NF-EN6200
UAM Radius Integration
with ANTMEDIA

<u>Document Contains</u>

UAM-NAS Configuration – NetFox Firewall

End User Login Flow

Release 3.0
Issue 1
Apr 2023

Disclaimer

Precautions have been taken to ensure accuracy of the information provided in this manual. Typographic or pictorial errors that are brought to our attention will be corrected in subsequent issues. NetFox reserves the right to revise this documentation and to make changes in content from time to time without obligation to provide notification of such changes. NetFox provides this documentation without warranty expressed, implied, statutory, or otherwise and specifically disclaims any warranty of merchantability or fitness for a particular purpose. NetFox may make improvements or changes in the in this documentation at any time. Product specifications in this manual are provided for the convenience of our customers. They are all correct at the time of publication. NetFox reserves the right to make product changes from time to time, without prior notification, which may change certain specifications or functions described here.

UAM Hotspot (NAS) Integration Manual

This document talks about the configuration to be done in NetFox Next Generation Firewall Product to co-work with Antamedia AAA Radius Server.

Please note:

1. The integration is available for NetFox NF Series of Next Generation Firewall (NGFW) only
2. Support on NF-10 Series of SDWAN Routers not available
3. NAS add on license is required in NF-Series to do the necessary configuration for the Radius integration
4. NF Series is a NGFW product built with Routing, DPI Firewall, Web Security and VPN Modules along with NAS (UAM) integration add on module
5. NF Series has multiple models based on concurrent device license support. Based on the concurrent user's requirement the choice of the model will vary. Talk to NetFox Presales experts for choices.

NF Series – Basic Configuration

Pre-requisite:

1. Laptop / Desktop with any standard browser (IE/Chorme/Firefox/Safari)
2. Ethernet cable (Preferably CAT-6 or above)

Steps:

1. Unpack the NetFox NF Series box (Based on the choice of model either it will be with a power adapter or built in Power Supply Unit (PSU).
2. Power on the NGFW, you can able to hear single beep on initial power on and after 40 secs a double beep. This indicates the NGFW is booted and ready to do initial configuration
3. For example, if you have product with 4 Ethernet ports named as Port1 – Port4 then connect the Laptop / Desktop to Port-3 using the CAT-6 cable
4. Ensure your Laptop / Desktop Ethernet Adaptor is set as "Obtain IP Automatically"
5. Open a browser and type https://192.168.100.1:4433
6. https server certificate error will occur as it has as self-signed certificate, click on "Advanced" and then click on "Accept the Risk and Continue".
7. Login page will open and request for username & password
8. Type username as "admin" & Password as "admin99"
9. Product Dashboard screen will open with all the required details.
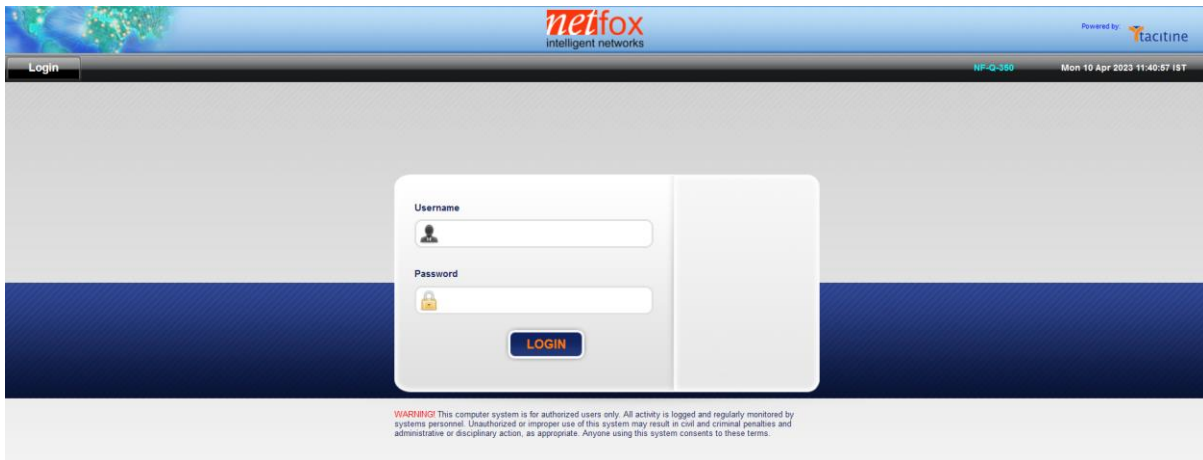
Configuring WAN (Internet Service Provider – Links)

1. Click on "Configuration" tab which is next to "Dashboard". This will open up all the available configuration in the product
2. In "Configurations" click on "Network Settings" choose "WAN-1"
3. Choose the WAN Connection Type as per the ISP link details either as PPPoE, DHCP or Static
4. Do the required configuration as per the ISP link details
5. Incase if you choose DHCP or in Static IP with local IP or NAT-ed IP address then
6. In the "Link Properties" on the "Link Failure Detection" option choose "Ping Remote IP" and configure Remote IP as "8.8.8.8"

