



Anybus Defender Documentation

User Manual

Version 2.5.2

For PDF Documents

Before you begin

This manual contains bookmarks that are detected by PDF viewer software. Use these bookmarks to navigate the documentation

Adobe Acrobat

The Bookmark button in **Adobe Acrobat** is on the right side and looks like:



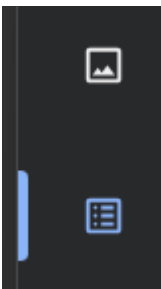
Microsoft Edge Browser

The Bookmark button in built-in **Microsoft Edge** PDF viewer is usually on the Upper Left Side and looks like:



Google Chrome Browser

For the built-in **Google Chrome** PDF viewer, the bookmark button is called the **Document Outline** which is toggled on the upper left:



Release Notes

Improvements

- Add support for Siemens S7 in the Industrial DPI Engine
- Add syslog and NRPE packages, available in package manager
- Add a warning if an IP address is configured on multiple interfaces
- Added a diagnostic support package that can help our team diagnose issues in the field
- Added support for wireless interfaces on new hardware platforms
- Updated names of several well-known ports
- Improved IP and subnet validation across interface configuration pages
- Updated ARP-scan to improve asset discovery
- Enhanced the functionality of the Remote Management configuration page
- Clarified the behavior of the Release/Relinquish lease button on the Status Interfaces page
- Added tracking of version history in the system configuration
- UI updates to the Simple NAT, User Management, and System Update screens
- Added a warning message when checking for online updates without internet connectivity
- Prevented clearing of saved assets when Asset Management is disabled

Bug Fixes

- Aligned package availability and feature access with license permissions
- Fixed an issue where a monitor would not show any output if it was not connected at boot
- Fixed an issue where some graphs on the System Monitoring page would display incorrectly
- Fixed an issue where some support packages for VM instances were removed on factory default
- Fixed an issue where invalid aliases in the config could cause errors in rendering Firewall rules
- Fixed some issues related to editing limiters on the Traffic Shaper page
- Fixed an issue where errors were not displayed as a part of some steps in the OpenVPN Wizard
- Fixed an issue where the settings icon for widgets on the dashboard could render incorrectly
- Fixed an issue where changes could not be saved for remote users
- Fixed an issue where removing the last Industrial DPI rule would cause industrial pages to break
- Fixed an issue where users with only a single interface permission could not login
- Fixed an issue where some config changes were not logged appropriately
- Fixed an issue with the LAN anti-lockout rule that could prevent access to the UI
- Fixed an issue where SimpleNAT could create duplicate WAN rules or fail to delete rules
- Fixed an issue where thermal sensor readings would ignore chosen units
- Fixed an issue where default packages could be removed when restoring a configuration
- Fixed an issue where Defender Networks could appear as an alias on some pages
- Fixed an issue on the Remote Management page where the Save button did not properly apply changes
- Fixed an issue where editing a user could trigger a username input error
- Fixed a crash when deleting a template with no rules
- Fixed an issue where existing WireGuard tunnels or peers could not be edited
- Fixed inconsistencies in Status Monitoring time zones
- Fixed an issue where disabling a graph in Status Monitoring had no effect
- Various other minor bug fixes

Additional Documentation

Documentation is consistently being updated as more features and functionality are added and refined

If this document doesn't include needed information, please contact **HMS Support** at info@hms-networks.com

Document Conventions

Abbreviations

Abbreviation	Full Description
ICS	INDUSTRIAL CONTROL SYSTEM
NIC	Network Interface Card
RA	Remote Access
NAT	Network Address Translation
1:1	One to One (a type of NAT)
LAN	Local Area Network
WAN	Wide Area Network
NTP	Network Time Protocol
DHCP	Dynamic Host Configuration Protocol
CIDR	Classless Inter Domain Routing
CA	Certificate Authority
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
SSL	Secure Socket Layer
TLS	Transport Layer Security
VoIP	Voice over Internet Protocol
CIP	Common Industrial Protocol (EtherNet/IP)
Jump Server	A jump server or secure administrative host is a (special-purpose) computer on a network typically used to manage devices in a separate security zone.

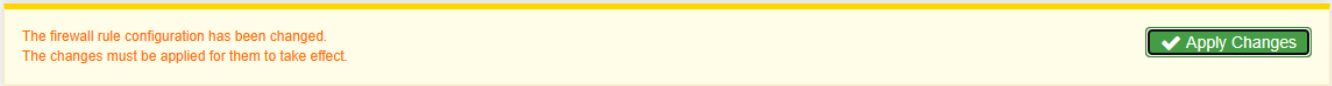
Subnet Mask to CIDR Quick Reference

Subnet Mask	CIDR	Notes
255.255.255.255	/32	SINGLE IP ADDRESS
255.255.255.254	/31	Special use (point-to-point)
255.255.255.252	/30	2 useable IP addresses
255.255.255.248	/29	6 useable IP addresses
255.255.255.240	/28	14 useable IP addresses
255.255.255.224	/27	30 useable IP addresses
255.255.255.192	/26	62 useable IP addresses
255.255.255.128	/25	126 useable IP addresses
255.255.255.0	/24	254 useable IP addresses
255.255.254.0	/23	508 useable IP addresses
255.255.252.0	/22	1016 useable IP addresses
255.255.248.0	/21	2032 useable IP addresses
255.255.240.0	/20	4064 useable IP addresses

Common WebGUI Interactions

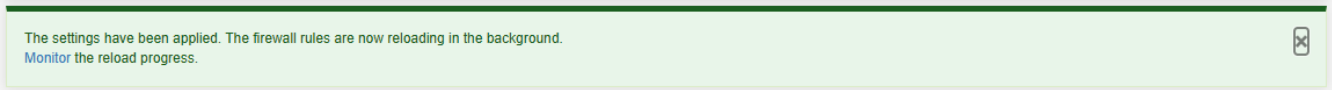
Applying Changes

When adding or making changes to the configuration via the Anybus Defender WebGUI, in many cases, after the change is saved, the WebGUI will require the changes to be “applied”. The change is saved but has not “gone live” in Anybus Defender yet. A banner will appear at the top of the section being edited:



Sample Apply Changes Banner

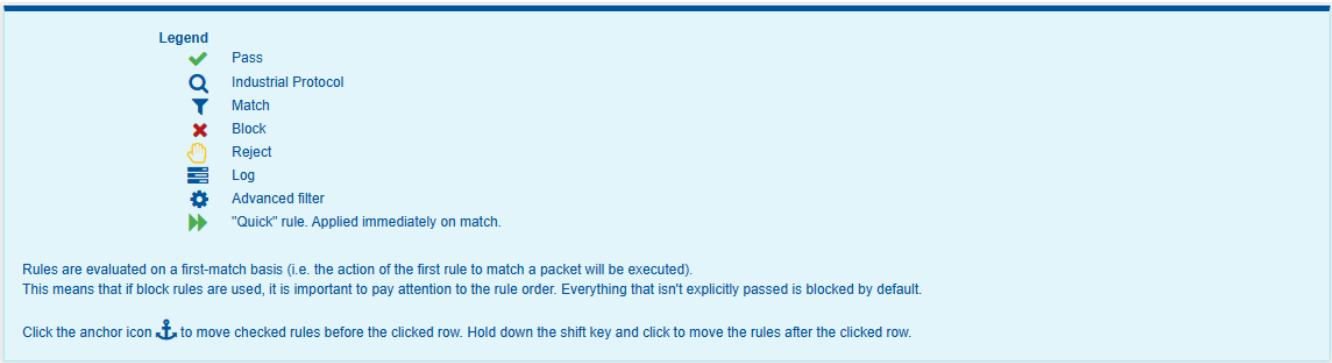
Once the changes are applied, they become active and the Anybus Defender will display a confirmation that the changes have been applied successfully. Click the X on the right side of the confirmation to close it:



Sample Changes Applied Confirmation Banner

Context Help/Additional Information

The  information icon will appear in various locations through the WebGUI. When clicked, additional information about a given topic will be displayed:



Information Legend with Appropriate Icon Definitions

Overview

Next-Gen Protection

The Anybus Defender is a state-of-the-art cybersecurity device to handle any Industrial Control System Security required on the plant floor or IT server room. The key features of the Anybus Defender are:

- Diverse product line to handle any deployment scale
- Comprehensive WebGUI that uses a standard web browser to access all functionality
- Setup wizards for Simple and Standard NAT configurations
- A stateful firewall that keeps track of the state of active connections traversing it, allowing for enhanced security and granular control of network traffic. A state table maintains knowledge about established connections, including the state of the connection (such as whether it's part of an established session or a new connection attempt)
- Extensive diagnostics
- VPN server, clients, and secure connections to devices
- User Manager with groups, user certificates, and ability to include LDAP or Radius authentication servers
- Captive Portal to control device access
- External packages that can be imported and used (Snort, Asset Manager, etc.)
- Deep Packet Inspection (DPI) that allows finite control of access to PLCs, HMIs, and similar devices

Hardware Models

Anybus Defender Product Line

Here is a list of web links and datasheets for all the Anybus Defender models offered:

[4002 NAT/FW](#) [Datasheet](#)

[4002 DPI/FW](#) [Datasheet](#)

[4002 PRO/FW](#) [Datasheet](#)

[6004 NAT/FW](#) [Datasheet](#)

[6004 DPI/FW](#) [Datasheet](#)

[6004 PRO/FW](#) [Datasheet](#)

[6024 NAT/FW](#) [Datasheet](#)

[6024 DPI/FW](#) [Datasheet](#)

[6024 PRO/FW](#) [Datasheet](#)

[1004 NAT/FW](#) [Datasheet](#)

Console and Web Configuration Interfaces

The Anybus Defender devices can be accessed in one of these ways:

1. Direct Connection via The Console
2. WebGUI
3. SSH (Secure Shell)

Console Direct Connection

Using a USB-based keyboard and a monitor using HDMI or VGA port (if available), the Anybus Defender Console can be accessed

```
ICS360.Defender/amd64 (ICS360-Defender.localdomain) (ttyv0)

** Welcome to ICS360.Defender 2.5.2-RELEASE-2023122519 (amd64) **
** Hostname: ICS360-Defender **
*** License variant: PRO ***

WAN (wan)      -> vmx0      -> v4/DHCP4: 192.168.68.88/22
LAN (lan)      -> vmx1      -> v4: 192.168.200.2/24

0) Logout (SSH only)          10) Filter Logs
1) Assign Interfaces          11) Restart webConfigurator
2) Set interface(s) IP address 12) Update from console
3) Reset admin password       13) Enable Secure Shell (sshd)
4) Reset to factory defaults  14) Restore recent configuration
5) Reboot system              15) Offline update
6) Shutdown system
7) Ping host
40) Enable Mgmt Anti-lockout   41) Enable WAN Mgmt Anti-lockout

Enter an option: █
```

Direct Connect Screen

Licensing

Anybus Defender License Features

Here is a table listing all the license types and their feature sets:

	NAT (-NAT)	DPI (-DLT)	PROFESSIONAL (-PRO)
GENERAL	✓	✓	✓
Cybersecurity Console Manage/Monitor multiple Defenders	✓	✓	✓
NAT Network Address Translation	✓	✓	✓
DIAGNOSTICS Troubleshoot traffic, network, and device config	✓	✓	✓
NOTIFICATIONS Email, Syslog, Telegram, Pushover	✓	✓	✓
STATEFULL FIREWALL Control network traffic	✓	✓	✓
REMOTE ACCESS IPSec, SSL, WireGuard, VPN		✓	✓
CERTIFICATE MANAGEMENT Local / Enterprise		✓	✓
USER MANAGEMENT AD/LDAP/RADIUS/Local Authentication Types	✓ Local Users	✓	✓
DHCP Dynamic Host Configuration Protocol		✓	✓
CAPTIVE PORTAL Control supplier access		✓	✓
DNS Domain Name System		✓	✓
ASSET DETECTION & MONITORING Track network assets by type, serial number, firmware, etc.	✓	✓	✓
PACKAGES Adds additional functionality above base system	✓	✓	✓
RULES/POLICY SCHEDULER Schedule rules by date/time/duration		✓	✓
NTP (Network Time Protocol) Synchronize time to master clocks		✓	✓
DPI (Deep Packet Inspection) Finite control of access to PLC/HMI/Devices		✓	✓

	NAT (-NAT)	DPI (-DLT)	PROFESSIONAL (-PRO)
IPS/IDS Snort / Suricata		✓	✓
LOAD BALANCING Use multiple uplinks to increase throughput			✓
TRAFFIC SHAPING			✓
HIGH AVAILABILITY Redundancy for critical paths			✓

To access the License section of the Anybus Defender, use the WebGUI to navigate to the **System/License** page:

System / License

Anybus Defender details

UUID: 19a94d56-40ec-79c9-6e73-4cd417a438d1
 Serial: VMware-56 4d a9 19 ec 40 c9 79-6e 73 4c d4 17 a4 38 d1
 MAC addr: 00:0c:29:a4:38:d1

Copy to Clipboard Export

License Information

Identifier: p8Qb-9Aw4-pn13-UREA
 Variant: PRO
 Features: NAT INDPRO GENERAL VPN FILTER DHCP NTP DYNDNS CAPTIVEPORTAL PKG DNS EXTRASERVICES TRAFFICSHAPER SCHEDULE FAILOVER CERTMGR REMOTEUSER

Upload License

License file No file chosen

License

The firewall will discard the old license, if present, and use the new uploaded one.

