



# **Shield Pro**

## **Quick Start Guide**

# Quick Start Guide



## In the box:



Power Adapter



Shield



Network Cables

## Let's get started!

Before installing Shield you will first need to determine which operating mode best fits your needs. To help with this process, please pick from one of the following scenarios:

### Router Mode: **(Recommended)**

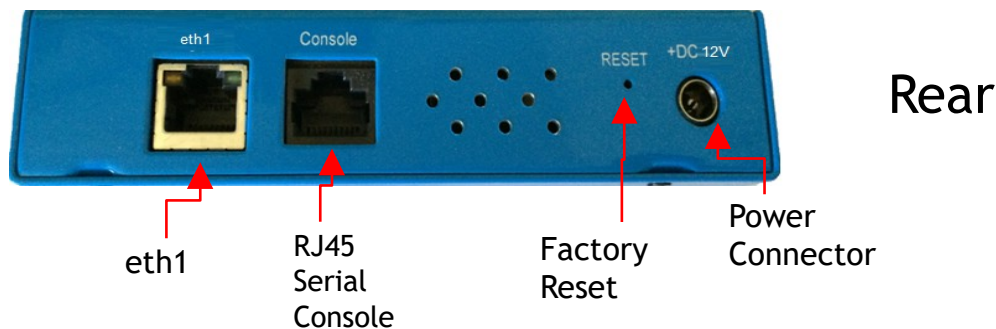
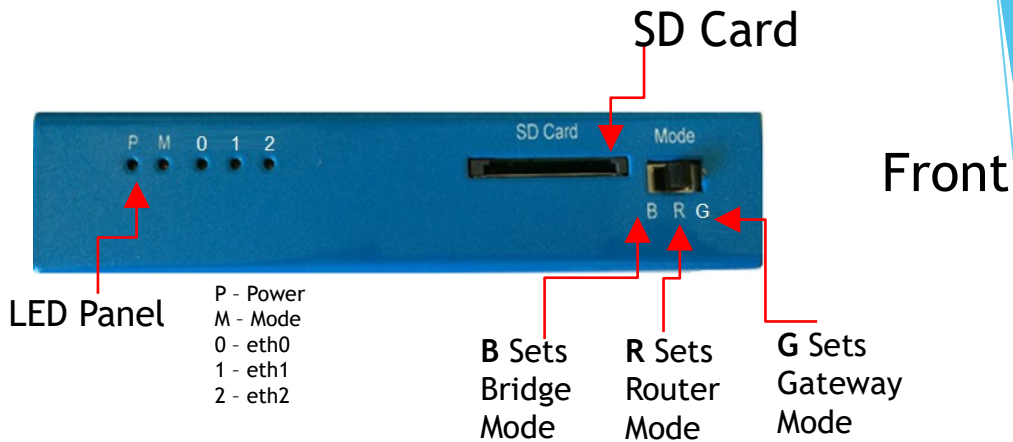
- Best overall performance
- Feature-set
  - Intrusion Prevention
  - Web Filtering
  - Dynamic DNS
  - Virtual Private Network

### Bridge Mode:

- Feature-set
  - Intrusion Prevention
  - Web Filtering (Must set Shield as Domain Name System)
  - Dynamic DNS
  - Virtual Private Network

### Gateway Mode:

- Experimental mode - should not be used in production environments.
- Feature-set
  - Intrusion Prevention
  - Web Filtering (Must set Shield as Domain Name System)
  - Dynamic DNS
  - Virtual Private Network



## Important Notes

- ✓ SD Card is no longer supported
- ✓ Switching modes requires a full system restart
- ✓ Serial console follows Cisco standard - 115200 8n1 (115200 baud, 8 data bits, no parity bit, 1 stop bit.)
- ✓ You must register your Shield in order to receive updates, warranty, and technical support.  
<https://ITUSnetworks.com/register>

# ROUTER MODE

- 1 Connect the **Shield** as shown.