---

www.netfoxfirewall.com
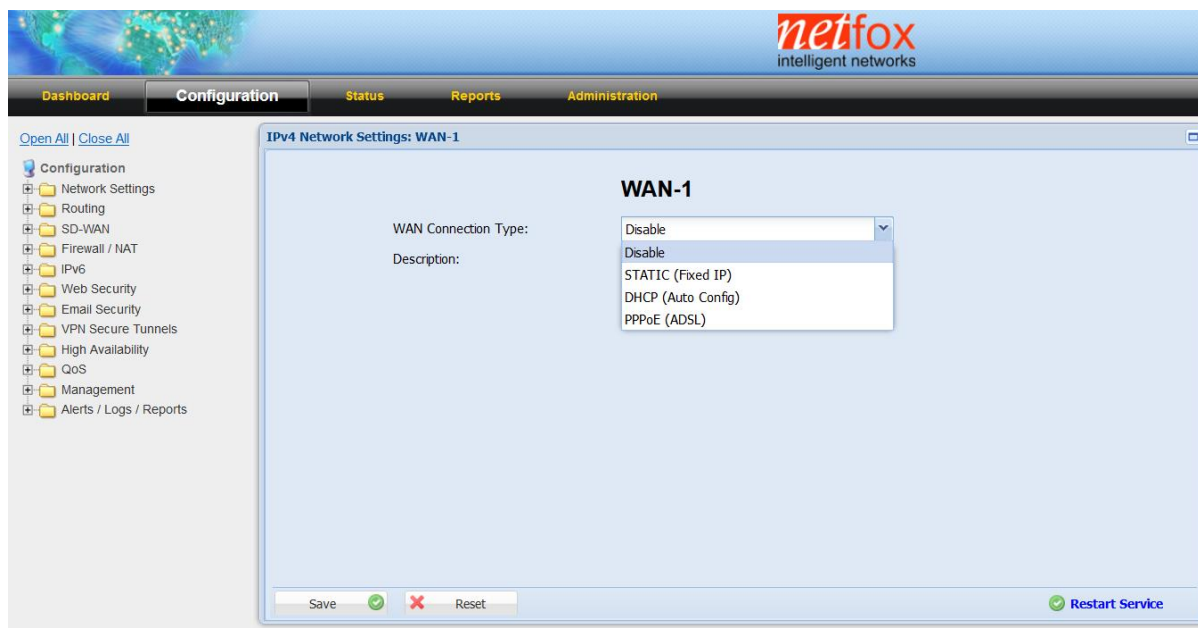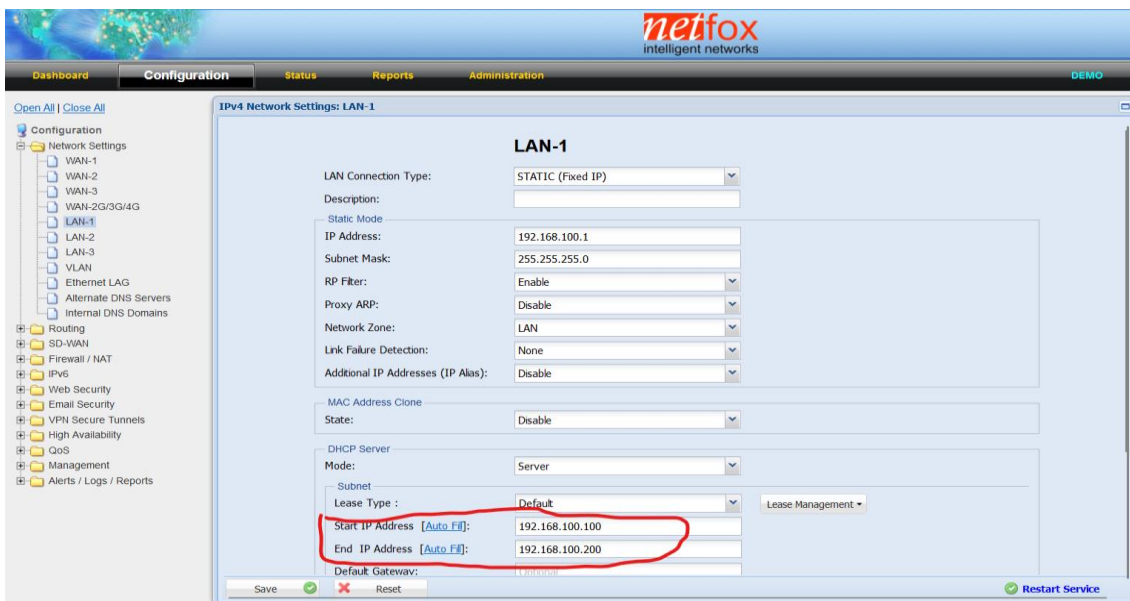
7. With this the configuration for the "WAN-1" is done, click on the "Save" and "Restart Service"

8. Connect the ISP link Ethernet cable to "PORT-1" of the NF NGFW appliance

9. Click on "Dashboard" to check whether the ISP link came up and working in the firewall

10. WAN-1 / WAN-2 status can also view from "Dashboard" – "IPV4 Port Status" from the left side tree

11. Incase if the location has more than 1 Internet connection then follow the above steps to configure the second internet connection in "WAN-2" and connect the ISP link Ethernet cable to PORT-2 in the NF NFGW appliance.