License Page of WebGUI

Upgrading a License

All Anybus Defender units get shipped from the factory with a license already applied. However, the license can be upgraded at any time with an upgrade purchase. Contact sales@hms-networks.com to inquire about current license types and pricing

Creating a License File

From the **System/License** page, use the **Copy to Clipboard** or, better yet, the **Export** button to create a license request file. Send that request file to sales@hms-networks.com (this assumes the appropriate license has been purchased)

Applying a New License

❗ Applying a new license will temporarily shutdown and restart the Anybus Defender device

A reply email will contain the license file. From the **Upload License** section, click the **Choose File** button. Select the new license then click the **License** button.

The Anybus Defender device will restart. From the **License** or **Dashboard** page, the **License** Information section will show which **Variant** (see table above) and which **Features** are enabled

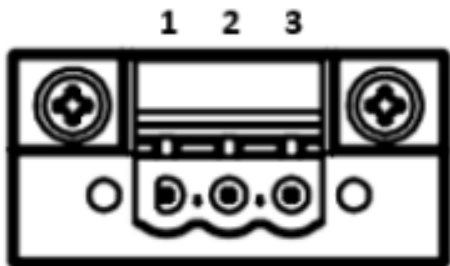
Powering Up

⊗ The Anybus Defender is shipped with a secure profile (default) on the WAN interface. The LAN interface is open and not considered secure

Power Connections

Typically, most Anybus Defender units will require 24VDC supplied to the power connection

For the PICO, NANO, and MINI units, a 3-pole Phoenix connector is used to wire in power and ground:



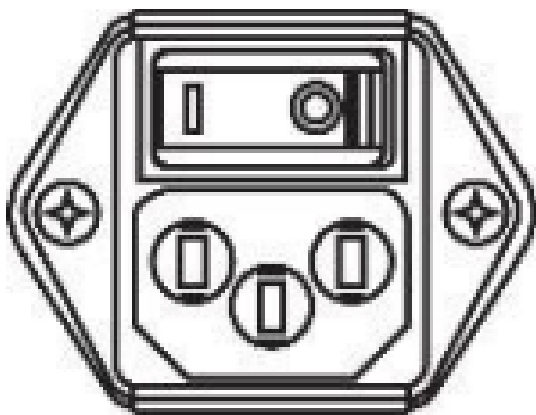
PIN 1: V+

PIN 2:  (Chassis Ground)

PIN 3: V-

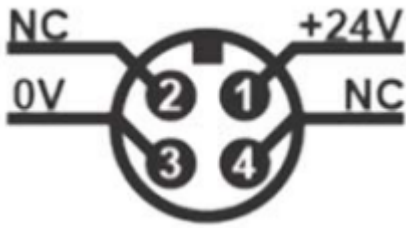
Phoenix Connector with Terminal Callouts

For the 1U unit, the same 24VDC connector shown above or a standard 120VAC connection is available depending on order:



Standard 120VAC Plug with Power Toggle Switch

For the IP65 unit, a sealed 4-Pin M12 connector is used:



M12 Connector Pinout

❗ Except for the 1U 120VAC models, most Anybus Defender units will immediately power up once the required voltage is applied to the unit. Older units or the 1U and IP65 models may have a power button that must be pressed

To ensure proper power up, each unit has a power indicator.

Network Connections

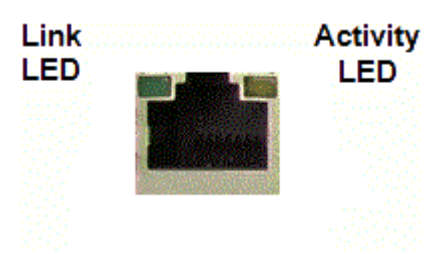
⊗ The Anybus Defender is shipped with a secure profile (default) on the WAN interface. The LAN interface is open and not considered secure

RJ45 Network Connections

Most Anybus Defender models have at least 2 RJ45 Ethernet ports representing NICs for each port. One port is labeled **IGB0 (RE0** for older units) and **IGB1 (RE1** for older units). Out of the box, the **IGB0** port is the WAN or enterprise NIC and the **IGB1** port is LAN or local network NIC

❗ The NICs can be repurposed for any network configuration required

Each port connection has two indicators, a **Link** and **Activity** LED:



Ethernet Port with LEDs

LED	Color	Description
LINK LED	AMBER OR GREEN	AMBER ON: OPERATING AS A GIGABIT CONNECTION (1000 MBPS) GREEN ON: OPERATING AS A 100-MBPS CONNECTION OFF: OPERATING AS A 10-MBPS CONNECTION.
Activity LED	Green	Blinking: There is activity on this port. Off: No link is established.

WebGUI Login

⊗ The Anybus Defender is shipped with a secure profile (default) on the WAN interface. The LAN interface is open and not considered secure

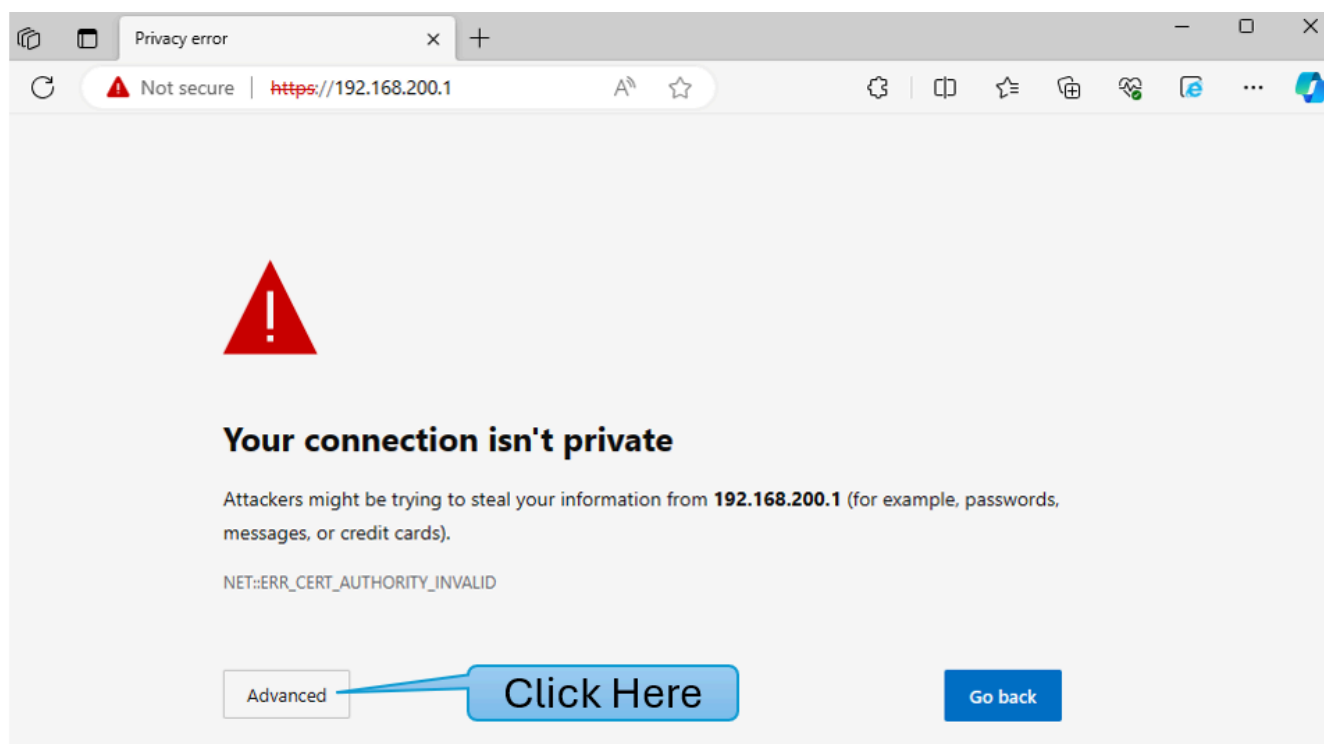
For Access to the Anybus Defender WebGUI

Using the [LAN Network Connection](#), connect a PC to the LAN NIC. Be sure the PC's NIC is set to **192.168.200.xxx** where xxx is any number greater than 1. The subnet mask should be set to **255.255.255.0**

WebGUI Login

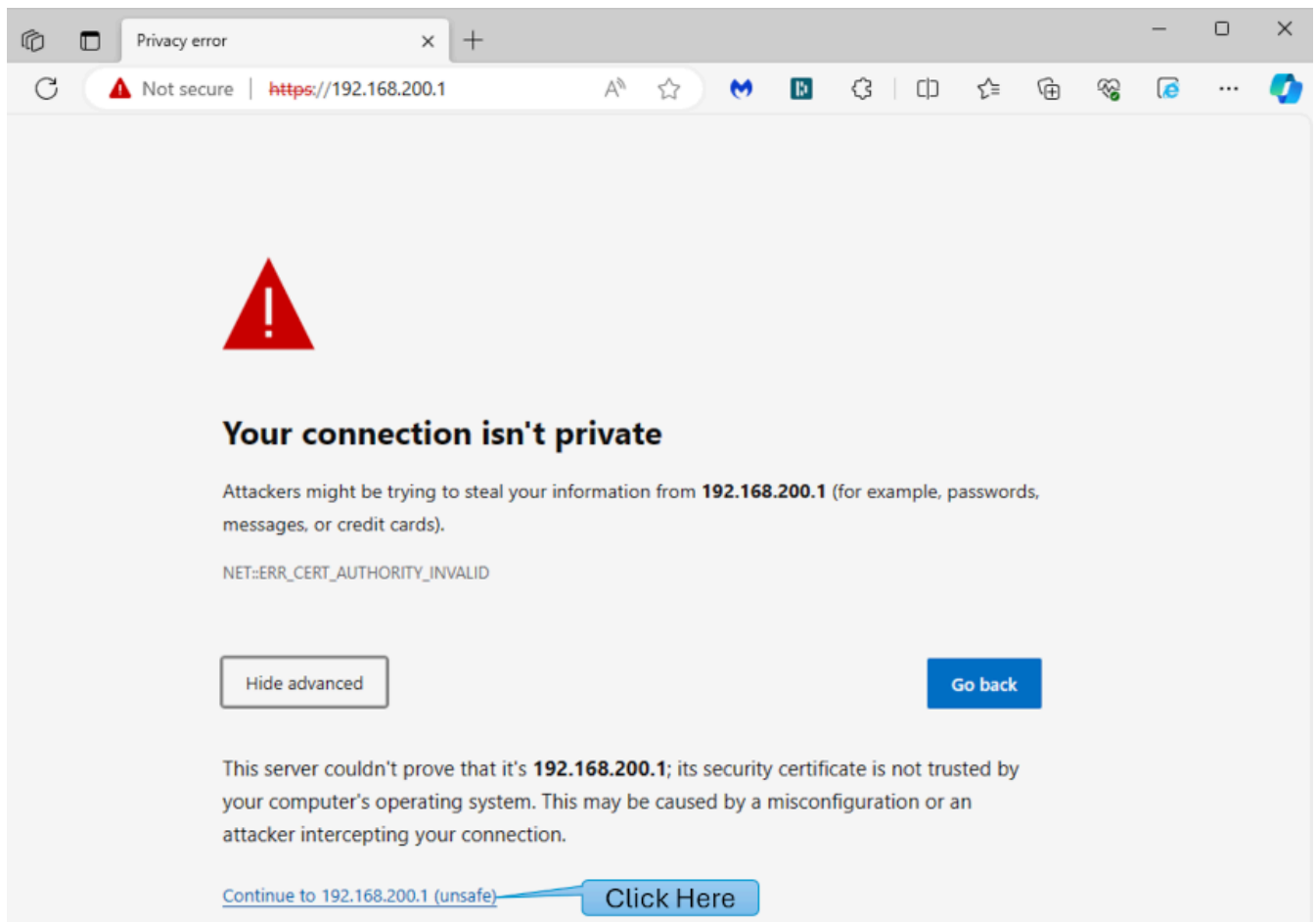
The default LAN IP address of the Anybus Defender is **192.168.200.1** with a subnet mask of **255.255.255.0**. Using a web browser (Microsoft Edge or Google Chrome is recommended), type in the LAN IP address

When connecting to an unconfigured Anybus Defender, web browsers may indicate an unsecured connection. This notice is normal as the current configuration of the security appliance doesn't contain the necessary settings to prevent the warning. If this screen does not appear, continue to the next paragraph. Otherwise, click **Advanced** then **Proceed to 192.168.200.1 (unsafe):**



Connection not Private Warning

then



Connection not Private Warning

After an initial Welcome Screen when the Anybus Defender is first powered up, a login screen will appear requiring a **Username** and **Password** to be entered. The default **Username** is **admin** and the default **Password** is **defender**:

⊗ It is very important to change the default password when creating a configuration for the Anybus Defender



Login to Anybus Defender

Username

Enter your username

Password

Enter your password

Login

Login with Default Credentials

Simple NAT Wizard

Overview

The Simple NAT Wizard is a quick and easy way to set up:

1. A new Admin Password to replace the default password (highly recommended)
2. The WAN IP Address, Subnet Mask, and any Upstream Gateway address
3. The LAN IP Address and Subnet Mask
4. Allowing WAN side access to the Anybus Defender WebGUI
5. Allowing WAN and LAN pings
6. Any 1:1 NAT Mappings needed

Accessing the Simple NAT Wizard

If the license used in the Anybus Defender is set to **SIMPLE-NAT**, the Simple NAT Wizard will automatically load upon login. Any other license will require navigating to **System>Setup Wizard** to start the Wizard.

