



ANGLER

User manual

2019-03-03

V2.1

<u>CONNECTING THE APPLIANCE TO THE NETWORK</u>	1
WHAT'S IN THE BOX	1
BEFORE YOU BEGIN	1
WIRING, POWER-UP	2
<u>INITIAL SETUP</u>	3
WEB CONSOLE ACCESS	3
EVENTS/ALERTS	4
SYSTEM SETTINGS	5
SYSTEM INFORMATION	6
CONFIGURE NOTIFICATION CHANNELS	7
NETWORK SETUP	8
WHITELISTING SELECT DEVICES	8
ACTIVE RESPONSE	9
<u>SENSORS</u>	9
SSH	10
FTP	10
WEB	11
FILE SHARE	11
PORT SCAN	13
LOW INTERACTION SERVICES	13
HOST INTRUSION DETECTION	16
REMOTE - API	17
<u>FIRMWARE AND UPGRADE</u>	20
RESET THE SETTINGS	20
UPGRADING THE FIRMWARE	20
<u>TECHNICAL SUPPORT</u>	22



The appliance represents a deception device - real OS on real hardware that is setup as a decoy to lure in cyber-attackers. Its configured profiles are designed to mimic the types of targets the attackers are interested in. Since almost any access to this system should, by definition, be suspicious, it detects breaches reliably with precision and speed while keeping the number of false positive IOC alerts near zero.

The device detects and captures new attacks and methods that are employed during attacker's lateral move. It advertises and exposes a configurable set of services that the attacker will inevitably explore. Additionally, the device monitors itself for compromise and port scan indication. When any IOC event is detected, it will be reported via email and/or syslog to the administrator. When enabled, the device can initiate an active response to the attacker's machine.

Connecting the appliance to the network

What's in the box

The product package contains the following items:

- The appliance
- (1) AC power cable, North American type
- (1) Ethernet patch cable
- Quick setup card

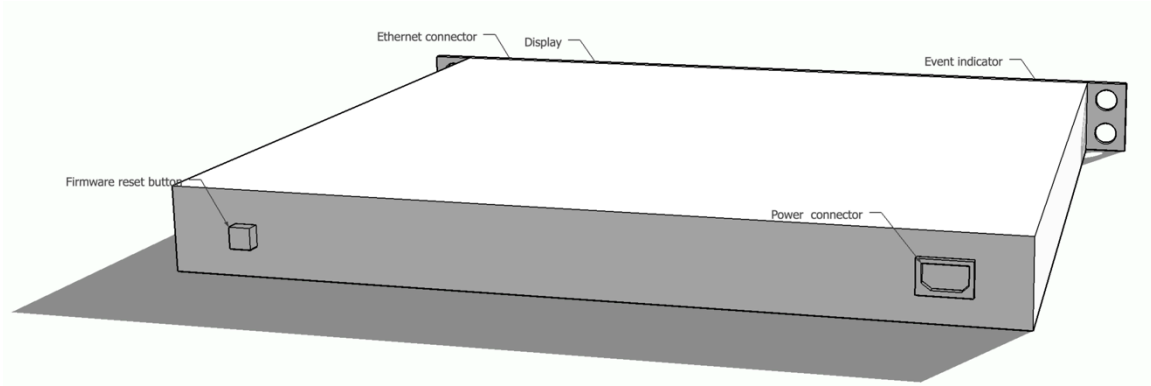
If any of the parts are damaged or missing, please contact us. If a re return of the product is desired, original packaging and the box are required.