Configuring LAN (Local Area Networks – Links)

1. LAN-1 is part of "Confguration – Network Settings – LAN-1 (The physical port in the NGFW appliance is PORT-3)
   Please note: Incase the appliance you have purchased has 6 Ethernet Port by default then the LAN-1 physical port is named as "PORT-4" in the sticker.

2. The default LAN-1 interface IP is 192.168.100.1 and the DHCP Server is enabled with DHCP pool range from 192.168.100.100 – 192.168.100.200

---

www.netfoxfirewall.com

3. If required the LAN IP can be changed as per choice of the customer and subsequently the DHCP pool size can also be increased to meet the DHCP expected ranges.
4. Additionally, if LAN-2 (a separate LAN Segment is required can also be configured under LAN-2 configuration tab

Configuring UAM -Hotspot NAS Module

Network Access Server (NAS) / Universal Access Method (UAM)

NAS Module has 3 configurable screens

- NAS Server Settings
- Exclusions (Whitelist IP / Domains)
- Bandwidth Settings (on the ISP level)

NAS: Server Settings

Table 1 NAS: Server Settings: Control

Field	Description
Service	Checkbox used to enable or disable the NAS Module. The NAS module is enabled when the checkbox is selected
Description	Relevant name to identify the NAS Module

Table 2 NAS: Server Settings: Radius Server Settings

Field	Description
NAS Identifier	Identifier used to identify the UAM / NAS to post the details back from Radius Server Values: Name or MAC address Example: Name: ANTAMEDIA-BLR | MAC: 00:0A:00:00:00:00
Accounting Server	External Radius Server
Radius Server IP / Name	Support values: IP address | FQDN
NAS Secret	Secret key to handshake with the radius server
NAS IP	IP address of the UAM / NAS Supported Values: Auto Detect | Specify On choice of specify the IP address of the NAS can be configured
Protocol	UDP
Authentication Port	1812 (Standard Port)
Accounting Port	1813 (Standard Port)
Interim Update Interval	Time interval in which the UAM/NAS provide usage information to Radius server Values: max up to 10 minutes | Default: 3 mins
CoA Port	3799 (Standard Port)

Table 3 NAS: Server Settings: User Login Settings

Field	Description
Authentication Method	Radius Login
NAS Web Server Address	Values: Auto Detect & Specify | Default: Auto Detect On choice of specify the IP / Name of the NAS web server can be configured
Captive Portal	Values: Internal Web Server (Port 80) Internal SSL Web Server (Port 443) External Web Server (Port 80) External SSL Web Server (Port 443)