❗ Loading the **Setup Wizard** will present 2 button options: **>> Next** and **>> Use Simple NAT Wizard**. Be sure to select the **>> Use Simple NAT Wizard** option. The other button will start the **Standard NAT Wizard**

Simple NAT Wizard Configuration

Wizard / NAT Configuration /

NAT Configuration

Hostname

Anybus-Defender

EXAMPLE: myserver

Admin Password

Confirm Admin Password

WAN IP Configuration

Interface Mode

DHCP

IP Address

192.168.70.204

Subnet Mask

24

Upstream Gateway

192.168.70.1

LAN IP Configuration

IP Address

192.168.200.2

Subnet Mask

24

Configure 1:1 NAT Mappings

Interface	Northbound IP	Southbound IP	Description	Actions
wan	192.168.100.22	192.168.200.122	Zone1 Sta2 PLC	

>> Add 1:1 NAT

>> Apply

Simple NAT Wizard Page

Anybus Defender Configuration

- **Hostname:** Optional ability to change the default Hostname given to the Anybus Defender
- **Admin Password:** New admin password can be changed here (highly recommended)
- **Confirm Admin Password:** Re-type admin password used above

WAN IP Configuration

- **Interface Mode:** Set to either **DHCP** if a DHCP server will automatically set the WAN IP, Subnet, and Gateway or **Static** to enter the configuration manually.
- **IP Address:** (Available only on **Static** Interface Mode) Type in the desire IP address for the WAN network
- **Subnet Mask:** (Available only on **Static** Interface Mode) Use the dropdown to select the proper Subnet Mask using the [Subnet Mask to CIDR Table](#) for reference

LAN IP Configuration

- **IP Address:** Type in the desire IP address for the LAN network
- **Subnet Mask:** Use the dropdown to select the proper Subnet Mask using the [Subnet Mask to CIDR Table](#) for reference

Configure 1:1 NAT Mappings

2 buttons appear here:

- **>> Add 1:1 NAT** will load the 1:1 NAT Creation page (see below)
- **>> Apply** will save all the current Anybus Defender Configuration, WAN and LAN Network settings, and all newly-configured 1:1 NAT configurations

New 1:1 NAT Creation

Wizard / NAT Configuration / New 1:1 NAT Creation

Step 1 of 2

New 1:1 NAT Creation

Create a new 1:1 NAT Entry

1:1 NAT Rule Creation

Northbound Interface

WAN

Southbound Interface

LAN

Northbound IP Address

192.168.70.117

External IP Address

Southbound IP Address

192.168.200.137

Internal IP Address

Description

S05OP12 PLC

>> Add 1:1 NAT

1:1 NAT Creation Page

Clicking the >> **Add 1:1 NAT** button will load the **New 1:1 NAT Creation** page. From here, a **Northbound** (usually WAN) and **Southbound** (usually LAN) mapping can be created to allow Northbound access to a Southbound device:

1:1 NAT Rule Creation

- **Northbound Interface:** Use the dropdown to select the Interface to be used for Northbound
 - **Southbound Interface:** Use the dropdown to select the Interface to be used for Southbound
 - **Northbound IP Address:** Type in the IP address to be used as the Northbound address
- !** This IP address must be unique and NOT the same address as the Northbound Interface that was configured above
- **Southbound IP Address:** Type in the IP address of the actual Southbound device
 - **Description:** Optional text that can be typed in to identify this device

Once completed, the >> **Add 1:1 NAT** button must be clicked to save the new 1:1 mapping. The Simple NAT Wizard main page will load with the new 1:1 Mapping in the **Configure 1:1 NAT Mappings** section:

Configure 1:1 NAT Mappings					
	Interface	Northbound IP	Southbound IP	Description	Actions
	wan	192.168.70.117	192.168.200.137	S05OP12 PLC	

1:1 NAT Mapping Table

Also, A message will appear on the top of the page warning that changes need to be applied:

Wizard / NAT Configuration /

The 1:1 NAT rules have changed. The changes must be applied to take effect.

Apply Changes Warning Banner

Click the >> **Apply** button next to the >> **Add 1:1 NAT** button to apply all changes

WAN Access to the WebGUI

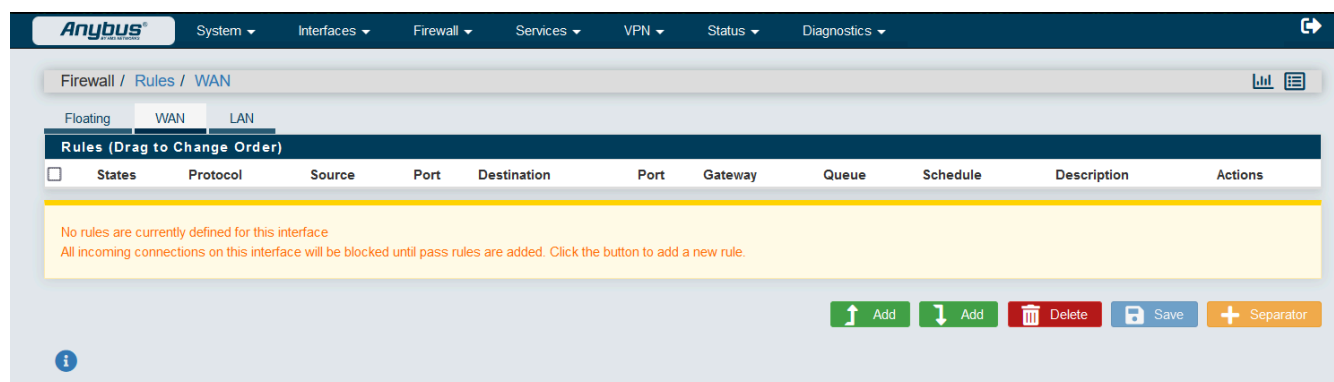
Prerequisites

To be able to access the WebGUI, either the [Simple NAT Wizard](#) needs to be completed or a rule has to be added manually. When properly configured, the WAN gateway address can be used in the web browser instead of the LAN

Manual WAN Access Rule Creation

! This functionality requires at least the **NAT** license or greater

To allow access to the WebGUI from the WAN, navigate to **Firewall>Rules>** then be sure the **WAN** tab is selected:



Firewall>Rules>WAN Section

Click either + **Add** button at the lower right of the **Rules** table to load the **Rule Creation** page. Adjust the rule settings exactly as shown below:

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass
 Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
 Hint: Choose an Industrial Profile to send packets matching the flow for extra evaluation to the classifier.

Disabled ☐ Disable this rule
 Set this option to disable this rule without removing it from the list.

Interface WAN
 Choose the interface from which packets must come to match this rule.

Address Family IPv4
 Select the Internet Protocol version this rule applies to.

Protocol TCP
 Choose which IP protocol this rule should match.

Source

Source ☐ Invert match. any Source Address /
Display Advanced
 The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination ☐ Invert match. This firewall (self) Destination Address /
Destination Port Range HTTPS (443) HTTPS (443)
 From Custom To Custom
 Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☐ Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description Allow WAN management
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options Display Advanced

Save

Settings to Allow WAN Access to WebGUI

Save and Apply the new rule and it should now appear on the **WAN Rules** table:

Firewall / Rules / WAN

Floating **WAN** LAN OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐ ✓ 4 / 112 K B	IPv4	TCP	*	*	This Firewall	443 (HTTPS)	*	none		Allow WAN management	Anchor Edit Copy Delete

↑ Add ↓ Add Delete Save + Separator

WAN Access Rule on Rules Table

Now the WAN address can be used in the web browser to access the WebGUI

Basic Troubleshooting

Overview

If the power light does not energize, confirm the presence and polarity of 24VDC to the appliance (older Anybus Defender units may have a power button that needs to be pressed)

❗ The power connector only fits into the plug on the Anybus Defender a certain way. The polarity (+ / -) is printed above the [connector on the front of the appliance](#)

WebGUI

Logging Into the WebGUI

After typing the default IP address into a browser window, if the Anybus Defender login or security challenge doesn't appear, check the following:

1. Make sure the appliance is powered up by observing the white power indicator light (older units will have the power light surrounding the power button)
2. Confirm that an RJ45 Ethernet cable is connected to the LAN interface (IGB1 or RE1) from the PC
3. Confirm that the PC from which the login is attempted has an IP address in the 192.168.200.x address range

Console

Visual Confirmation of Startup

As described in the [Console Direct Connect Page](#), the front panel on the appliance has video and USB ports. Connecting a display to one of the video ports should provide visual confirmation that Anybus Defender is powered up and has successfully started. When the appliance has completed bootup, a login prompt should appear:

Dashboard Overview

Overview

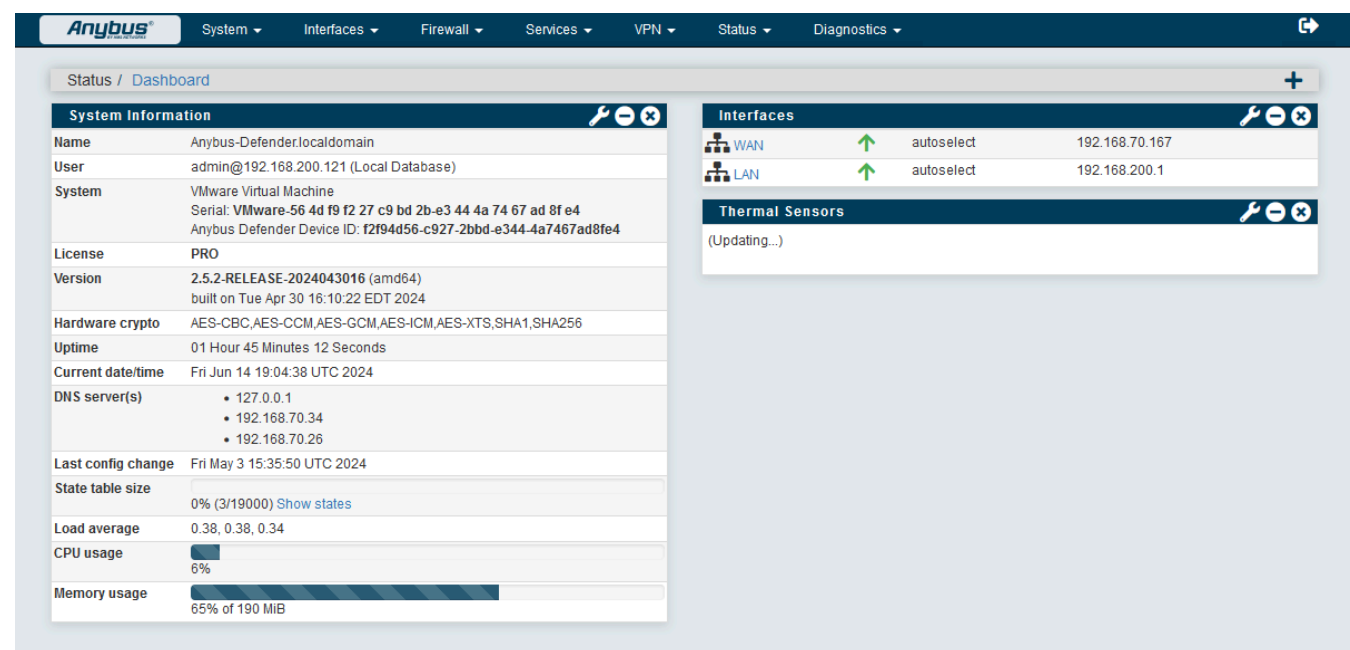
The Dashboard of the Anybus Defender WebGUI houses widgets that can be displayed on the dashboard page and shows general status on various aspects of the appliance. This dashboard is automatically loaded when first logging into the WebGUI. It can also be access from 2 other places:

