...

Label	Color and Status	Description
	Blue (blinking)	ONA is starting
	Off	Not operational

10/100/1000 RJ-45 Port LEDs

The RJ-45 ports on both the Network side and Device side of the ONA have two bi-colored (amber/green) LEDs. The one on the left side indicates the port speed and the one on the right side shows the level of link activity.

Label	Color and Status	Description
Speed	Amber (steady)	100 Mbps
	Amber (blinking)	N/A
	Green (steady)	1000 Mbps
	Green (blinking)	N/A
	Off	10 Mbps
Link/Activity	Amber (steady)	N/A
	Amber (blinking)	N/A
	Green (steady)	Blink rate indicates level of link activity
	Green (blinking)	Blink rate indicates level of link activity
	Green (blinking slow)	Port disabled
	Off	No Link

Restarting the ONA

Restart the ONA by disconnecting and then reconnecting power as described below:

- If the ONA is connected to a PoE capable network switch, disconnect the Ethernet cable connected to the RJ-45 port with the cloud symbol. Wait at least 45 seconds and then reconnect it.
- If the ONA is connected to an external power adapter, disconnect it for at least 45 seconds and then reconnect it.

Running diagnostics on the ONA

Use the diagnostics to verify that the ONA is operating properly.

To enter Diagnostics, use following procedure:

Before you begin

Ensure the ONA is in Mode 0. Diagnostics only run in Mode 0.

Procedure

1. Disconnect the ONA from the network switch and any device it may be attached to.
2. Use an Ethernet cable to connect the ONA Device port to its Network port, as a loopback is required to run diagnostics.
3. Connect the ONA to an external power adapter.
4. Watch the Status LED.
 - a. Slow blinking Amber indicates the ONA is booting.
 - b. Slow blinking Blue indicates that the diagnostics started.
5. Determine if the ONA passes or fails.
 - a. The ONA passes if it continues flashing slow blinking Blue.
 - b. The ONA fails if the Status LED is either fast blinking Red (for a continuous error in the test) or slow blinking Magenta (tests are now passing but previous tests failed).

If the ONA fails, return it to Extreme Networks.

The diagnostic tests do not exit automatically. You have to power cycle the ONA by disconnecting the Ethernet loopback cable and the external power adapter. Then reconnect the cables you disconnected in step 1 and the external power adapter to reset the ONA.

If you do not disconnect the Ethernet loopback cable before resetting the ONA, the diagnostics will restart.

If you disconnect the Ethernet loopback cable while diagnostics are running, it creates a failure state and the Status LED flashes red, but the diagnostics continue running.

Upgrading a standalone ONA using the Manual Configuration menu

Use this procedure to upgrade the ONA when you first receive it. This method uses a PC to access the ONA's Manual Configuration menu.

Procedure

1. From the PC that you are going to use for this upgrade procedure, go to the Extreme Networks support website, <https://extremeportal.force.com/>, and download the ONA software image that you want to use.
2. Connect a PC to the RJ-45 port on the Device side of the ONA.

*** Note:**

Make sure the PC's network port is enabled with DHCP client.

3. Insert a paper clip into the reset switch. Press and hold the reset button before applying power to the ONA.
4. Connect the cable from the network switch to the Network side of the ONA for PoE power. If PoE power is unavailable, connect an external power adapter.
5. Continue pressing and holding the reset button until the Status LED cycles through a steady red/green/blue. Then release the reset button and the Status LED flashes a steady amber, which indicates that the Manual Configuration menu is running.

*** Note:**

After this step, wait for a few seconds so that the PC gets an IP address for the ONA over DHCP.

6. On the PC, use a browser to connect to the ONA configuration menu with the address `http://192.168.100.1`.

*** Note:**

You cannot go directly to this web page. You must complete steps 1–5 first.

7. Click **Upgrade Software**.
8. Select the software upgrade package that you want to upload.
9. Click **Send** to upload the image to the ONA. This may take up to five minutes.

*** Note:**

Do not refresh or close the webpage during the upgrade.

10. Click **Return to Configuration page**.
11. Click **Reboot into Operational Mode**.
12. Disconnect the PC.

Upgrading a deployed ONA

See the *Open Networking Adapter 1101GT Release Notes* for the latest information on upgrading ONA software on a deployed service.