	For ANTAMEDIA: Choose – External SSL Web Server External web server URL to be configured is https://wifihotspot.rs/login/netfox
Internal Web Server Port	2280 (This is the port use by NAS to communicate to the guest users)
Redirect URL after login	Values: Original Request URL Specify Redirect URL Welcome URL In ANTAMEDIA being the captive portal is from the Radius the Redirect UTL after login is controlled by the Radius server
Account Status after login	Values: 1. Show in Popup Window (Pop up windows with login successful message along with time, reset password option (user details) 2. Disable It is advisable to configure as "Disable" as most of the apple IOS wont support show in pop window
User Idle Timeout(min)	Values: From 5 – 14400 mins | Default:30 mins
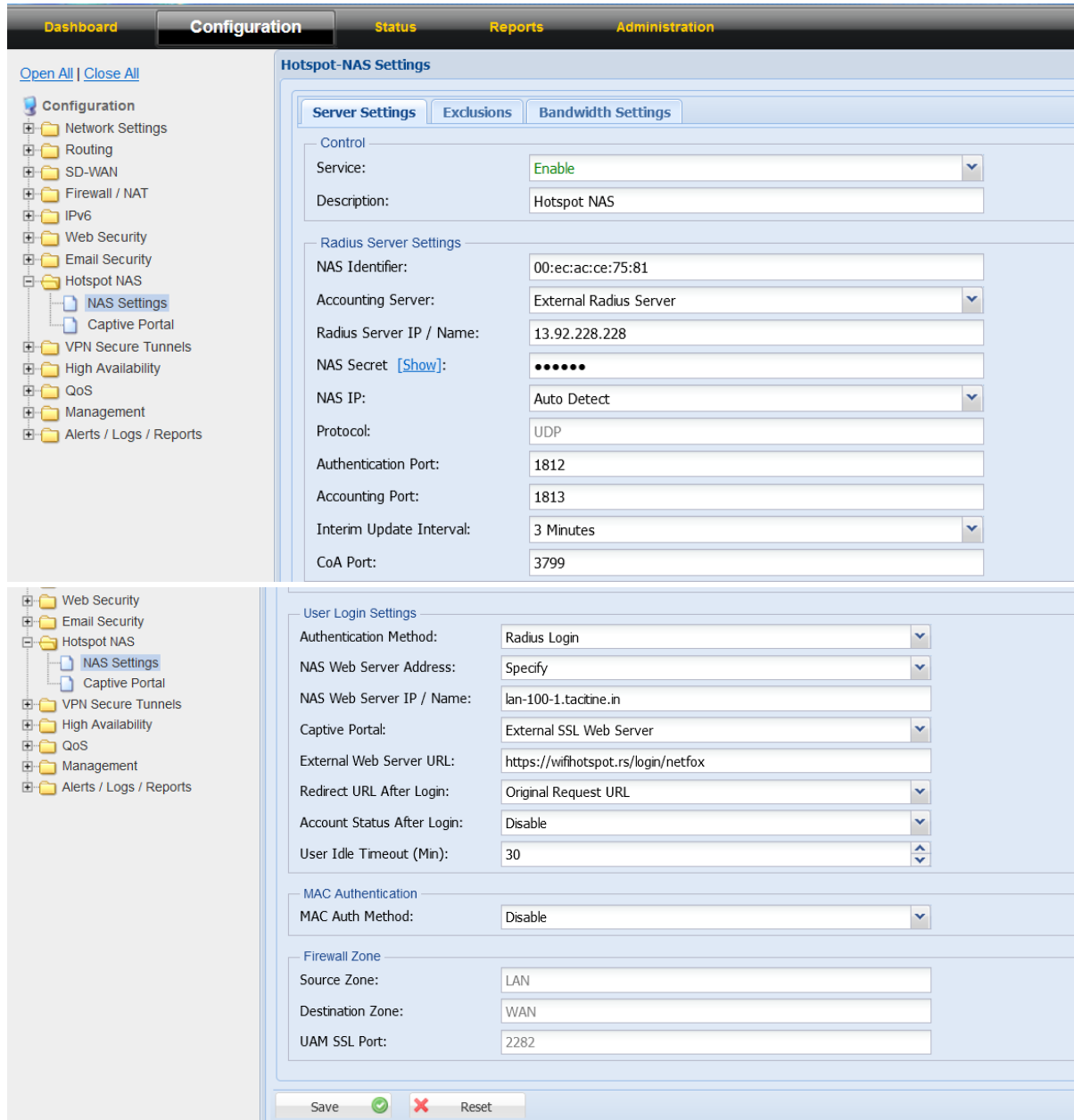
Table 4 NAS: Server Settings: MAC authentication

Field	Description
MAC Authentication Method	Values: Disable MAC as username MAC as username and password Default: Disable

Table 5 NAS: Server Settings: Firewall Zone (not editable)

Field	Description
Source Zone	LAN
Destination Zone	WAN
UAM Port	2281

Tested - Configuration snapshot for NAS Server Settings

NAS Settings: Exclusion (Whitelist)

NetFox NAS exclusion support whitelist of domains, exclusion of IPV4 IP, IPV6 IP and Source MAC.

The IP address, MAC and domains added in the exclusion list do not require authentication from Radius or in other words will work without Radius authentication.
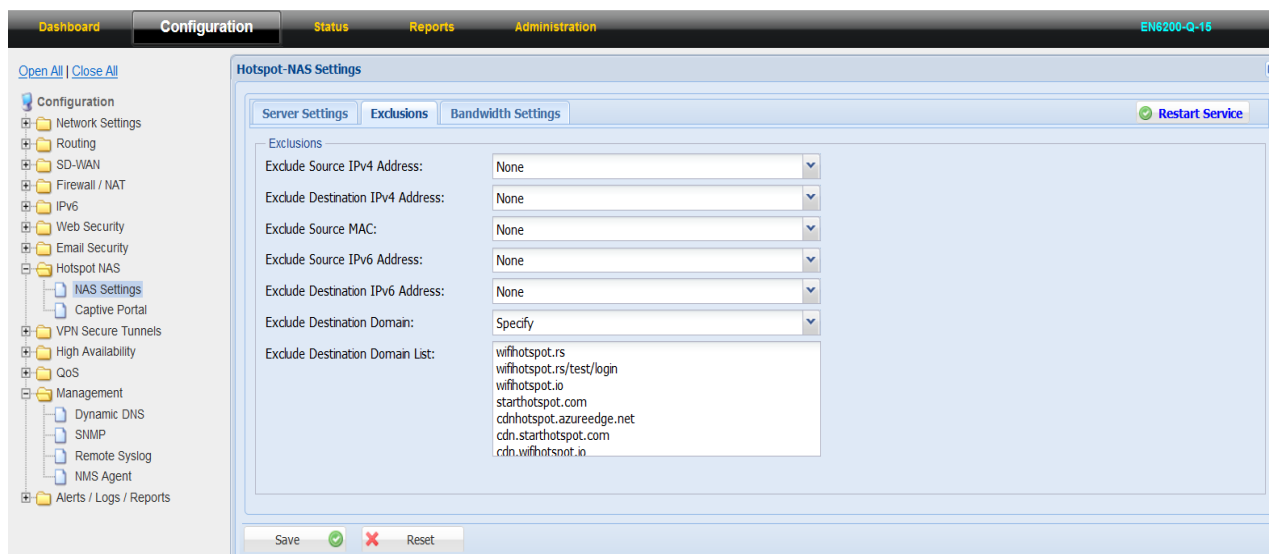
Table 6 NAS Settings: Exclusions