- 2 Set **Shield** mode switch to "R"



- 3 Power off the Modem and access point

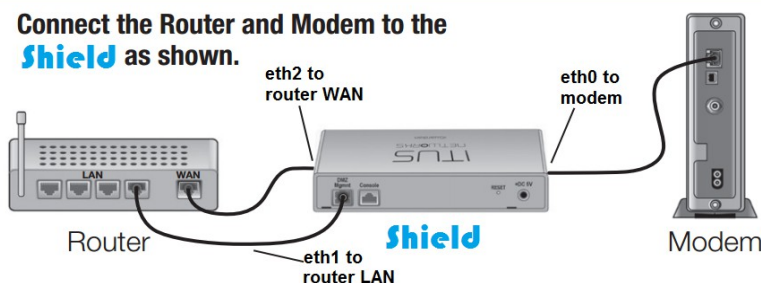
- 4 Power on access point then **Shield**, then Modem

## About Router Mode

- ▶ With two devices, set your existing wireless router to access-point mode.
- ▶ With all-in-one device, set your all-in-one device to modem-only mode.
- ▶ Eth0 is the WAN and is set to DHCP Client. Eth2 is the LAN and is set to DHCP Server.
- ▶ The Web User Interface is accessible on <https://10.10.10.10> or at <https://shield.lan>

# BRIDGE MODE

- 1 Connect the Router and Modem to the **Shield** as shown.



- 2 Set **Shield** switch to "B"



- 3 Power off the Modem and Router

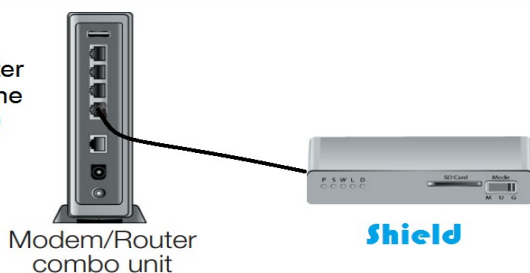
- 4 Power on the Router, then **Shield**, then Modem

## About Bridge Mode

- ▶ Eth0 and Eth2 are set as a transparent bridge and are 'invisible' on the WAN.
- ▶ Eth1 is a DHCP client attached to the LAN; it is used for management & updates.
- ▶ The Web User interface is accessible on <https://x.x.x.111> where x.x.x is your LAN IP.
- ▶ For Web Filter to function you will need to configure your routers Address of DNS Name Server as the LAN IP of the Shield

# GATEWAY MODE

- 1 Connect the Modem/Router combo unit the **Shield** eth0 interface



- 2 Set **Shield** switch to "G"



- 3 Power on the **Shield**

## About Gateway Mode

- ▶ Eth0, Eth1, and Eth2 bridged and configured as DHCP clients attaching to the LAN.
- ▶ The Web User interface is accessible on <https://x.x.x.111> where x.x.x is your LAN IP.
- ▶ For Web Filter to function you will need to configure your routers Address of DNS Name Server as the LAN IP of the Shield
- ▶ Gateway mode is experimental and should not be used in production environments.

# Quick Start Guide



## Setting Up Your Shield

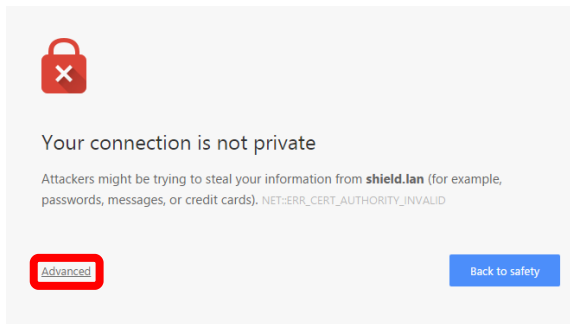
- Go to <https://shield.ian>

Note: Please allow 5 minutes after plugging in your Shield before beginning these steps.

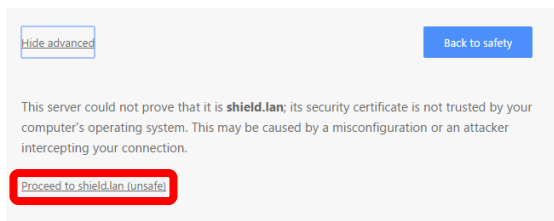
- If a message appears saying your connection is not private, use the following steps:

Note: The below steps are specific to Google Chrome.