1. The Anybus Defender icon on the top left of the menu bar:



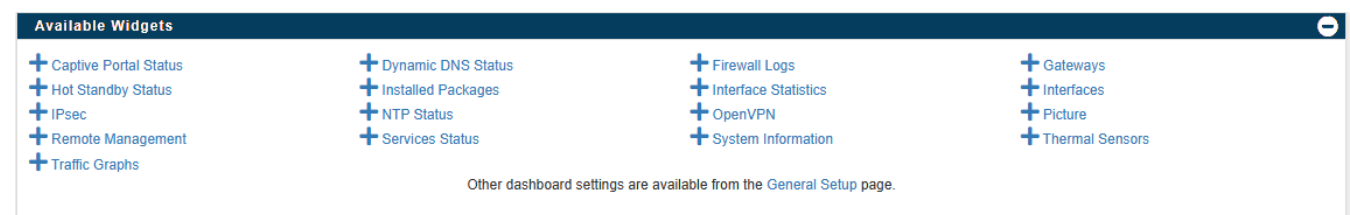
2. Clicking on the **Status>Dashboard** menu item

By default, the [System Information](#), [Interfaces](#), and [Thermal Sensor](#) widgets are visible on the dashboard:



Adding Widgets

On the upper right of the dashboard page is a button that allows widgets to be added to the dashboard page. Clicking the plus button will open an Available Widgets panel:



Available Widgets Panel

From there, the next to each widget allows it to be added to the dashboard section

Removing or Collapsing Widgets

On the widget title, two buttons are used for collapsing  or expanding  the title bar. The  button removes the widget from the dashboard

Widget Settings

More widgets have a  on the upper right on the title bar. That will toggle on/off an extra panel that will allow settings to be adjusted on the widget

Capture Portal Status

Captive Portal Status				
IP address	MAC address	Username	Session start	Last activity

Captive Portal Status Widget

Overview

If the [Captive Portal](#) Feature is used, the **Captive Portal Status** widget will display any users that have logged into the Anybus Defender via the portal. The user's IP address, MAC address, Username, Session Start, and Last activity will appear on a list

Dynamic DNS Status

Dynamic DNS Status			
Int.	Service	Hostname	Cached IP
WAN	Azure DNS	Test	0.0.0.0

Dynamic DNS Status Widget

Overview

If the [Dynamic DNS](#) (DDNS) Feature is used, the **Dynamic Status** widget will display any users that have logged into the Anybus Defender via the portal. The DDNS Interface, Service Type, Hostname, and Cached IP address will appear on the list

Settings

Widget title

Dynamic DNS Status

Interface	Service	Hostname	Show
WAN	Azure DNS	Test	☒

Save

None

Dynamic DNS Status Settings

These items can be configured for this widget:

- **Widget title:** The title bar of this widget can be changed from its default name
- **Show Checkbox(es):** Allows selectively showing/hiding DDNS entries on the list
- **Save Button:** Saves the current widget configuration
- **All/None Button:** Toggles **All** or **None** of the checkboxes explained above

Firewall Logs

Firewall Logs				
Act	Time	IF	Source	Destination
✖	2024-01-29 14:18:27.324406+00	WAN	192.168.68.83	192.168.71.255:54915
✖	2024-01-29 14:18:28.323185+00	WAN	192.168.68.83	230.0.0.1:6666
✖	2024-01-29 14:18:28.323235+00	WAN	192.168.68.53	255.255.255.255:6667
✖	2024-01-29 14:18:28.323263+00	WAN	192.168.68.80	255.255.255.255:6667
✖	2024-01-29 14:18:28.323290+00	WAN	192.168.68.83	192.168.71.255:54915

Firewall Logs Widget

Overview

The [Firewall Logs](#) Logs widget shows the latest list of [Firewall Rules](#) that have been triggered based on network activity

Settings

Widget title

Firewall Logs

Number of entries

5

Filter actions

☐ Pass ☐ Block ☐ Reject

Filter interface

ALL

Update interval

60

Seconds

Save

Firewall Logs Settings

These items can be configured for this widget:

- **Widget title:** The title bar of this widget can be changed from its default name
- **Number of entries:** Number of rows to show on the Logs table
- **Filter actions:** Choose whether only Pass and/or Block and/or Rejects rules appear on the Logs table
- **Filter interface:** Dropdown selection to choose which interface to show on the Logs table, including All interfaces
- **Update Interval:** Number entry box to set the time interval for the Logs table refresh
- **Save Button:** Saves the current widget configuration

Gateways

Gateways   					
	Name	RTT	RTTsd	Loss	Status
	WAN_DHCP  192.168.68.1	0.9ms	0.4ms	0.0%	Online

Gateways Widget

Overview

The [Gateways](#) widget shows a list of any configured gateways and their current status

Settings

Widget title

Gateways

Display

☒ Gateway IP

☐ Monitor IP

☐ Both

Gateway

WAN_DHCP

Show

☒

Save

All

Gateways Settings

These items can be configured for this widget:

- **Widget title:** The title bar of this widget can be changed from its default name
- **Display options:** Use the radio button selector to choose one of these options:
 - **Gateway IP:**
 - **Monitor IP:**
 - **Both:**
- **Gateway Table:** List of all current gateways. Each can be shown/hidden using the **Show** checkbox
- - **Save Button:** Saves the current widget configuration
 - **All/None Button:** Toggles **All** or **None** of the checkboxes explained above

Hot Standby Status

Hot Standby Status		
Hot Standby Interface	IP Address	Status
No Hot Standby Interfaces Defined. Click here to configure Hot Standby.		

Hot Standby Widget

Overview

The [Hot Standby](#) widget shows a list of any interfaces that has been configured as a hot standby. The List will show the Interface, IP Address, and Status of each hot standby

Installed Packages

Installed Packages				
Name	Category	Version	Description	Actions
✓ API	sysutils	1.3.4_1	Provide modular RESTful APIs for use by a remote server.	 
✓ AssetMgmt	sysutils	1.0.1_6	A package to scan hosts on the network and identify OS and/or Industrial Protocol information.	 
✓ RemoteMgmt	sysutils	0.5.1	A package to integrate with a remote management server to allow remote control/visibility of this instance	 
 = Update  = Current  = Remove  = Information  = Reinstall Newer version available Package is configured but not (fully) installed or deprecated				

Installed packages Widget

Overview

Any packages installed from the [Packages Manager](#) will show on this list. Each row consists of:

- **Name:** The name of the package
- **Version:** The version number of the package
- **Actions:** Depending on the package type, these buttons will be present:
 -  Uninstalls the package
 -  Reinstalls the package
 -  (Where applicable) Loads more information on the package

Interface Statistics

Interface Statistics   		
	WAN	LAN
Packets In	42328	50671
Packets Out	43152	37493
Bytes In	1.65 MiB	8.27 MiB
Bytes Out	1.44 MiB	12.64 MiB
Errors In	0	0
Errors Out	0	0
Collisions	0	0

Interface Statistics Widget

Overview

This widget displays network traffic statistics for each [Interface](#) on a table. The table items are:

Interface Columns: Each interface (WAN and LAN in the example above) will have a table column for its own network statistics

 These columns can be inverted to show each interface as a row using the **Settings** below

Packets In: Total number of incoming packets to the unit for each interface

Packets Out: Total number of outgoing packets from the unit for each interface

Bytes In: Total number of incoming bytes to the unit for each interface

Bytes Out: Total number of outgoing bytes from the unit for each interface

Errors In: Total number of incoming errors to the unit for each interface

Errors Out: Total number of outgoing errors from the unit for each interface

Collisions: Total number of collisions that occurred from the unit for each interface



Settings

Widget title

Interface Statistics

Orientation

☒ Each interface in a column

☐ Each interface in a row

Interface	Show
WAN	☒
LAN	☒
Stats Item	Show
Packets In	☒
Packets Out	☒
Bytes In	☒
Bytes Out	☒
Errors In	☒
Errors Out	☒
Collisions	☒

Save

None

Interface Statistics Settings

These items can be configured for this widget:

- **Widget title:** The title bar of this widget can be changed from its default name
- **Orientation:** Radio button selection to change the row/column configuration of the interfaces and their respective network statistics:
 - **Each interface in a column:** The interfaces will be the columns and the network statistics will be the rows
 - **Each interface in a row:** The network statistics will be the columns and the interfaces will be the rows
- **Interface and Stats Checkboxes:** Toggle whether each Interface and Stat item is shown/hidden with the right-hand checkboxes
- **Save Button:** Saves the current widget configuration
- **All/None Button:** Toggles **All** or **None** of the checkboxes explained above

NTP Status

NTP Status		
Server Time	19:20:51 UTC	
Sync Source	No active peers available	

NTP Status Widget

Overview

This widget shows a list of any [NTP Clock](#) that have been configured for this unit. This will show the **Server Time** and **Server Source** of the NTP Server

OpenVPN

OpenVPN		
Server UDP:1194		
Name/Time	Real/Virtual IP	
fusiondevs	47.26.2.170:1194	
Mon Jan 29 19:46:57 2024	172.19.0.2	

OpenVPN Widget

Overview

This widget shows a list of any [OpenVPN Servers](#) that have been configured for this unit. There may also be [Users](#) connected to each server which will appear as a list under each OpenVPN Server section

For each OpenVPN server, the user list will contain this information:

Name/Time: The username login time when connected to the server

Real/Virtual IP: The actual IP address allocated to the user and the internal [Tunnel IP Address](#) created by the OpenVPN configuration



Settings

Name	Show
Server UDP:1194	☒

 Save  None

OpenVPN Settings

These items can be configured for this widget:

- **OpenVPN Server List:** Each OpenVPN server can be shown/hidden by using the checkboxes on the right
- **Save Button:** Saves the current widget configuration
- **All/None Button:** Toggles **All** or **None** of the checkboxes explained above

Picture



Picture Widget

Overview

This widget allows an image file to be loaded and shown on the dashboard. Compatible images files are .tiff, .jfif, .bmp, .gif, .svg, .png, .jpeg, .svgz, .jpg, .webp, .ico, .xbm, .dib, .ppj, .apng, .tif, .avif



Settings

Widget title	Picture
New pictures:	Choose File No file chosen
Save	

Picture Settings

These items can be configured for this widget:

- **Widget title:** The title bar of this widget can be changed from its default name
- **New Picture:** Use the **Choose File** button to load a compatible image file
- **Save:** Click to save the picture to the Anybus Defender

i If this widget is removed then re-added, the last saved picture will still appear

Remote Management

Remote Management

Status

NOT ENABLED [Configure](#)

Server

NOT CONFIGURED

Remote Management Widget

Overview

This widget shows the status of the **Anybus Cybersecurity Console (ACC)** connection. The items shown are:

- **Status:** Whether this unit is connected to a ACC instance
- **ACC Server:** The IP address and Port of the connected ACC instance

i The Anybus ACC product is a separate application used to manage multiple Anybus Defender units. Contact sales@hms-networks.com for more information

Services Status

Services Status			  
Service	Description	Action	
 dpinger	Gateway Monitoring Daemon	 	
 identifyasset	Asset Management	 	
 openvpn	OpenVPN server:	 	
 remote_management	DCC Integration	 	
 syslogd	System Logger Daemon	 	
 unbound	DNS Resolver	 	

Services Status Widget

Overview

This widget displays a list of all the [Services](#) configured to run on the Anybus Defender. Each service on the list has these columns:

- Running/Stopped Indicators:** on the left side of each row are two icons indicating whether the service is Running  or Stopped 
- Service:** The service name
- Description:** Description of the service
- Action:** When a service is running, the **Restart**  and **Stop**  **Service** buttons appear. If a service is stopped, the **Start Service**  button will attempt to start the service

Settings

Widget title

Service	Show
dpinger	☒
identifyasset	☒
openvpn	☒
remote_management	☒
syslogd	☒
unbound	☒
vmware-guestd	☒
vmware-kmod	☒

Services Status Settings

These items can be configured for this widget:

- **Widget title:** The title bar of this widget can be changed from its default name
- **Services Checkboxes:** Toggle whether each Service item is shown/hidden with the right-hand checkboxes
- **Save Button:** Saves the current widget configuration
- **All/None Button:** Toggles **All** or **None** of the checkboxes explained above

System Information

System Information		 
Name	Anybus-Defender.localdomain	
User	admin@192.168.200.121 (Local Database)	
System	VMware Virtual Machine Serial: VMware-56 4d f9 f2 27 c9 bd 2b-e3 44 4a 74 67 ad 8f e4 Anybus Defender Device ID: f2f94d56-c927-2bbd-e344-4a7467ad8fe4	
License	PRO	
Version	2.5.2-RELEASE-2024043016 (amd64) built on Tue Apr 30 16:10:22 EDT 2024	
Hardware crypto	AES-CBC,AES-CCM,AES-GCM,AES-ICM,AES-XTS,SHA1,SHA256	
Uptime	01 Hour 55 Minutes 48 Seconds	
Current date/time	Fri Jun 14 19:15:14 UTC 2024	
DNS server(s)	• 127.0.0.1 • 192.168.70.34 • 192.168.70.26	
Last config change	Fri May 3 15:35:50 UTC 2024	
State table size	0% (4/19000) Show states	
Load average	0.32, 0.41, 0.39	
CPU usage	5%	
Memory usage	63% of 190 MiB	