Field	Description
Exclude Source IPV4 address	Values: None | Specify For IP to exclude from Radius Authentication please choose "Specify" and add the IPV4 IP address
Exclude Destination IPV4 address	Values: None | Specify For the destination IPs to get exclude from Radius Authentication please choose "Specify" and add the IPV4 Destination IP address
Exclude Source MAC	Values: None | Specify To exclude source MAC address of a selected devices choose "Specify" and add the MAC address
Exclude Source IPV6 address	Values: None | Specify For IP to exclude from Radius Authentication please choose "Specify" and add the IPV6 IP address
Exclude Destination IPV6 address	Values: None | Specify For the destination IPs to get exclude from Radius Authentication please choose "Specify" and add the IPV6 Destination IP address
Exclude Destination Domain	Values: None | Specify To whitelist domains from Radius server authentication choose "Specify" and input the domain names

For the testing purpose below are the domains are requested to be whitelisted from UAM-NAS module
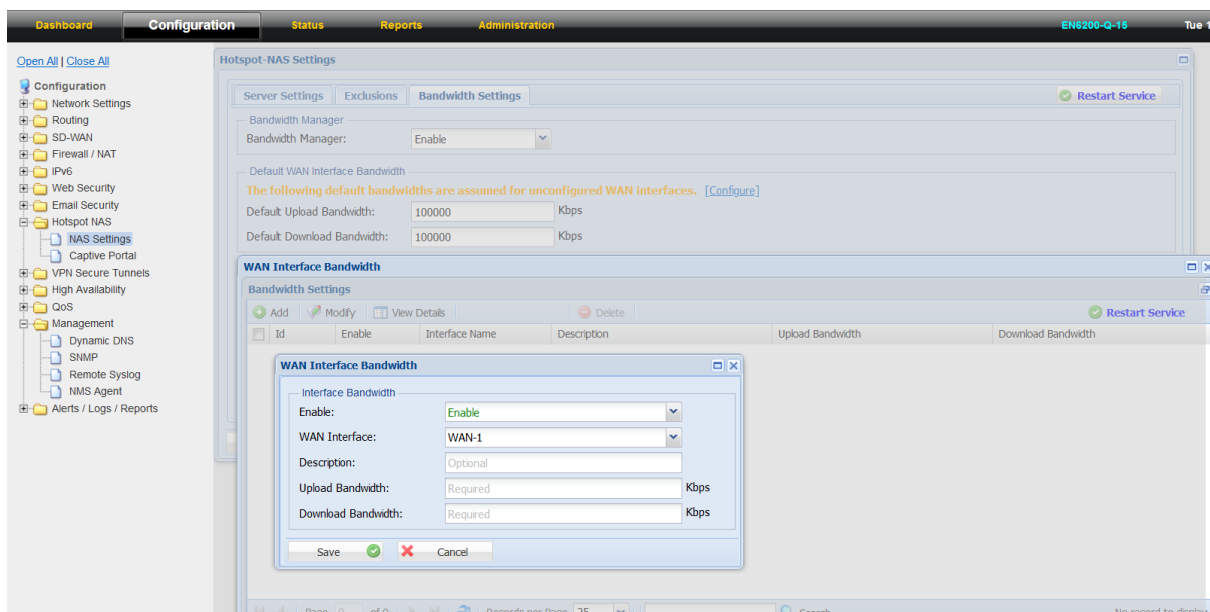
    wifihotspot.rs
    wifihotspot.io
    starthotspot.com
    cdnhotspot.azureedge.net
    cdn.starthotspot.com
    cdn.wifihotspot.io
    t-msedge.net
    static.cloudflareinsights.com

NAS Settings: Bandwidth Settings

NetFox NAS Bandwidth Settings has support to added multiple ISP connection bandwidth speed which help to aggregate the bandwidth and ensure the dynamic algorithm is kicking in right time to manage the bandwidth for the guest users.

If the location has only one ISP link, then input the upload and download bandwidth of the ISP link in Bandwidth Settings tab.