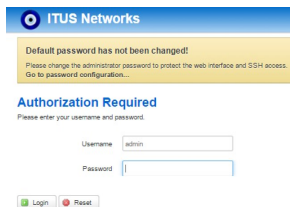
- Click “Advanced.”



- Click “Proceed to shield.ian”



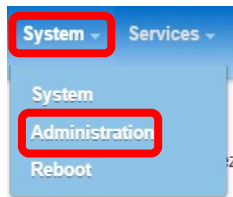
- The login page for the Shield WebUI should now appear with a banner on the top half.



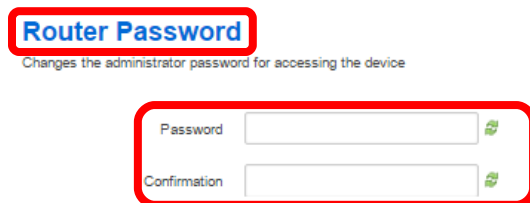
- The banner is stating that the default password needs to be changed.

## Changing Password

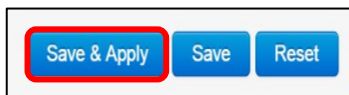
- Log in to the Shield using the default credentials:  
Username: admin  
Password: itus
- Navigate to the “System” menu, and select the tab labeled “Administration.”



- Once on the “Administration” page, go to the section labeled “Router Password.”
- Enter a new password for the Shield.

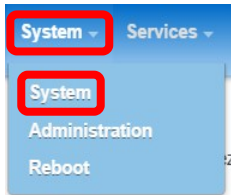
A screenshot of the 'Router Password' section. The title 'Router Password' is highlighted with a red rectangle. Below it is a subtitle: 'Changes the administrator password for accessing the device'. There are two input fields: 'Password' and 'Confirmation', both with green eye icons to the right. The entire form area is enclosed in a red rectangle.

- Scroll to the bottom of the page, and click “Save & Apply.”

A screenshot of three buttons at the bottom of the page: 'Save & Apply', 'Save', and 'Reset'. The 'Save & Apply' button is highlighted with a red rectangle.

## Setting Time Zone

- Navigate to the “System” menu and select the tab labeled “System.”

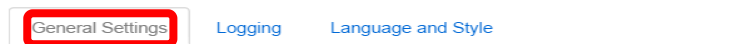


- Once on the “System” page, click on the tab labeled “General Settings.”

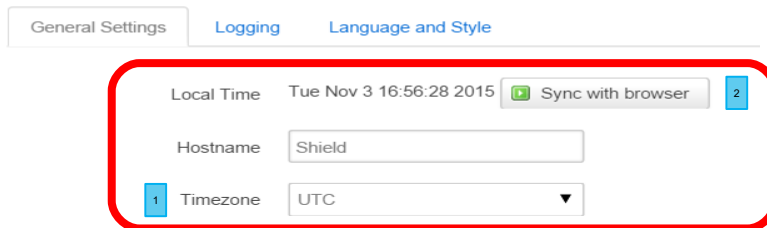
### System

Here you can configure the basic aspects of your device like its hostname or the timezone.

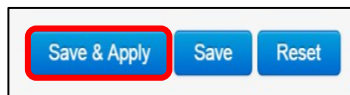
#### System Properties



- Choose the appropriate time zone from the Timezone dropdown menu and then click on “Sync with browser” button.



- Scroll to the bottom of the page, and click “Save & Apply.”

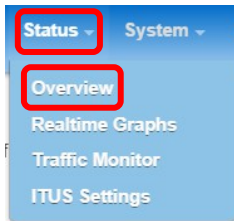


# Quick Start Guide

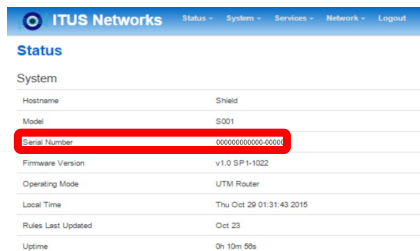
## Register your Shield

You must register your Shield in order to receive updates, warranty, and technical support.

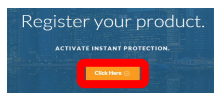
- Navigate to the “Status” menu, and click on the tab labeled “Overview.”