System Information Widget

Overview

This widget shows common system information on the Anybus Defender, license, uptime, etc. Information included:

- **Name:** The name of the Anybus Defender unit
- **User:** The current user logged into the WebGUI
- **System:** The **Serial Number** and **Device ID** of the unit
- **License:** The current [License](#) installed
- **Version:** The current firmware version of the Anybus Defender with its build date
- **Hardware crypto:** List of all encryption types supported in this unit
- **Uptime:** Number of Hours, Minutes, and Seconds the unit has been running
- **Current date/time:** Date and Time set within the unit
- **DNS server(s):** All DNS used in the unit
- **Last config change:** last applied changes to the unit
- **State table size:** number of **States** configured within the unit. Use the [Show States](#) link to load the actual States table
- **Load average:**
- **CPU usage:** Percentage of the CPU used
- **Memory usage:** Percentage of the Memory used



Settings

Item	Show
Name	☒
User	☒
System	☒
BIOS	☒
Version	☒
CPU Type	☒
Hardware Crypto	☒
Kernel PTI	☒
MDS Mitigation	☒
Uptime	☒
Current Date/Time	☒
DNS Server(s)	☒
Last Config Change	☒
State Table Size	☒
MBUF Usage	☒
Temperature	☒
Load Average	☒
CPU Usage	☒
Memory Usage	☒
Swap Usage	☐
Disk Usage	☐

Save

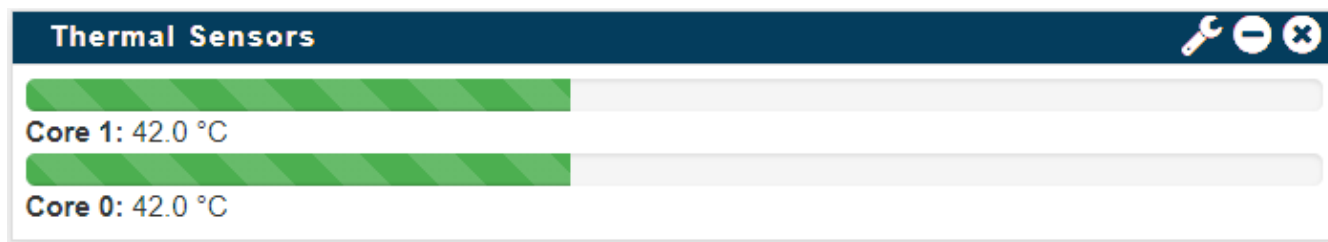
All

System Information Settings

These items can be configured for this widget:

- **System Info Checkboxes:** Toggle whether each System Information item is shown/hidden with the right-hand checkboxes
- **Save Button:** Saves the current widget configuration
- **All/None Button:** Toggles **All** or **None** of the checkboxes explained above

Thermal Sensors



Thermal Sensors Widget

Overview

This widget shows a temperature gauge and readout of each CUP core in the Anybus Defender

Settings

The screenshot shows the "Thermal Sensors Settings" panel. It is divided into two main sections: "Thresholds in °C (1 to 100):" and "Display settings:". Under the thresholds section, there are four input fields: "Zone Warning:" (60), "Zone Critical:" (70), "Core Warning:" (60), and "Core Critical:" (70). Under the display settings section, there are two checkboxes: "Show raw output (no graph):" and "Show full sensor name:", both of which are currently unchecked. A blue "Save" button with a floppy disk icon is located at the bottom right of the settings panel. Below the settings, there is a note: "* A proper Thermal Sensor / Module can be configured under System > Advanced > Miscellaneous : Thermal Sensors section."

Thermal Sensors Settings

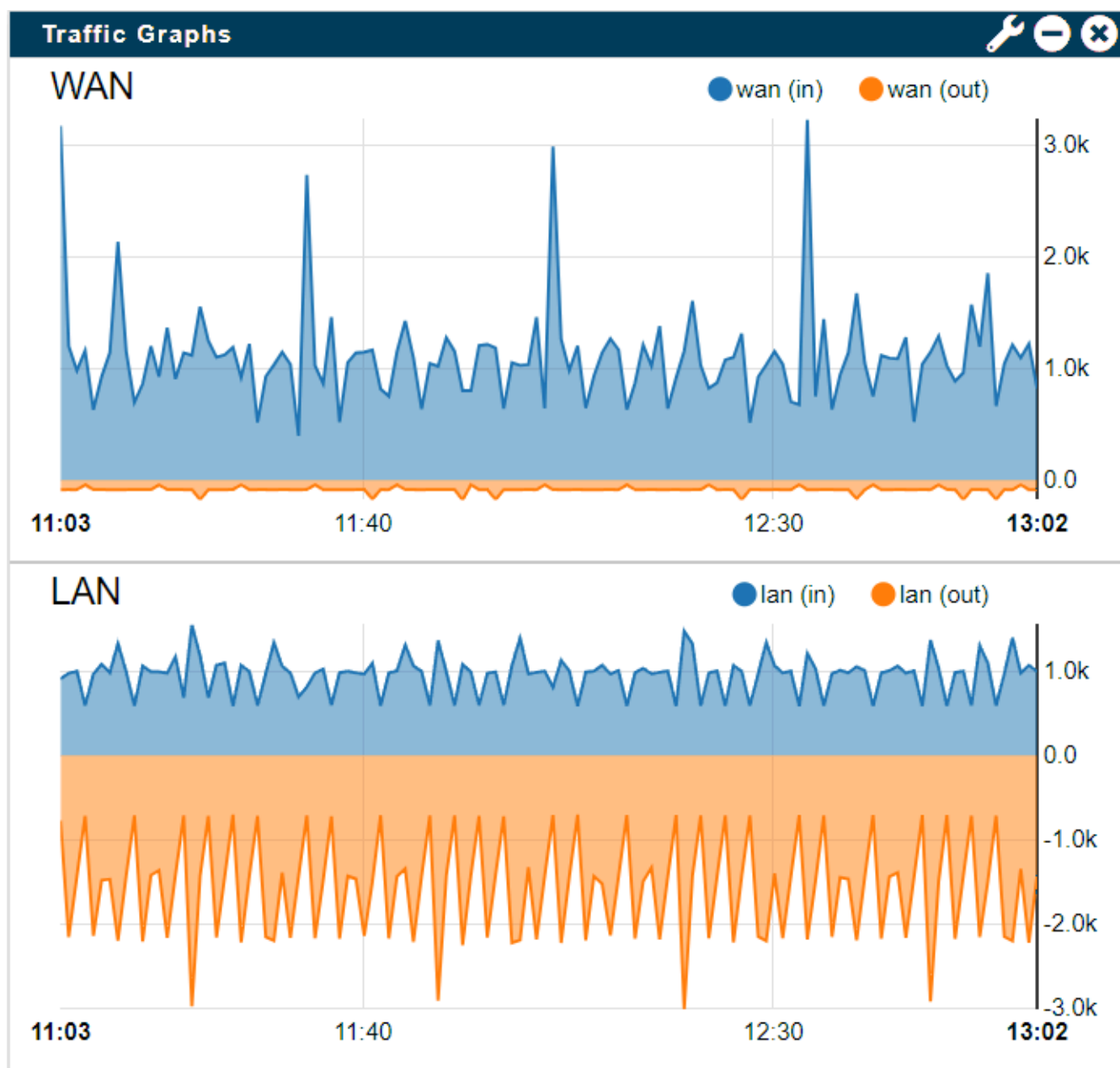
These items can be configured for this widget:

Thresholds in °C (1-100): The **Zone** and **Core** Warning and Critical thresholds can be adjusted here **Display settings:** Options available:

- **Show raw output (no graph):** Only show the temperature values and remove the gauges
- **Show full sensor name:** Show the actual name given for each CPU core instead of the generic **Corex** name
- **Save Button:** Saves the current widget configuration

i As mentioned in the Settings text, the CPU type can be adjusted in the **System>Advanced>Miscellaneous>Thermal Sensors** section of the WebGUI. This should only be needed if older Anybus Defender units are used

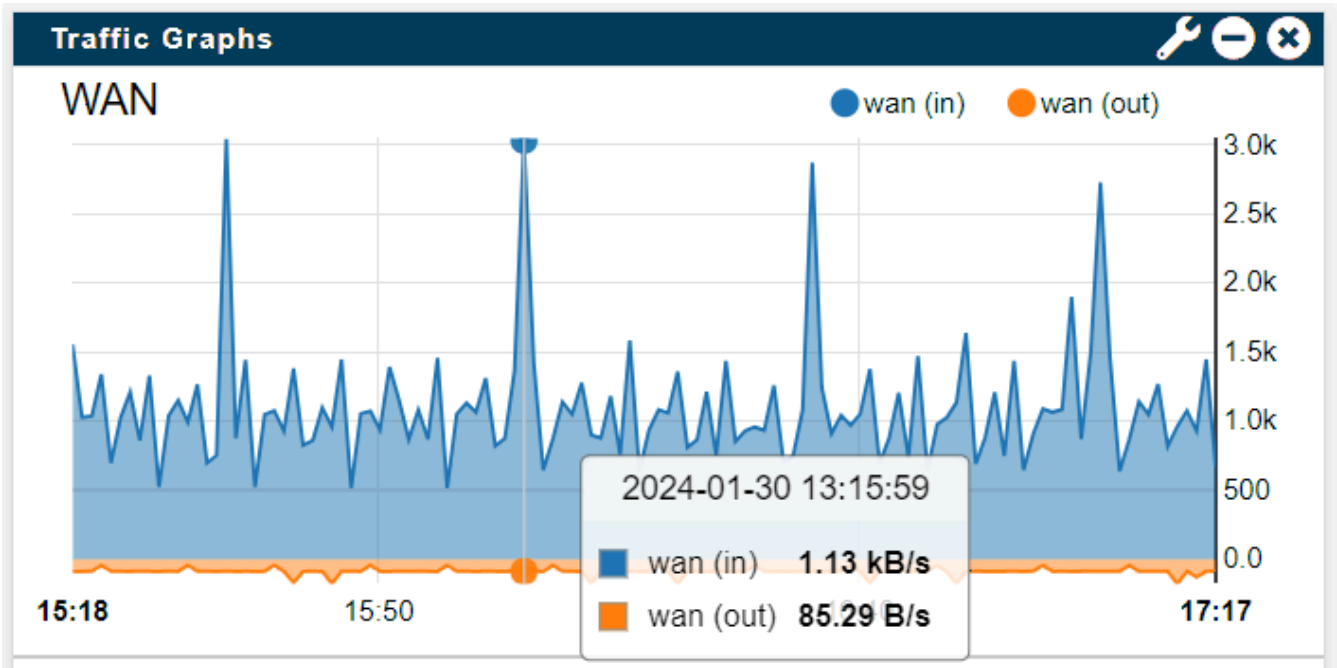
Traffic Graphs



Traffic Graphs Widget

Overview

This widget shows an X/Y chart with the inbound and outbound traffic amount over time. Use your pointer to mouse over sections to see a snapshot of the traffic amount, legend, and datetime stamp:



Traffic Graph Mouse Over



Settings

Refresh Interval	1
Inverse	On
Unit Size	Bytes
Background updates	Keep graphs updated on inactive tab. (increases cpu usage)
Graph Smoothing	<input type="range"/>

Interface	Show
WAN	☒
LAN	☒

Save

None

Thermal Sensors Settings

These items can be configured for this widget:

- **Refresh Interval:** Interval in seconds to refresh the graph readings
- **Inverse:** Toggle On/Off whether to have the inbound and outbound graphics share the same graph area or have WAN and LAN occupy opposite sides, top and bottom, of the graph area
- **Unit Size:** Set whether the units shown on the graph are in **Bits** or **Bytes**
- **Background updates:** Options are:

- **Keep graphs updated on inactive tab:** Keeps updating graph even when inactive. This increases the CPU usage
- **Clear graphs when not visible:** Clears and stops updates to graph when not being shown. This decreases CPU usage when not in use
- **Graph Smoothing:** Adjustable slide to increase/decrease the rounding and "smoothness" of the graph pens
- **Interface:** Allows toggling On/Off each interface graph

Interfaces

Interfaces   			
 WAN		1000baseT <full-duplex>	192.168.70.194
 LAN		100baseTX <full-duplex>	192.168.200.1

Interfaces Widget

Overview

This widget shows all the configured interfaces of the Anybus Defender with this information:

- **Interface Name:** The name of the interface. Clicking on the name will load it [Interface Configuration](#) page
- **Up/Down Indicators:** Up or down arrows indicating if that interfacing is connected
- **Speed and Duplex:** Detected network speed (10/100/1000base T) and if full or half duplex is used
- **IP Address:** The gateway IP address of the interface

Settings

Interface	Show
WAN	☒
LAN	☒

 Save  None

System Information Settings

These items can be configured for this widget:

- **Interface Checkboxes:** Toggle whether each Interface is shown/hidden with the right-hand checkboxes
- **Save Button:** Saves the current widget configuration
- **All/None Button:** Toggles **All** or **None** of the checkboxes explained above