Before you begin

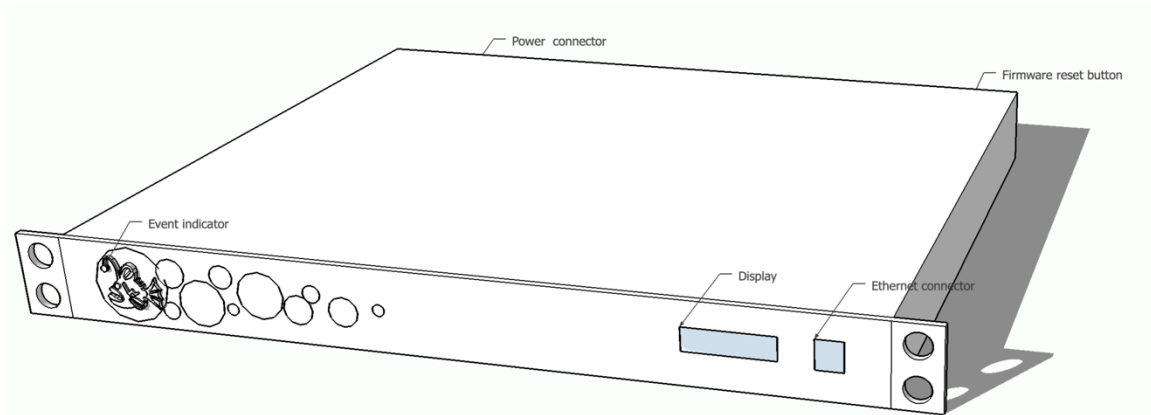
You will require a 85-264VAC power outlet and a network connection, DHCP enabled.

Wiring, power-up

Insert the power cable into the power connector on the backside and connect it to the power outlet.



The Ethernet cable is connected to the front, Ethernet connector, next to the display.



Within 60 seconds of being connected to a power source, the display will show the host name, Ethernet IP address that is assigned to the appliance via DHCP and the number of active events.

Initial setup

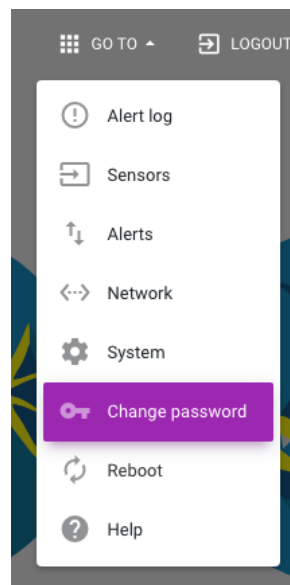
Web console access

Using a web browser connect via http or https to the IP address assigned to the appliance (visible in the display area)

Ex: https://<assigned IP>/

The appliance uses a self signed certificate - please acknowledge the browser's warnings and/or add the site to the exception list. The certificate will re-generate at every restart of the appliance. When prompted for credentials, use '**admin**' as the username and '**secret**' as the password.

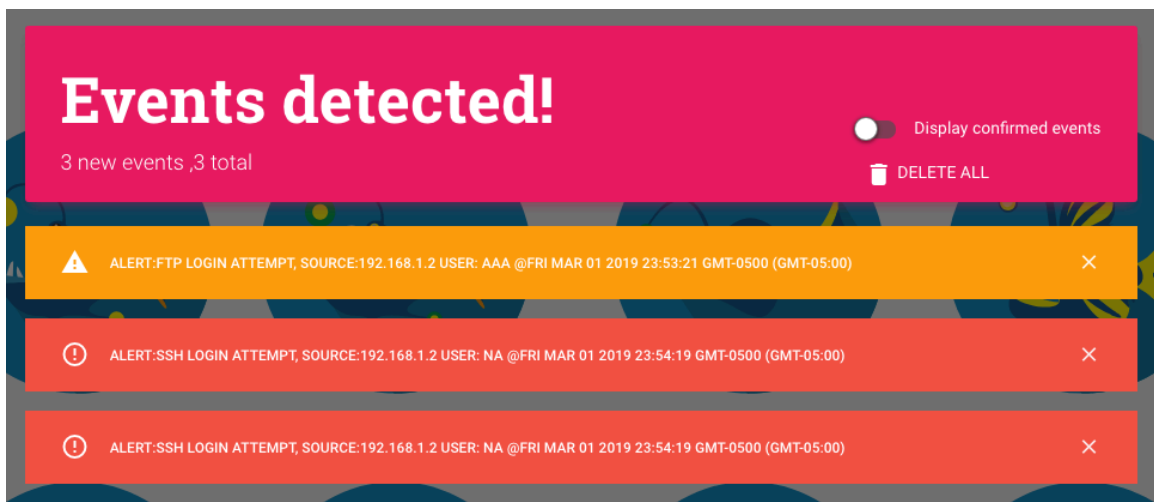
After the initial login, it is recommended to change the default password by navigating to the menu 'Go To>Change Password' option. After the password is changed, you will need to log off and log on again.