Please note: The bandwidth speed calculation is set in "kbps"

For example: If customer have only one ISP link then do the following

1. Click on NAS Settings – Bandwidth Settings
2. Set Bandwidth Manager as <mark>"Enable"</mark>
3. In the "Default WAN Interface Bandwidth settings "Input the Default Upload and Download bandwidth of the IPS link
4. Click on "save" and then Restart Service

Incase if the customer <mark>has multiple ISP links</mark>, then in the "Default WAN Interface Bandwidth Settings" <mark>add</mark> all the ISP links which is getting configured in NF Series and then input in Upload and Download bandwidth. Then click on "Configure"

1. WAN Interface Bandwidth settings will open
2. Click on "Add"
3. "Enable" the Interface
4. Choose the WAN Interface from the dropdown menu (example: WAN1, WAN2, WAN4G)
5. Input the upload and download bandwidth as per the ISP plan
6. Repeat the above for the other available ISP links configured in the NF Series firewall

Option to upload SSL Certificates

To upload the SSL Certificates

1. Click on "<mark>Administration</mark>" tab
2. Choose System Management option in the left tree
3. Click on <mark>Web Server Settings</mark>
4. Click on "<mark>Upload Customer Certificate</mark>"
5. Upload the relevant certificate, Private key and Certificate Chain

Please note: only "<mark>pem</mark>" format is supported
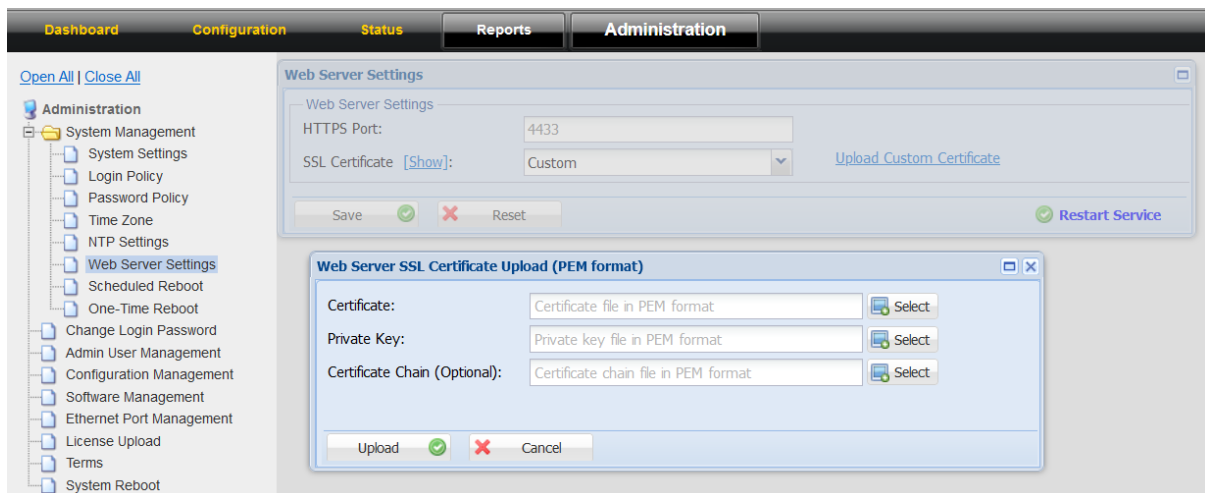
Logged In User Details

NF Series NGFW has detailed logs and reports for the entire suite of feature sets if offers. Related to UAM-NAS the logged in active users, Bandwidth Toppers among the live users and Account Status (atleast once logged in user details) are available in a mouse click.

Click on <mark>"Status"</mark> on the Top bar and then click on "<mark>Hotspot NAS</mark>" on the left tree.

Hotspot NAS – Active Users

All the live users will be part of the active users. For each active users the live bandwidth graph is available and also their usage details. If required the active users can be disconnected using admin privilege

Hotspot NAS – Bandwidth Toppers

Among the live (active) users at any point in time the bandwidth topper table shows the users in descending order with the highest bandwidth users on top of the table. It is listed highest to lowest.

Hotspot NAS – Account Status

This log shows all the users who logged in atlease once in the system. It holds the history of their usage on Today, This week, This month, Lifetime Total, Total sessions etc. Per user level the bandwidth usage graphs can be downloaded and also Daily Usage.

User Detail Reports – Hotspot NAS

This is the history kept for a period of 60 days and archive of 180 in NF Series NGFW. NF Series has built in 64GB or above SSD which has the ability to hold the reports for the above said time period. It has more than 24 reports which includes Hotspot NAS reports as well.

Click on <mark>Report</mark> on the Top bar and then click on <mark>Hotspot NAS</mark> on the left tree.

Reports – Hotspot NAS – User Sessions

User session provides all the uses logged in and logged out details on session level with total time on the network, their upload and download details. Session report can be downloadable in .csv format and we can search for Today, This week, This Month and Customer period based on the requirement.