Overview

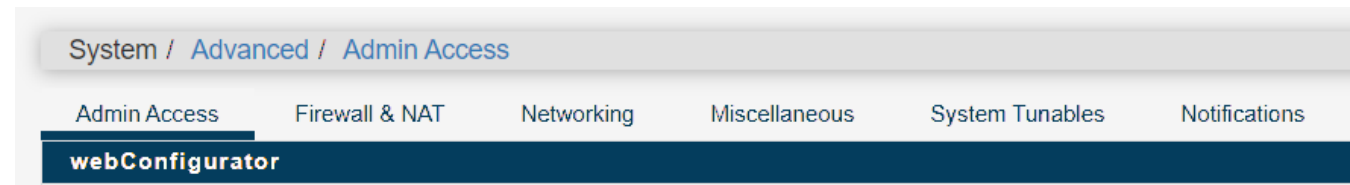
Overview

The advanced settings for the Anybus Defender including:

- [Administrator Access](#)
- [Firewall NAT](#)
- [Networking](#)
- [Miscellaneous](#)
- [System Tunables](#)
- [Notifications](#)

Admin Access

Overview



System / Advanced / Admin Access Page

This page has settings related to administrator access to the Anybus Defender. The **System / Advanced / Admin Access** page is divided into four sections:

WebConfigurator

Admin Access	Firewall & NAT	Networking	Miscellaneous	System Tunables	Notifications
webConfigurator					
Protocol	☐ HTTP ☒ HTTPS (SSL/TLS)				
SSL/TLS Certificate	webConfigurator default (65b0eb1f85376) Certificates known to be incompatible with use for HTTPS are not included in this list.				
TCP port	Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.				
Max Processes	2 Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.				
WebGUI redirect	☐ Disable webConfigurator redirect rule When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.				
HSTS	☐ Disable HTTP Strict Transport Security When this is unchecked, Strict-Transport-Security HTTPS response header is sent by the webConfigurator to the browser. This will force the browser to use only HTTPS for future requests to the firewall FQDN. Check this box to disable HSTS. (NOTE: Browser-specific steps are required for disabling to take effect when the browser already visited the FQDN while HSTS was enabled.)				

WebConfigurator Section of System / Advanced / Admin Access Page

- **Protocol:** Select either **HTTP** or **HTTPS (SSL/TLS)** for the WebGUI access. **HTTPS** is highly recommended for better security
- **SSL/TLS Certificate:** List of SSL/TLS certificates compatible with the Anybus Defender. a webConfigurator certificate is automatically installed when the WebGUI is first accessed
- **TCP port:** A custom TCP port number. This will override the default port number of 80 for HTTP or 443 for HTTPS
- **Max Processes:** Maximum number of simultaneous users allowed to login to the WebGUI
- **WebGUI redirect:** Check to disable redirect of the listening port automatically
- **HSTS:** Check to disable the **HTTP Strict Transport Security** which forces the web browser to use only HTTPS in the URL for access to the Anybus Defender
- **OC SP Must-Staple:** Check to force the **OCSP (Online Certificate Status Protocol)** to be used in **nginx**. This will require uploading the certificate as a full chain or this will be ignored by **nginx**
- **WebGUI Login Autocomplete:** Checking this allows auto-complete from the web browser to work when logging into the WebGUI. Some browsers will not recognize this setting

⚠ Using this option is less secure and may not be allowed based on the company security policies

- **WebGUI login messages:** Check to disable logging of any WebGUI successful logins

- **Anti-lockout:** Check to disable the LAN WebGUI anti-lockout rule. This disables the anti-lockout rule that always allows LAN access to the WebGUI

❗ Disabling this can lock out access to the WebGUI if other firewall rules are not in place allowing access

- **WAN Management Anti-lockout:** Check to disable the WAN WebGUI anti-lockout rule. This disables the anti-lockout rule that always allows WAN access to the WebGUI

❗ Disabling this can lock out access to the WebGUI if other firewall rules are not in place allowing access (or existing LAN anti-lockout are not present)

- **Management Anti-lockout:** Check this to automatically apply anti- lockout rule for ALL interfaces of the Anybus Defender
- **DNS Rebind Check:** Check this to disable protection from DNS rebinding attacks
- **Alternate Hostnames:** Manual entry of alternate hostname(s) for DNS Rebinding and HTTP_REFERER checks. Use spaces between each hostname if more than one is used
- **Browser HTTP_REFERER enforcement:** Check this box to disable the protection against [HTTP_REFERER](#) redirection attempts
- **Browser tab text:** Check this box to show the current WebGUI page followed by the host name instead of the reverse

Secure Shell

Secure Shell	
Secure Shell Server	☐ Enable Secure Shell
SSHD Key Only	Password or Public Key ▼ When set to <i>Public Key Only</i>, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure shell access. If set to <i>Require Both Password and Public Key</i>, the SSH daemon requires both authorized keys and valid passwords to gain access. The default <i>Password or Public Key</i> setting allows either a valid password or a valid authorized key to login.
Allow Agent Forwarding	☐ Enables ssh-agent forwarding support.
SSH port	22 Note: Leave this blank for the default of 22.

Secure Shell Section of System / Advanced / Admin Access Page

- **Secure Shell Server:** Check this box to enable Secure Shell for any extra secure connection requirements
- **SSHD Key Only:** If **Secure Shell** is enabled, use this dropdown to select which authorization types are accepted. Options are:
 - **Password or Public Key:** Either a password or valid key can be used to login
 - **Public Key Only:** Only a valid key can be used to login
 - **Require Both Password and Public Key:** Both a password AND a valid key are required to login
- **Allow Agent Forwarding:** Check this box to enable ssh-agent forwarding support
- **SSH port:** Manual entry of a custom SSH port. Leaving it blank defaults to port 22

Login Protection

Login Protection

Threshold

30

Block attackers when their cumulative attack score exceeds threshold. Most attacks have a score of 10.

Blocktime

120

Block attackers for initially blocktime seconds after exceeding threshold. Subsequent blocks increase by a factor of 1.5. Attacks are unblocked at random intervals, so actual block times will be longer.

Detection time

1800

Remember potential attackers for up to detection_time seconds before resetting their score.

Pass list

Address

/

128

Addresses added to the pass list will bypass login protection.

Add address

+ Add address

Login Protection Section of System / Advanced / Admin Access Page

- **Threshold:** Setting for the threshold when a potential attacker score has met or exceeded this value
- **Blocktime:** Setting in seconds to block a potential attacker after the threshold above has been met or exceeded. Subsequent attacks will increase this time by 1.5
- **Detection time:** Setting for how long in seconds to remember a potential attacker before resetting their score
- **Pass list:** List of IP addresses or hostnames that are allowed to bypass the login protection
- **Add address:** Use the + **Add address** button to add more Pass list addresses to the list

Console Options

Console Options

Console menu

☐ Password protect the console menu

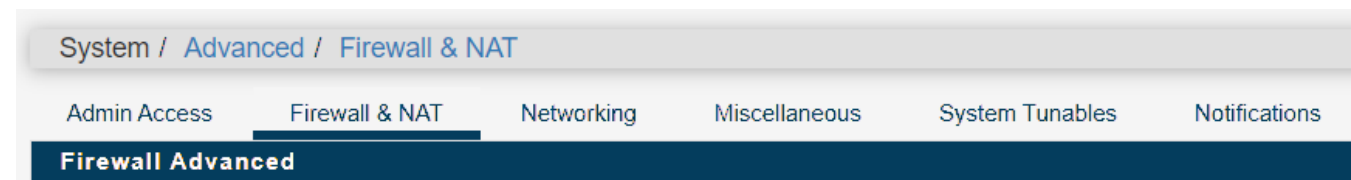
Console Options Section of System / Advanced / Admin Access Page

- **Console Menu** When unchecked, this allows for direct access to the [Console](#) without the need for logging in with an admin-level user. This may be used to prevent completely being locked out of the Anybus Defender

⚠ Disabling this Console password protection can be potentially dangerous to anyone with access to the physical unit

Firewall & NAT

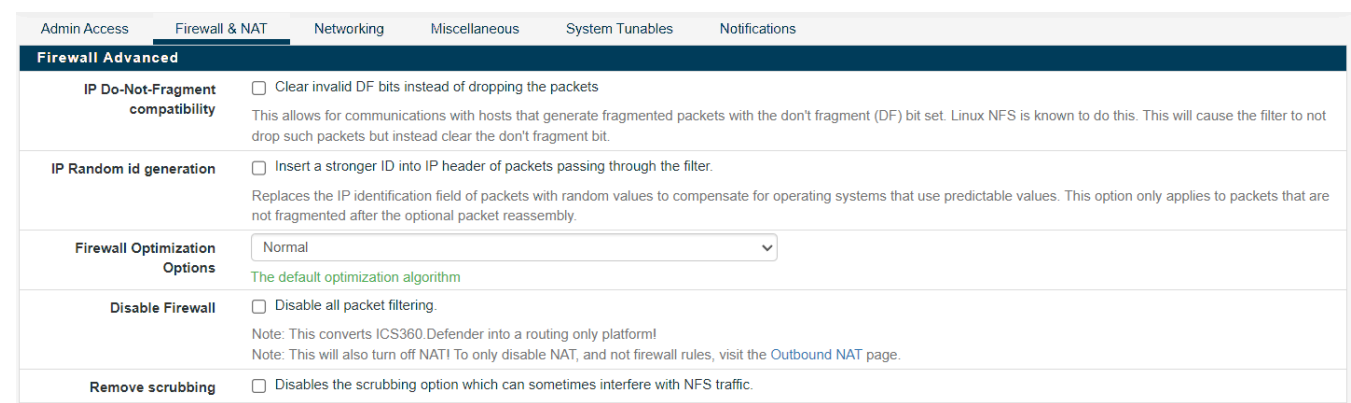
Overview



System / Advanced / Firewall & NAT Page

This page has settings related to the Firewall and NAT of the Anybus Defender. The **System / Advanced / Firewall & NAT** page is divided into four sections:

Firewall Advanced



Firewall Advanced Section of System / Advanced / Firewall & NAT Page

- **IP Do-Not-Fragment compatibility:** Check this box to allow for communications with hosts that generate fragmented packets with the **Don't Fragment (DF)** bit set. Instead of dropping the packets, the DF bit will be cleared instead
- **IP Random id generation:** Check this box to replace IP identification field in packets with random values instead. This setting only applies to packets that are not fragmented
- **Firewall Optimization Options:** Use the dropdown to select these options
 - **Normal:** The standard optimization algorithm, which is optimal for most environments
 - **High-latency:** Used for high-latency links, such as satellite links. Expires idle connections later than default
 - **Aggressive:** Expires idle connections quicker. More efficient use of CPU and memory but can drop legitimate connections earlier than expected. This option can also improve performance in high-traffic deployments with lots of connections, such as web services
 - **Conservative:** Tries to avoid dropping any legitimate connections at the expense of increased memory usage and CPU utilization. Can aid in environments that require long-lived but mostly idle UDP connections
- **Disable Firewall:** Check this to disable any packet filtering by the firewall and the NAT. This essentially turns the Anybus Defender into a switch

⊗ This setting will disable ANY firewall and NAT rules and should only be used for troubleshooting purposes

- **Remove scrubbing:** Check this to disable the scrubbing option which can sometime interfere with **Network File System (NFS)** traffic

- **Firewall Adaptive Timeouts:** Two entries are available for excessive state entries. The setting on the left is the number of state entries before adaptive scaling begins. All timeout values are scaled linearly with factor $(\text{adaptive.end} - \text{number of states}) / (\text{adaptive.end} - \text{adaptive.start})$. Defaults to 60% of the Firewall Maximum States value, The value on the right, when reached, has all timeout values become zero, effectively purging all state entries immediately. This value is used to define the scale factor, it should not actually be reached (set a lower state limit, see below). Defaults to 120% of the Firewall Maximum States value
- **Firewall Maximum States:** Maximum number of connections to hold in the firewall state table
- **Firewall Maximum Table Entries:** Maximum number of table entries for systems such as aliases, sshguard, snort, etc, combined
- **Firewall Maximum Fragment Entries:** Maximum number of packet fragments to hold for reassembly by scrub rules
- **Static route filtering:** Check this box to bypass any firewall checks for any traffic entering and leaving on the same interface. This only applies to static routes defined. This may be desirable in some situations where multiple subnets are connected to the same interface
- **Disable Auto-added VPN rules:** Check this box to disable any automatically-added rules for IPsec
- **Disable reply-to:** Check this box if multiple WANs are used and bridging is also used to disable automatic reply-to messages from the same interface
- **Disable Negate rules:** Check this box if multiple WANs are used to disable traffic from reaching directly connected devices and VPN networks when using policy routing
- **Allow APIPA:** This allows **Automatic Private IP Addressing (APIPA)** traffic to pass but can not be routed
- **Aliases Hostnames Resolves Interval:** The interval, in seconds, that will be used to resolve hostnames configured on aliases. Leaving this blank defaults to 300s
- **Check certificate of aliases URLs:** Check this box to be sure the certificate is valid for all HTTPS addresses on aliases. If it is invalid or revoked, it will not be downloaded

Bogon Networks

Bogon Networks	
Update Frequency	Monthly
The frequency of updating the lists of IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA.	