Events/Alerts

When an event is detected and an alert generated, the appliance will publish the event on all enabled notification channels (SMS, Email, syslog), turn on the LED indicator on the front panel of the appliance, update the alert count in the display area and display a round white dot on the top left of the display when the IP and host information is displayed.

Information that is sent via the notification channels is displayed in the top section of the management console.



The screenshot shows a notification panel titled "Events detected!" with a pink background. It displays "3 new events ,3 total" and a toggle switch for "Display confirmed events" which is currently turned off. A "DELETE ALL" button with a trash icon is visible. Below the header, there are three alert messages, each with a close (X) icon on the right:

- ALERT:FTP LOGIN ATTEMPT, SOURCE:192.168.1.2 USER: AAA @FRI MAR 01 2019 23:53:21 GMT-0500 (GMT-05:00)
- ALERT:SSH LOGIN ATTEMPT, SOURCE:192.168.1.2 USER: NA @FRI MAR 01 2019 23:54:19 GMT-0500 (GMT-05:00)
- ALERT:SSH LOGIN ATTEMPT, SOURCE:192.168.1.2 USER: NA @FRI MAR 01 2019 23:54:19 GMT-0500 (GMT-05:00)

After your review is complete, clicking the 'Delete all' icon can clear the list of the events. If you want to dismiss/hide the alert while keeping a record of it, click on the X icon on the right side of the alert message. To display all records, including the ones that were dismissed previously, toggle 'Display confirmed events'. All dismissed alerts will be displayed using a light blue color background.

Events detected!

2 new events ,3 total

Display confirmed events

 DELETE ALL



ALERT:FTP LOGIN ATTEMPT, SOURCE:192.168.1.2 USER: AAA @FRI MAR 01 2019 23:53:21 GMT-0500 (GMT-05:00)



CONFIRMED ALERT:SSH LOGIN ATTEMPT, SOURCE:192.168.1.2 USER: NA @FRI MAR 01 2019 23:54:19 GMT-0500 (GMT-05:00)



ALERT:SSH LOGIN ATTEMPT, SOURCE:192.168.1.2 USER: NA @FRI MAR 01 2019 23:54:19 GMT-0500 (GMT-05:00)



System settings

This section allows you to specify the appliance's host name, the time zone, up to 4 NTP servers and the host and port of the update service that will provide firmware updates.

Note: The update server settings should be changed only when the appliance is behind a firewall and the actual update server address is NAT-ted or the port translated.

Edit system settings ? x

Host Name
AnglerDev

Hostname of this appliance

Timezone
UTC

Automatic updates

Update server
10.0.0.223

server used for updates and notifications

Port
8443

Port of the update/management server

NTP Enabled

NTP
time.google.com

NTP
time2.google.com

NTP
time3.google.com

NTP
time4.google.com

Enable experimental features

CLOSE SAVE CHANGES



System information

By accessing this panel, the following information about the system will be displayed in real time:

- Uptime and load average
- CPU temperature in Celsius
- Software revision/build number
- Total and available memory (kB)
- List of IP, MAC and name of the active interfaces.

System information ? x

Host Name
AnglerDev

Uptime
01:03:15 up 6 days, 21:02, load average: 2.00, 2.01, 2.00

CPU temperature
49.926

Revision
1550539375

Memory
MemTotal: 945516 kB, MemFree: 866608 kB

Connectivity

Name	MAC	IP
lan	7e:ba:ba:3e:06:e2	192.168.1.1
wlan	fe:27:7b:1d:3c:f4	10.0.0.61/DHCP

Showing 1 to 2 of 2 entries



CLOSE


In addition to the information displayed on the photo above, the built in display will show periodically the host name, Ethernet IP address and the number of events/alerts that are active in the system.