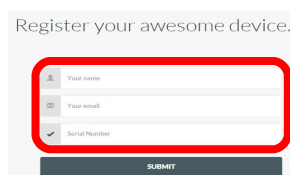
- Under the “System” group there will be a serial number used to register your Shield.



- Go to <https://itusnetworks.com/register>
- Click on the orange tab labeled “Click Here.”



- Enter in the following information:  
Name  
Email  
Shield Serial Number

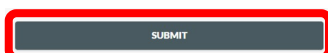


Register your awesome device.

<input type="text"/>	Your name
<input type="text"/>	Your email
<input type="text"/>	Serial Number

SUBMIT

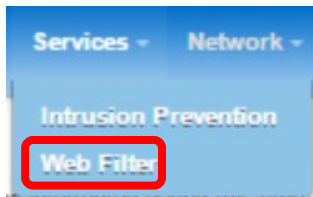
- Click “Submit”





## Viewing Web Filter Logs

- Navigate to the “Services” menu, and click on the tab labeled “Web Filter.”



- Once on the “Web Filter” page, click on the tab labeled “Logs.”

### Web Filter

Changes may take up to 60 seconds to take effect. Web access may be interr

Basic Settings

White List

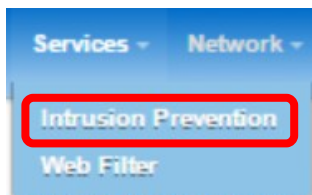
Black List

Logs

Block Page

## Viewing Intrusion Prevention Logs

- Navigate to the “Services” menu, and click on the tab labeled “Intrusion Prevention.”



- Once on the “Intrusion Prevention” page, click on the tab labeled “IPS Logs.”

### Intrusion Prevention

Changes may take up to 90 seconds to take effect, service may be interrupted during that time. The IPS engine will restart each time you click the Save & Apply or On/Off button.

Basic Settings

Exclude Rules

IPS Logs

## Understanding Intrusion Prevention Logs

12/06-07:40:00.312050 [Drop] [\*\*] [1:2019553:2] ET TROJAN Sofacy HTTP Request microsoft.org [\*\*] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.10.10.169:2503 -> 95.211.172.143:80

**Date Code** – This is the day and time at which the incident occurred. This is tied to the system clock; you may need to change your time zone if the logs have incorrect time stamps.

**Action** – This is the action applied to the traffic. By default Shield is set to 'Drop' all malicious traffic. Drop means the traffic is blocked by Shield and the bad traffic never reached its destination.

**SID** – This is the unique identifier for the rule that was matched. When excluding IPS rules, this is the value you'd enter into the 'Exclude Rules' section of the Shield's web user interface.

**Description** – This is a short description of what was matched. This tells you what the IPS saw and why the traffic was blocked. This information is encoded in the rule that was triggered.

**Classification** – This is used to identify the type of incident. This can be thought of as the 'category' of incident that was seen (and blocked) by Shield.

**Priority** – This is used to indicate the severity of the incident. The lower the number, the more severe the threat; ie, priority 1 incidents are considered more 'dangerous' than priority 3 incidents.

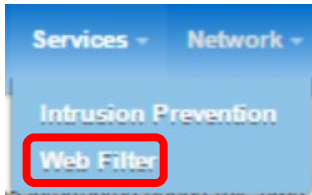
**Protocol** – This is the protocol that was used in the incident that triggered Shield to block the traffic.

**IPs & Ports** – This details the source & destination port and IP address. The first set of numbers are source IP address and port of the traffic, the second set of numbers are the destination IP address and port.

## Content Filtering Setup (Optional)

Default Content Filtering settings block ads, as well as malicious and illegal websites.

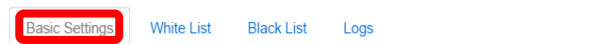
- Navigate to the “Services” menu, and click on the tab labeled “Web Filter.”



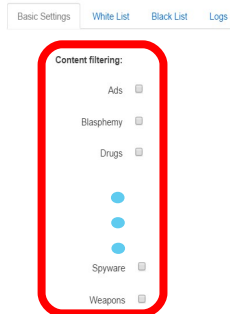
- Once on the “Web Filter” page, click on the tab labeled “Basic Settings.”