Bogon Network of System / Advanced / Firewall & NAT Page

This checks for bogons or bogus IP addresses of a computer network. Bogons include IP packets on the public internet that contain addresses that are not in any range allocated or delegated by the **Internet Assigned Numbers Authority (IANA)** or a delegated **Regional Internet Registry (RIR)** and allowed for public internet use

- **Update Frequency** Use this dropdown to update the bogon list, either monthly, weekly, or daily

Network Address Translation

Network Address Translation	
NAT Reflection mode for port forwards	disabled - The pure NAT mode uses a set of NAT rules to direct packets to the target of the port forward. It has better scalability, but it must be possible to accurately determine the interface and gateway IP used for communication with the target at the time the rules are loaded. There are no inherent limits to the number of ports other than the limits of the protocols. All protocols available for port forwards are supported. - The NAT + proxy mode uses a helper program to send packets to the target of the port forward. It is useful in setups where the interface and/or gateway IP used for communication with the target cannot be accurately determined at the time the rules are loaded. Reflection rules are not created for ranges larger than 500 ports and will not be used for more than 1000 ports total between all port forwards. Only TCP and UDP protocols are supported. Individual rules may be configured to override this system setting on a per-rule basis.
Reflection Timeout	Enter value for Reflection timeout in seconds. Note: Only applies to Reflection on port forwards in NAT + proxy mode.
Enable NAT Reflection for 1:1 NAT	☐ Automatic creation of additional NAT redirect rules from within the internal networks. Note: Reflection on 1:1 mappings is only for the inbound component of the 1:1 mappings. This functions the same as the pure NAT mode for port forwards. For more details, refer to the pure NAT mode description above. Individual rules may be configured to override this system setting on a per-rule basis.
Enable automatic outbound NAT for Reflection	☐ Automatic create outbound NAT rules that direct traffic back out to the same subnet it originated from. Required for full functionality of the pure NAT mode of NAT Reflection for port forwards or NAT Reflection for 1:1 NAT. Note: This only works for assigned interfaces. Other interfaces require manually creating the outbound NAT rules that direct the reply packets back through the router.
TFTP Proxy	WAN LAN Choose the interfaces on which to enable TFTP proxy helper.

Network Address Translation Section of System / Advanced / Admin Access Page

- NAT Reflection mode for port forwards:** Dropdown selector to choose from these options:
 - disabled:** No reflection done
 - NAT + proxy:** Uses a helper program to send packets to the target of the port forward. It is useful in setups where the interface and/or gateway IP used for communication with the target cannot be accurately determined at the time the rules are loaded. Reflection rules are not created for ranges larger than 500 ports and will not be used for more than 1000 ports total between all port forwards. Only TCP and UDP protocols are supported
 - Pure NAT:** Uses a helper program to send packets to the target of the port forward. It is useful in setups where the interface and/or gateway IP used for communication with the target cannot be accurately determined at the time the rules are loaded. Reflection rules are not created for ranges larger than 500 ports and will not be used for more than 1000 ports total between all port forwards. Only TCP and UDP protocols are supported

i Individual rules may be configured to override this system setting on a per-rule basis

- Reflection Timeout:** Enter a time in seconds for reflection timeout

i Only applies to Reflection on port forwards in **NAT + proxy** mode as explained above

- Enable NAT Reflection for 1:1 NAT:** Check this box for **Automatic creation of additional NAT redirect rules from within the internal networks**

i Reflection on 1:1 mappings is only for the inbound component of the 1:1 mappings. This functions the same as the pure NAT mode for port forwards. For more details, refer to the pure NAT mode description above. Individual rules may be configured to override this system setting on a per-rule basis

- Enable automatic outbound NAT for Reflection:** Check is box for **Automatic creation of outbound NAT rules that direct traffic back out to the same subnet it originated from.** Required for full functionality of the pure NAT mode of NAT Reflection for port forwards or NAT Reflection for 1:1 NAT

i This only works for assigned interfaces. Other interfaces require manually creating the outbound NAT rules that direct the reply packets back through the router

- TF TP Proxy:** Selector to choose which interface(s) will have **Trivial File Transfer Protocol (TFTP)** proxy helpers enabled

State Timeouts (seconds - blank for default)

State Timeouts (seconds - blank for default)	
TCP First	120
TCP Opening	30
TCP Established	86400
TCP Closing	900
TCP FIN Wait	45
TCP Closed	30
TCP Tsdiff	30
UDP First	60
UDP Single	30
UDP Multiple	60
ICMP First	20
ICMP Error	10
Other First	60
Other Single	30
Other Multiple	60

State Timeouts Section of System / Advanced / Admin Access Page

- **TCP First:** The first packet of a TCP connection
- **TCP Opening:** The state before the destination host has replied
- **TCP Established:** An established TCP connection where the three-way handshake has been completed
- **TCP Closing:** One side has sent a TCP FIN packet
- **TCP FIN Wait:** Both sides have exchanged FIN packets and the connection is shutting down. Some servers may continue to send packets during this time
- **TCP Closed:** One side has sent a connection reset (TCP RST) packet
- **TCP Tsdiff:** The allowed TCP timestamp difference
- **UDP First:** The first UDP packet of a connection has been received
- **UDP Single:** The source host has sent a single packet but the destination has not replied
- **UDP Multiple:** Both sides have sent packets
- **ICMP First:** An ICMP packet has been received
- **ICMP Error:** An ICMP error was received in response to an ICMP packet
- **Other First, Single, Multiple:** Same as UDP above but for other protocols

Networking

Overview

System / [Advanced](#) / [Networking](#)

[Admin Access](#)[Firewall & NAT](#)[Networking](#)[Miscellaneous](#)[System Tunables](#)[Notifications](#)

IPv6 Options

System / Advanced / Networking Page

This page has settings related to networking of the Anybus Defender. The **System / Advanced / Networking** page is divided into two sections:

IPv6 Options

IPv6 Options

Allow IPv6

☐ All IPv6 traffic will be blocked by the firewall unless this box is checked

NOTE: This does not disable any IPv6 features on the firewall, it only blocks traffic.

IPv6 over IPv4 Tunneling

☐ Enable IPv6 over IPv4 tunneling

These options create an RFC 2893 compatible mechanism for IPv4 NAT encapsulation of IPv6 packets, that can be used to tunnel IPv6 packets over IPv4 routing infrastructures. IPv6 firewall rules are [also required](#), to control and pass encapsulated traffic.

Prefer IPv4 over IPv6

☒ Prefer to use IPv4 even if IPv6 is available

By default, if IPv6 is configured and a hostname resolves IPv6 and IPv4 addresses, IPv6 will be used. If this option is selected, IPv4 will be preferred over IPv6.

IPv6 DNS entry

☐ Do not generate local IPv6 DNS entries for LAN interfaces

If a LAN interface's IPv6 configuration is set to Track, and the tracked interface loses connectivity, it can cause connections to this firewall that were established via hostname to fail. This can happen unintentionally when accessing the firewall by hostname, since by default both IPv4 and IPv6 entries are added to the system's DNS. Enabling this option prevents those IPv6 records from being created.

DHCP6 DUID

Raw DUID: As stored in DUID file or seen in firewall logs

A DHCPv6 Unique Identifier (DUID) is used by the firewall when requesting an IPv6 address.

By default, the firewall automatically creates a dynamic DUID-LLT which is not saved in the firewall configuration. To ensure that the same DUID is retained by the firewall at all times, enter a DUID in this section. The new DUID will take effect after a reboot or when the WAN interface(s) are reconfigured by the firewall.

If the firewall is configured to use a RAM disk for /var, the best practice is to store a DUID here; otherwise, the DUID will change on each reboot.

Raw DUID

Copy DUID

You may use the Copy DUID button to copy the system detected DUID shown in the placeholder.

Firewall Advanced Section of System / Advanced / Firewall & NAT Page

- Allow IPv6:** Check this box to allow IPv6 traffic through the firewall

This does not disable any IPv6 features on the firewall, it only blocks traffic
- IPv6 over IPv4 Tunneling:** Check this box to enable IPv6 over IPv4 tunneling. These options create an RFC 2893 compatible mechanism for IPv4 NAT encapsulation of IPv6 packets, that can be used to tunnel IPv6 packets over IPv4 routing infrastructures. IPv6 firewall rules are also required, to control and pass encapsulated traffic
- Prefer IPv4 over IPv6:** Check this box to always resolve to IPv4 if both IPv6 and IPv4 hostnames can be resolved
- IPv6 DNS entry:** Check this box to not generate local IPv6 DNS entries for LAN interfaces. If a LAN interface's IPv6 configuration is set to Track, and the tracked interface loses connectivity, it can cause connections to this firewall that were established via hostname to fail. This can happen unintentionally when accessing the firewall by hostname, since by default both IPv4 and IPv6 entries are added to the system's DNS. Enabling this option prevents those IPv6 records from being created

- **DHCP6 DUID:** Dropdown to select which DHCPv6 Unique Identifier (DUID) method to use (this is used by the firewall when requesting IPv6 addresses). Options are:
 - **Raw DUID:** As stored in DUID file or seen in firewall logs. Use the **Raw DUID** area below this dropdown to enter a DUID
 - **DUID-LLT:** Based on Link-layer Address Plus Time. Use the **DUID-LLT** entries below this dropdown to enter the **Time** and **Link-layer address**
 - **DUID-EN:** Assigned by Vendor based on Enterprise Number. Use the **DUID-EN** entries below this dropdown to enter the **IANA Private Enterprise Number** and **Identifier**
 - **DUID-LL:** Based on Link-layer only. Use the **DUID-LL** entry below this dropdown to enter the **Link-layer address**
 - **DUID-UUID:** Based on Universally Unique Identifier. Use the **DUID-UUID** entry below this dropdown to enter the **Universally Unique Identifier**

❗ By default, the firewall automatically creates a dynamic DUID-LLT which is not saved in the firewall configuration. To ensure that the same DUID is retained by the firewall at all times, enter a DUID in this section. The new DUID will take effect after a reboot or when the WAN interface(s) are reconfigured by the firewall. If the firewall is configured to use a RAM disk for /var, the best practice is to store a DUID here; otherwise, the DUID will change on each reboot

Network Interfaces

Network Interfaces	
Hardware Checksum Offloading	☐ Disable hardware checksum offload Checking this option will disable hardware checksum offloading. Checksum offloading is broken in some hardware, particularly some Realtek cards. Rarely, drivers may have problems with checksum offloading and some specific NICs. This will take effect after a machine reboot or re-configure of each interface.
Hardware TCP Segmentation Offloading	☒ Disable hardware TCP segmentation offload Checking this option will disable hardware TCP segmentation offloading (TSO, TSO4, TSO6). This offloading is broken in some hardware drivers, and may impact performance with some specific NICs. This will take effect after a machine reboot or re-configure of each interface.
Hardware Large Receive Offloading	☒ Disable hardware large receive offload Checking this option will disable hardware large receive offloading (LRO). This offloading is broken in some hardware drivers, and may impact performance with some specific NICs. This will take effect after a machine reboot or re-configure of each interface.
hn ALTQ support	☒ Enable the ALTQ support for hn NICs. Checking this option will enable the ALTQ support for hn NICs. The ALTQ support disables the multiqueue API and may reduce the system capability to handle traffic. This will take effect after a machine reboot.
ARP Handling	☐ Suppress ARP messages This option will suppress ARP log messages when multiple interfaces reside on the same broadcast domain.
Reset All States	☐ Reset all states if WAN IP Address changes This option resets all states when a WAN IP Address changes instead of only states associated with the previous IP Address.

Network Interfaces of System / Advanced / Firewall & NAT Page

- **Hardware Checksum Offloading** Check this box to disable hardware checksum offloading.

❗ Checksum offloading is broken in some hardware, particularly some Realtek cards. Rarely, drivers may have problems with checksum offloading and some specific NICs. This will take effect after a machine reboot or re-configure of each interface

- **Hardware TCP Segmentation Offloading:** Check this box to disable hardware TCP segmentation offloading (TSO, TSO4, TSO6)

❗ This offloading is broken in some hardware drivers, and may impact performance with some specific NICs. This will take effect after a machine reboot or re-configure of each interface

- **Hardware Large Receive Offloading:** check this box to disable hardware large receive offloading (LRO)

❗ This offloading is broken in some hardware drivers, and may impact performance with some specific NICs. This will take effect after a machine reboot or re-configure of each interface

- **hn ALTQ support:** Checking this option will enable the ALTQ support for hn NICs

❗ The ALTQ support disables the multiqueue API and may reduce the system capability to handle traffic. This will take effect after a machine reboot

- **ARP Handling:** Check this box to suppress ARP messages when multiple interfaces reside on the same broadcast domain
- **Reset All States:** Check this box to resets all states when a WAN IP Address changes instead of only states associated with the previous IP Address

Miscellaneous

Overview

System / [Advanced](#) / [Miscellaneous](#)

Admin AccessFirewall & NATNetworkingMiscellaneousSystem TunablesNotifications

Proxy Support

System / Advanced / Miscellaneous Page

This page has settings related to miscellaneous settings of the Anybus Defender. The **System / Advanced / Miscellaneous** page is divided into six sections:

Proxy Support

Admin AccessFirewall & NATNetworkingMiscellaneousSystem TunablesNotifications

Proxy Support

Proxy URL

Hostname or IP address of proxy server this system will use for its outbound Internet access.