Configure notification channels

Every time an event is detected, the appliance will send an alert via all enabled notification channels:

-  Syslog. Please specify the address of the syslog server, the protocol and the port that is listening on. The configured facility and level will be applied to all alerts that are sent.
-  Email - SMTP (Simple Mail Transfer Protocol)

-  SMS via remote management center. If the appliance is registered to use the remote management center, in addition to remote configuration and availability monitoring, all alerts will be sent via SMS to a number of cell phones configured in the remote management center app.

Network setup

Default networking settings are configured via DHCP. If you require a static IP address to be configured, scroll down or use the menu option to navigate to the 'Network' option of the console. Change the protocol to 'Static' and fill the address, netmask , gateway and DNS servers.

Click 'Save Changes' button to activate the settings.

The appliance has the capability to activate additional interfaces that will cause the appliance to present multiple IP/MAC addresses on the network. Choose 'Virtual interfaces' option to specify how many additional interfaces are required in addition to the default hardware interfaces. Once 'Update' button is clicked, the appliance will reconfigure itself with the specified number of interfaces, configured by default to be configured via DHCP. These new interfaces are named vrlan1..vrlanX and can be individually configured to use static IP addresses or continue using DHCP.

To remove the virtual interfaces, set the count to zero.

Note: the MAC address of the hardware and virtual interfaces will change every time the number of interfaces is updated.

Whitelisting select devices

The appliance will discard all events generated by devices in the whitelist. Usually this list includes machines or appliances that scan or probe the internal network.



Active response

The appliance, if authorized, can initiate an ARP MITM attack on the IP address that is associated with any of the alerts attempting to block it from accessing the net. Because of the potential effects, please enable this feature after the appliance is fully configured and monitored for a period of time. When this feature is enabled and active due to an event being detected, the top navigation bar will display a blinking red icon.

Angler

  GO TO ▾  LOGOUT

To remove an IP from the active list, click on the blinking icon, find the IP of interest in the list and click on the X button to remove it from the list.

Blocked IPs

×



CLOSE

Sensors

In order to create a believable decoy, the appliance exposes a number of real and simulated services that mimic services and software packages relevant to your business domain. To minimize the configuration time, the 'Quick' configuration mode offers pre-packaged sensor configurations that can be


activated by selecting the closest vertical to your business domain, and confirming the selection using the 'Apply' button.


The current configuration will be discarded and replaced by the selected vertical package.

Vertical

Real Estate

Select an industry vertical

 The profession of buying, selling, or renting land, buildings, or housing

 ssh, ftp, port scan detector, share:AssetMgmt/Assets, MsSQL, HTTP Alternate (see port 80), FileNET RMI/BadRequest,

[APPLY](#)

If you need to further customize the appliance's sensors select 'Advanced' mode.



If enabled, any authentication attempts are reported via all configuration channels immediately.

x

SSH login attempt monitoring (any ssh login attempt will be reported)

[CLOSE](#) [SAVE CHANGES](#)



If enabled, any authentication attempts are reported via all configuration channels immediately. The configuration screen allows the customization of the FTP banner message.

FTP login attempt monitoring (any ftp login attempt will be reported)



Banner

Unauthorized access prohibited.

Text to be displayed at logon

CLOSE

SAVE CHANGES



WEB

If enabled, any access to port 80 or 443 that is not authenticated within 30 seconds will be reported.

Web access monitoring

Enabled

Any access to port 80 or 443 that is not authenticated within 30 seconds will be reported

CLOSE

SAVE CHANGES



File share

If enabled, the appliance will expose a network shared drive where a number of dummy files will be present. Any connections and access of the files will be reported immediately.



Enable sharing services



Name

AnglerDev

CIFS name

Share Name

HRConfidential

CIFS share name

Alert on share open/close



Shared files

Type	Name
txt	passwords.txt
xls	salaries.xls
txt	bonuses.txt

Showing 1 to 3 of 3 entries



CLOSE

SAVE CHANGES

If enabled, the appliance will monitor port-scanning attempts. The configuration screen allows the customization of the port scanning detection algorithm.