Reports – Hotspot NAS – Session Summary
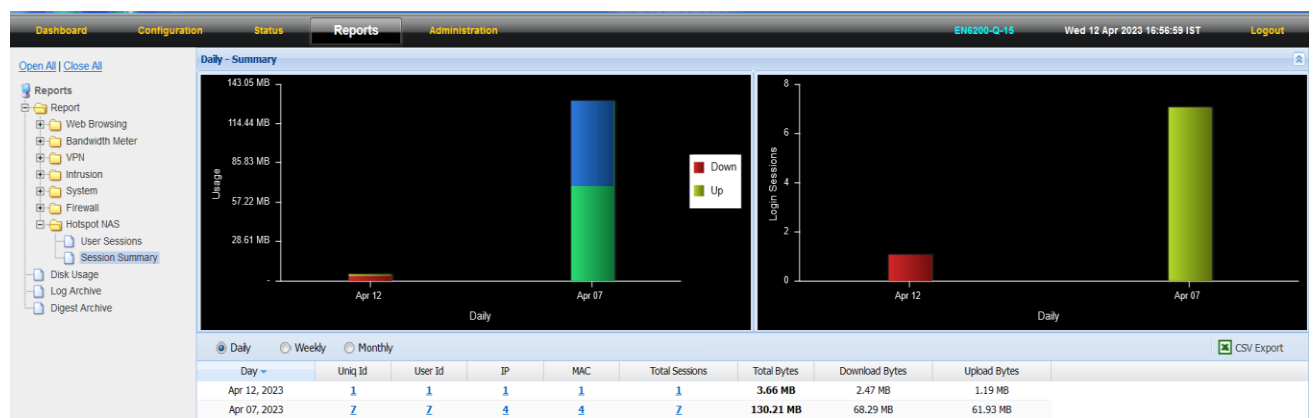
Session Sumary is available on Daily, Weekly & Monthly basis and can be filter based on IP, MAC, Sessions and User ID. The report will be available for 60 days in the NF Series NGFW

---

www.netfoxfirewall.com

Guest User Login Flow

1. The product support both wired and wireless devices in the network for Radius authentication
2. Incase of Wi-Fi devices like laptop, tablets or mobile phones first the device need to connect to the Wi-Fi AP SSID (with or without password)
3. Once connected to Wi-Fi Access Points if it is a mobile or tablet the device automatically open up the captive portal from Radius Server as the NAS device redirect all the request to https://wifihotspot.rs/login/netfox
4. If the users are using laptop or desktop then few browsers with older version automatically opens up the captive portal and the latest upgraded browsers user need to open the browser and type any "http" website like "ndtv.com" "neverssl.com" or any such website to get the captive portal
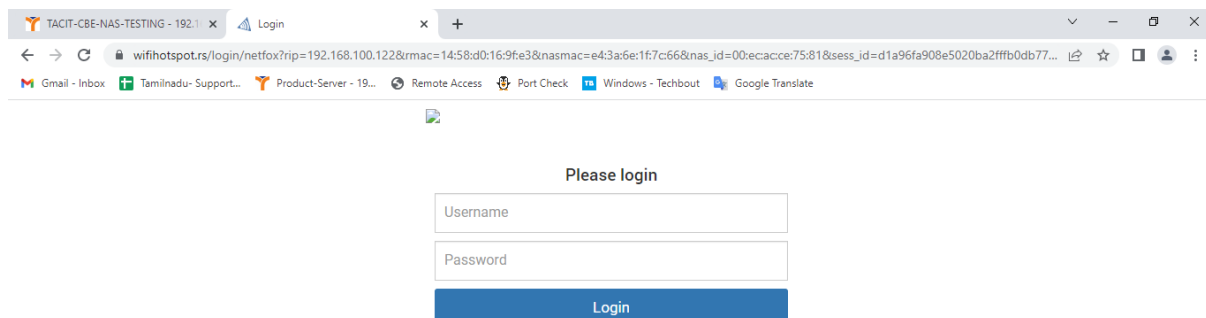
Note:

NetFox NF series NAS module on identifying the user trying to connect to internet will redirect the user to external SSL captive portal https://wifihotspot.rs/login/netfox and along with that redirect in the URL will send all the required information to Radius server to post back the user details.

The redirect URL from NetFox is as follows

https://wifihotspot.rs/login/netfox?rip=192.168.100.10&rmac=8c:8c:aa:65:29:73&nasmac=00:ec:ac:ce:75:7f&nas_id=00:ec:ac:ce:75:81&sess_id=1edf41a9422dd5d8a895a3de16cd222a&submit_url=https://lan-100-1.tacitine.in:2282/submit/user_login.php&logout_url=https://lan-100-1.tacitine.in:2282/submit/logout.php&url=http://ndtv.com/