### Web Filter

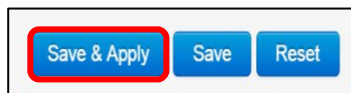
Changes may take up to 60 seconds to take effect. Web access may be interrupted during this time.



- A column of categories with check boxes next to them can be seen. Click on the check boxes for those categories that are to be filtered.



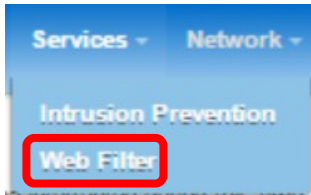
- When finished selecting categories to be filtered, scroll to the bottom of the page and click “Save & Apply.”



## Whitelisting Websites (Optional)

You can allow access to Web sites using the WhiteList.

- Navigate to the “Services” menu, and click on the tab labeled “Web Filter.”



- Once on the “Web Filter” page, click on the tab labeled “WhiteList.”

### Web Filter

Changes may take up to 60 seconds to take effect. Web access may be interrupted during this time.

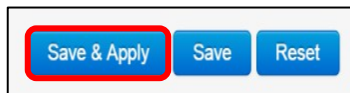
Basic Settings **White List** Black List Logs

- In the text box of “WhiteList,” websites that are **not** to be filtered can be entered.

Basic Settings White List Black List Logs

itus.io  
itusnetworks.com

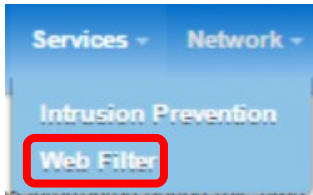
- When finished entering WhiteList websites, scroll to the bottom of the page and click “Save & Apply.”



## Blacklisting Websites (Optional)

You can deny access to websites using the BlackList.

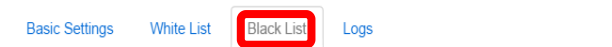
- Navigate to the “Services” menu, and click on the tab labeled “Web Filter.”



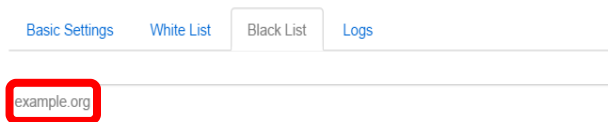
- Once on the “Web Filter” page, click on the tab labeled “BlackList.”

### Web Filter

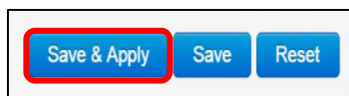
Changes may take up to 60 seconds to take effect. Web access may be interrupted during this time.



- In the text box of “BlackList”, websites that **are to be** filtered can be entered.



- When finished entering Black List websites, scroll to the bottom of the page and click “Save & Apply.”



## Possible Banner Notifications:

### Register Your Shield

#### Your Shield is not registered.

You must register in order to receive security and firmware updates.

--> [Click here to locate your serial number.](#)

--> [Click here to register your Shield.](#)

This means your Shield is not registered. Please go through the registration process at <https://itusnetworks.com/register>.

### Update Available

#### Update available!

Follow these steps to update the device:

- Reboot the device
- Hold the reset button on the back of the device for about 30 seconds as Shield powers on
- Wait a few minutes, device will boot into the selected operating mode when update is finished

[Go to system management ...](#)

Updates are now available for the Shield. Proceed following the instructions listed on the banner.

### Hotfix Applied

#### Hotfix Applied!.

Your Shield has been updated via a hotfix. Please reboot for changes to take effect.

--> [Click here to continue.](#)

A patch has been applied to your Shield. Please reboot for the patch to become active.

### Unexpected Occurrence

#### Oops, something went wrong.

The last update didn't complete as expected. Shield will automatically try again to update itself again tomorrow. This message disappears automatically when the update is successful.

--> [Click here to get help.](#)

The previous update for the Shield was unsuccessful. Another update attempt will be conducted the following day.

## Technical Support

<https://itus.io/support/#Help>

When contacting support, share your name, email address, Shield model, Shield mode, Shield Firmware Version, and a detailed description of the problem you are experiencing. This information allows our team to properly prepare for resolution when returning your contact request.

## Community Forums

<https://packetinspector.org/>

## Documentation

<https://itus.io/support/#Docs>