Edit port scan settings ✕

Port scan detection enabled

Weight

21

Total score needed to be reached to be thought a port scan attempt. The score is calculated as (Low Port Weight*HitCount) + (High Port Weight* Hit count).

Low Port = ports under 1024, Weight = 3

High Port = ports over 1024, Weight = 1

Delay

500

Time window for the scores to be calculated (hundredths of second).

Alert rate

30/minute

Maximum rate of alerts per unit of time

Burst

2

Maximum initial number of alerts before the alert rate is enforced.

[RESET TO DEFAULTS](#) [CLOSE](#) [SAVE CHANGES](#)

 **Low interaction services**

This sensor allows multiple custom services to be created based on a selection from a predefined list of known ports exposed by various applications from multiple verticals or a custom low interaction workflow.

To create a new service definition, select the + icon on the sensor's main configuration panel. A new record will be created and added to the list above. Follow the edit instructions to complete the configuration.

To edit an existing definition, select a record from the list above and click on the pencil icon.

After all the edits are complete, you must click on 'Save changes' button to persist and apply the changes.

Service enabled

TCP/UDP low interaction services

En	Type	Description
Y	8081/tcp	HTTP Alternate (see port 80):2 rules
Y	32771/udp	FileNET RMI/ParRequest:1 rule
Y	3306/tcp	MySQL:Close
Y	1527/tcp	oracle:Close
Y	9000/tcp	Echo:Echo
Y	2068/tcp	Avocent AuthSrv Protocol/LC32 IN DENIED:2 rules

Showing 1 to 6 of 6 entries

Edit New Delete

CLOSE SAVE CHANGES

Editing a service record

The following screen is displayed when a record is being edited:

Enabled

Port 10001 Protocol tcp

Port to listen on

Description

Interaction type

Pre-defined

Logic

Echo

CLOSE UPDATE

The user can specify the port and protocol by clicking on the magnifying glass icon. From here you can choose from a list of services as defined by IANA.

Services ×

Show entries Search:

Description	Port
ACA Services	62
ACAP	674
ACC RAID	2800
Accedian Performance Measurement	8793
ACCEL	4108

Showing 61 to 70 of 6,090 entries

Previous 1 ... 6 **7** 8 ... 609 Next

To select a service, either navigate until you find the service of interest, or search using the top right entry field (all data elements on the screen are searchable).

Click 'Select' to confirm the choice. The selected port and protocol as well as the service name will be auto filled in the service configuration screen.

The next choice is to select the interaction type as:

- Predefined. At the time of writing this manual, two options are available
 - Close: wait for input and close the channel after the CR is received.
 - Echo: send back the input after the CR is received.
- Custom rules. Multiple rule entries can be added and will be evaluated in the sequence in the list, every time there is new input available. To reorder the list, select a rule entry and use the icons.

A rule comprises of a regex expression that is applied on the input data. If there is a match, the rule will be executed and the remainder rules will not be executed.

If a rule is to be executed, the response data must be specified as well as it's encoding type. By using Base64 encoding, a larger character set can be used.

Also, a toggle switch can specify if the connection is to be closed after the response data is sent back.

Match RegEx
.*

When the expression matches the incoming data, the rule will fire and send the configured response

Send data
HTTP/1.1 200 OK<body></body>

Data to send back, encoding must be specified

Send data encoding
txt

Close connection after send

CLOSE UPDATE



Host intrusion detection

This sensor monitors the appliance's file system and processes as well as any outbound traffic. If enabled, any unauthorized change to the filesystem and unexpected process or communication that is initiated from within the appliance will trigger an event to be generated. The configuration screen allows the administrator to specify a whitelist of IPV4 addresses or ranges in CIDR notation. Please note that enabling various notification channels (for example syslog) will cause the underlying transport to be automatically whitelisted.

Enable host intrusion detection - monitor internal filesystem and processes to detect system compromise



Ignore outgoing NTP requests



Ignore outgoing DNS requests



Alert rate

30/minute

Maximum rate of alerts per unit of time

Burst

3

Maximum initial number of alerts before the alert rate is enforced.