On the above redirection request the Captive Portal will be loaded to users requesting for username and password
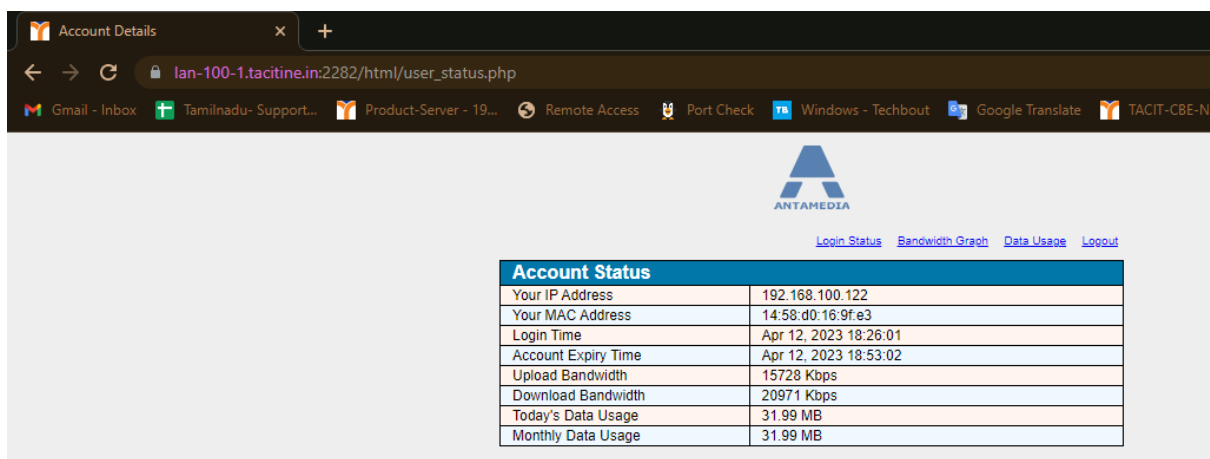

User need to enter the username and password provided by Antamedia team to get authenticated from the Radius Server and once in 3 mins NetFox NAS module will send user data usage information to Radius Server. On successful login the user will be automatically redirected to Antamedia website.
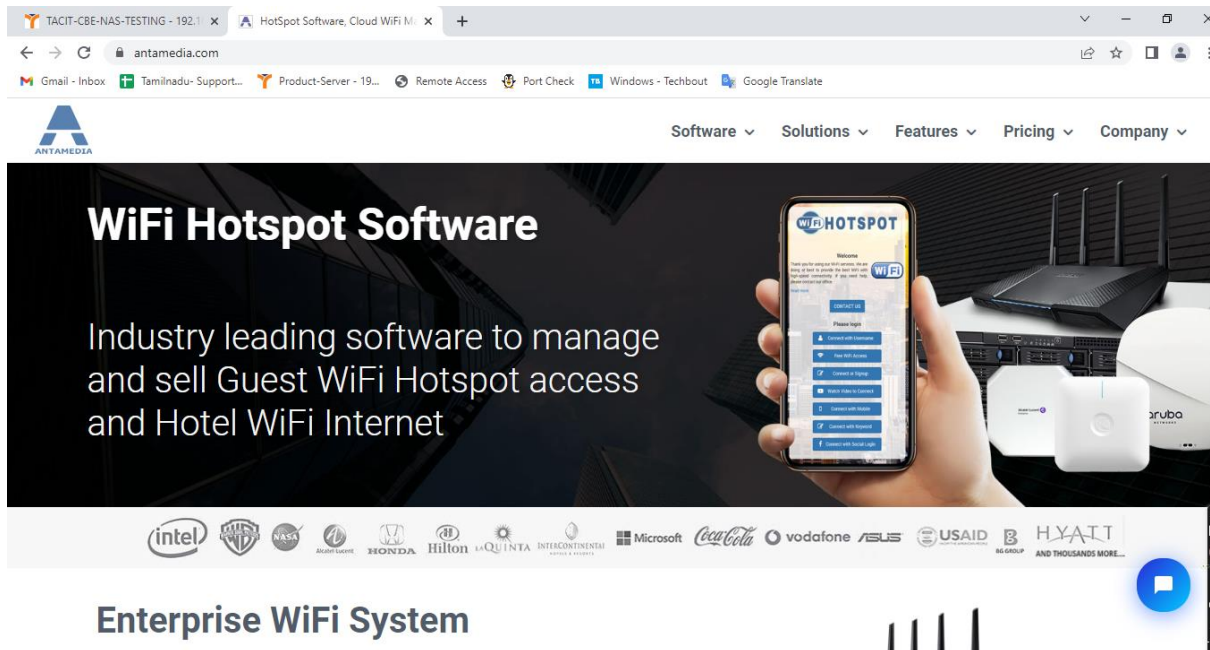
User Profile

Users at anytime want to view their profile like Login Status, Data Usage, Bandwidth Consumed or to change password can easily access their user profile by typing http://1.1.1.1 in the browser. This URL will open up the user profile window with options

1. Login Status (Login duration and option to logout)
2. Data Usage – Which provides daily usage details
3. Bandwidth Graph with option to filter for custom time period
4. Change Password
5. Logout