List of ip/ranges for which outbound traffic will not generate an alert

IPv4 CIDR

8.8.4.4/32

8.8.8.8/32

Showing 1 to 2 of 2 entries



CLOSE

SAVE CHANGES



Remote - API

Deploying remote sensors on additional servers or desktops within your enterprise will extend the appliance's monitoring area. These remote sensors can be written in a language of your choice, using a very simple but powerful JSON based API. Additionally, yourAngler co. has a number of pre-built java applications that can be executed virtually anywhere you can install a java virtual machine. For example, the Remote File system sensor will monitor a folder and its subfolders for changes. Remote RegEx log monitor can be configured to monitor an application log for RegularExpressions matches.

The API uses a TCP or UDP listener, on a port that defaults to 1234. It is recommended that you reconfigure the API listener to use a different IP port. The sender process must send the data using JSON encoding using a TCP or UDP connection to the above port. For details regarding JSON format please see the following links:

<https://www.json.org/>

<https://tools.ietf.org/html/rfc7159>

To process an inbound event, the received data must contain a key called 'key' with a value identical to the one configured in the appliance's API configuration page. If these values are not matching, the appliance will silently discard the event. All remaining keys and source IP related information will be collected and used to generate a notification message distributed via the configured notification channels.

Examples:

How to make an UDP API call from shell on a linux platform:

```
echo "{\"key':'abc', 'key1':'v1','key2':'v2' }" > /dev/udp/<APPLIANCE_IP>/<PORT>
```

How to make an TCP API call from shell on a linux platform:

```
echo "{\"key':'abc', 'key1':'v1','key2':'v2' }" > /dev/tcp/<APPLIANCE_IP>/<PORT>
```

The appliance's IP address can be found in the 'info' section of the web console or displayed on the built in OLED display (Ethernet IP).

The API function can be enabled or disabled by toggling 'Remote API events' button.

On the configuration screen, clicking 'Reset to defaults' button, port will be reset to 1234, the protocol will be set to UDP and the key will be regenerated.

Edit API sensor settings



Remote API events enabled

Port

1234

Port to listen for external API requests

Protocol

udp

Key

abc

Shared key that needs to be sent within the remote API calls

Sample UDP API call:

- `echo '{"key":"abc","key1":"v1","key2":"v2"}' > /dev/udp/APPLIANCE_IP/PORT`

Sample TCP API call:

- `echo '{"key":"abc","key1":"v1","key2":"v2"}' > /dev/tcp/APPLIANCE_IP/PORT`

RESET TO DEFAULTS

CLOSE

SAVE CHANGES

Firmware and upgrade

Reset the settings

To reset the appliance to the factory defaults of the latest firmware that was successfully loaded follow the following steps in sequence:

- Power-off the appliance – disconnect it from the power outlet.
- Press and hold the button on the right side of the back panel.
- While continuing to hold the power button, connect the power back to the appliance until the display area says 'Restoring firmware'
- Release the button. The appliance will delete all settings and replace them with a factory configuration and initiate a subsequent restart. After restart, the appliance will request a IP address via DHCP. You will have to adjust the web console URL to specify the new IP address (<https://<assigned IP>/>)
- Follow the instruction from 'Initial setup' section in this document



Upgrading the firmware

The appliance can automatically update itself to the latest version of the available firmware while keeping the current settings active, by setting the 'Automatic updates' flag under the system setting page. If the flag is not set, then the administrator can manually force an upgrade and can specify to keep or discard the current configuration.

Note: the system settings page contains the IP/FQDN and port of the update service.

Current firmware date/time

02/22/19 01:16:14

Available firmware date/time

02/22/19 01:16:14

Firmware image name

angler.img.gz

Release notes



Upgrade - keep existing configuration files

CLOSE

UPDATE

Technical support

Thank you for your purchase. If you require assistance setting up the appliance, please do not hesitate to contact us via email support@yourangler.com. For quick answers, please visit <http://faq.yourangler.com>