Proxy Port

Port where proxy server is listening.

Proxy Username

Username for authentication to proxy server. Optional, leave blank to not use authentication.

Proxy Password

Confirm

Proxy Support Section of System / Advanced / Miscellaneous Page

- **Proxy URL:** Enter the Hostname or IP address of proxy server this system will use for its outbound Internet access
- **Proxy Port:** Enter the port where proxy server is listening
- **Proxy Username:** Enter the Username for authentication to proxy server

Leaving this blank will disable any authentication

- **Proxy Password:** Enter a password and confirmation of the same password in the appropriate boxes for proxy server authentication login

Cryptographic & Thermal Hardware

Cryptographic & Thermal Hardware

Cryptographic Hardware

AES-NI CPU-based Acceleration

A cryptographic accelerator module will use hardware support to speed up some cryptographic functions on systems which have the chip. Loading the BSD Crypto Device module will allow access to acceleration devices using drivers built into the kernel, such as Hifn or ubsec chipsets. If the firewall does not contain a crypto chip, this option will have no effect. To unload the selected module, set this option to "none" and then reboot.

Thermal Sensors

Intel Core® CPU on-die thermal sensor

With a supported CPU, selecting a thermal sensor will load the appropriate driver to read its temperature. Setting this to "None" will attempt to read the temperature from an ACPI-compliant motherboard sensor instead, if one is present. If there is not a supported thermal sensor chip in the system, this option will have no effect. To unload the selected module, set this option to "none" and then reboot.

Cryptographic & Thermal Hardware Section of System / Advanced / Miscellaneous Page

- **Cryptographic Hardware:** Use this dropdown to select the cryptographic acceleration type to be used. Options are:

- **None:** No hard acceleration will be used
- **AES-NI CPU-based Acceleration:** A CPU-based hardware acceleration for compatible hardware
- **BSD Crypto Device (crptodev):** Allows access to acceleration devices using drivers built into the kernel, such as **Hifn** or **ubsec** chipsets

❗ Any change of these options will require a device reboot

- **Thermal Sensors:** Use this dropdown to select the proper thermal sensors depending on the CPU type used.

Options are:

- **None/ACPI:** attempts to read the temperature from an ACPI-compliant motherboard sensor instead, if one is present
- **Intel Core CPU on-die thermal sensor**
- **AMD K8, K10, and K11 CPU on-die thermal sensor**

❗ Most new Anybus Defender units use the Intel-based thermal sensors. Older units may use the AMD-type thermal sensors. To verify which setting to use, check the CPU Type from the [Dashboard System Information Page](#)

Kernel Page Table Isolation

Kernel Page Table Isolation	
Kernel PTI	☐ Forcefully disable the kernel PTI Meltdown workaround. If disabled the kernel memory can be accessed by unprivileged users on affected CPUs. This option forces the workaround off, and requires a reboot to activate. PTI is active by default only on affected CPUs, if PTI is disabled by default then this option will have no effect. Current PTI status: Enabled

Kernel Page Table Isolation Section of System / Advanced / Miscellaneous Page

- **Kernel PTI:** Check this to forcefully disable the kernel page-table isolation (PTI). This setting protects against the [Meltdown Vulnerability](#) of some CPU types. If disabled the kernel memory can be accessed by unprivileged users on affected CPUs. This option forces the workaround off, and requires a reboot to activate. PTI is active by default only on affected CPUs. If PTI is disabled by default then this option will have no effect

Microarchitectural Data Sampling Mitigation

Microarchitectural Data Sampling Mitigation	
MDS Mode	Mitigation disabled Microarchitectural Data Sampling mitigation. If disabled the kernel memory can be accessed by unprivileged users on affected CPUs. This option controls which method of MDS mitigation is used, if any. Current MDS status: Inactive

Microarchitectural Data Sampling Mitigation Section of System / Advanced / Miscellaneous Page

- **MDS Mode:** Use the dropdown to select which MDS mode is used. Options are:
 - **Default:**
 - **Mitigation disabled:** kernel memory can be accessed by unprivileged users on affected CPUs
 - **VERW instruction (microcode) mitigation enabled:**
 - **Software sequence mitigation enabled:**

❗ This setting is not recommended

- **Automatic VERW or Software selection:**

Schedules

Schedules	
Schedule States	☐ Do not kill connections when schedule expires
By default, when a schedule expires, connections permitted by that schedule are killed. This option overrides that behavior by not clearing states for existing connections.	

Schedules Section of System / Advanced / Miscellaneous Page

- Schedule States:** Check this box to kill connections when the schedule states expire. By default, when a schedule expires, connections permitted by that schedule are killed. This option overrides that behavior by not clearing states for existing connections

Gateway Monitoring

Gateway Monitoring	
State Killing on Gateway Failure	☐ Flush all states when a gateway goes down
The monitoring process will flush all states when a gateway goes down if this box is checked.	
Skip rules when gateway is down	☐ Do not create rules when gateway is down
By default, when a rule has a gateway specified and this gateway is down, the rule is created omitting the gateway. This option overrides that behavior by omitting the entire rule instead.	

Gateway Monitoring of System / Advanced / Miscellaneous Page

- State Killing on Gateway Failure:** Check this box to flush all states when a gateway goes down
- Skip rules when gateway is down:** Check this box to prevent any rule creation when a gateway is down. By default, when a rule has a gateway specified and this gateway is down, the rule is created omitting the gateway. This option overrides that behavior by omitting the entire rule instead

System Tunables

Overview

System / [Advanced](#) / [System Tunables](#)

Admin AccessFirewall & NATNetworkingMiscellaneousSystem TunablesNotifications

System Tunables

NOTE: The options on this page are intended for use by advanced users only.

Tunable Name	Description	Value	+ New
net.inet.ip.portrange.first		1024	
net.inet.tcp.blackhole	Do not send RST on segments to closed ports	2	
net.inet.udp.blackhole	Do not send port unreachable for refused connects	1	
net.inet.ip.random_id	Assign random ip_id values	1	
net.inet.tcp.drop_synfin	Drop TCP packets with SYN+FIN set	1	
net.inet.ip.redirect	Enable sending IP redirects	1	
net.inet6.ip6.redirect	Send ICMPv6 redirects for unforwardable IPv6 packets	1	
net.inet6.ip6.use_tempaddr	Create RFC3041 temporary addresses for autoconfigured addresses	0	
net.inet6.ip6.dad_enhanced	Enable Enhanced DAD, which adds a random nonce to NS messages for DAD.	0	
net.inet6.ip6.prefer_tempaddr	Prefer RFC3041 temporary addresses in source address selection	0	
net.inet.tcp.syncookies	Use TCP SYN cookies if the syncache overflows	1	
net.inet.tcp.recvspace	Initial receive socket buffer size	65228	
net.inet.tcp.sendspace	Initial send socket buffer size	65228	
net.inet.tcp.delayed_ack	Delay ACK to try and piggyback it onto a data packet	0	

System / Advanced / System Tunables Page

This page has settings only used for very advanced users or from the support team at HMS

⊗ These settings should only be altered by a qualified person. For any questions about these settings, contact info@hms-networks.com

Notifications

Overview

System / Advanced / Notifications

Admin AccessFirewall & NATNetworkingMiscellaneousSystem TunablesNotifications

General Settings

System / Advanced / Notifications

This page has settings related to all of the notification settings of the Anybus Defender. The **System / Advanced / Notifications** page is divided into five sections:

General Settings

General Settings

Certificate Expiration	☒ Enable daily notifications of expired and soon-to-expire certificates When enabled, the firewall will check CA and Certificate expiration times daily and file notices when expired or soon-to-expire entries are detected.
Certificate Expiration Threshold	27 The number of days at which a certificate lifetime is considered to be expiring soon and worthy of notification. Default is 27 days.

General Settings Section of System / Advanced / Miscellaneous Page

- **Certificate Expiration:** Check this box to enable daily notifications of expired or soon-to-expire certificates
- **Certificate Expiration Threshold:** The number of days at which a certificate lifetime is considered to be expiring soon and worthy of notification. The default is 27 days

Email

E-Mail

Disable SMTP	☐ Disable SMTP Notifications Check this option to disable SMTP notifications but preserve the settings below. Some other mechanisms, such as packages, may need these settings in place to function.
E-Mail server	 This is the FQDN or IP address of the SMTP E-Mail server to which notifications will be sent.
SMTP Port of E-Mail server	 This is the port of the SMTP E-Mail server, typically 25, 587 (submission) or 465 (smtps).
Connection timeout to E-Mail server	 This is how many seconds it will wait for the SMTP server to connect. Default is 20s.
Secure SMTP Connection	☐ Enable SMTP over SSL/TLS
Validate SSL/TLS	☒ Validate the SSL/TLS certificate presented by the server When disabled, the server certificate will not be validated. Encryption will still be used if available, but the identity of the server will not be confirmed.
From e-mail address	 This is the e-mail address that will appear in the from field

Email Section of System / Advanced / Notifications Page

- **Disable SMTP:** Check this box to disable SMTP notifications but preserve the settings below
- **E-mail server:** Enter the FQDN or IP address of the SMTP E-Mail server to which notifications will be sent
- **SMTP Port of E-Mail server:** Enter the port of the SMTP E-Mail server, typically 25, 587 (submission) or 465 (smtps)
- **Connection timeout to E-Mail server:** Enter how many seconds it will wait for the SMTP server to connect. Default is 20s
- **Secure SMTP Connection:** Check this box to use the secure SMTP over SSL/TLS

- **Validate SSL/TLS:** Check this box to always validate the SSL/TLS certificate presented by the server
- **From e-mail address:** The e-mail address that will appear in the **From** field
- **Notification E-Mail address:** The e-mail address to send email notifications to
- **Notification E-Mail auth password:** The e-mail account password and confirmation entries for SMTP authentication
- **Notification E-Mail auth mechanism:** use the dropdown to select the authentication mechanism used by the SMTP server. Options are:
 - **PLAIN:** OK for most SMTP servers
 - **LOGIN:** May be required for some Exchange or Office365 accounts
- **Test SMTP Settings:** Use the **Test SMTP Settings** to send a test notification

i The last SAVED values will be used for the test notification, not necessarily the values entered here

Sounds

Sounds	
Startup/Shutdown Sound	☐ Disable the startup/shutdown beep When this is checked, startup and shutdown sounds will no longer play.

Sounds Section of System / Advanced / Miscellaneous Page

- **Startup/Shutdown Sound"** Check this box to prevent the startup and shutdown sounds from playing

Telegram

Telegram	
Enable Telegram	☐ Enable Telegram Notifications Check this option to enable Telegram notifications. You will need a Telegram Bot and its associated API key. Instructions here.
API Key	123456789:ABCDEabcde_FGHIJfghijKLMNOklmnoPQRST Enter the Bot API key required to authenticate with the Telegram API server.
Chat ID	123456789 Enter the chat ID number (private) or channel @username (public) that will be used to send the notifications to.
Test Telegram Settings	Test Telegram Settings A test notification will be sent even if the service is not enabled. The last SAVED values will be used, not necessarily the values displayed here.

Telegram Section of System / Advanced / Miscellaneous Page

- **Enable Telegram:** Check this box to enable Telegram notifications

i A [Telegram Bot and its associated API key](#) are needed

- **API Key:** Enter the Bot API key required to authenticate with the Telegram API server
- **Chat ID:** Enter the chat ID number (private) or channel @username (public) that will be used to send the notifications to
- **Test Telegram Settings:** Use the **Test Telegram Settings** button to send a test notification even if the service is not enabled

i The last SAVED values will be used for the test notification, not necessarily the values entered here

Pushover

Pushover	
Enable Pushover	☐ Enable Pushover Notifications Check this option to enable Pushover notifications. An API key will need to be created and entered along with the Pushover account user key. API documentation.
API Key	azGDORePK8gMaC0QOYAMyEEuzJnyUi Enter the API key required to authenticate with the Pushover API server. Create API key here.
User Key	uQIRzpo4DXghDmr9QzzfQu27cmVRsG Enter user key of the Pushover account
Notification Sound	Device Default Select notification sound. Notification Sound documentation with audio.
Message Priority	Normal Priority Select message priority. Message Priority documentation.
Emergency Priority Notification Retry Interval	60 This specifies how often (in seconds) the Pushover servers will send the same notification for Emergency Priority notifications until the notification is acknowledged. This parameter must have a value of at least 30 seconds between retries. Default is 1 minute.
Emergency Priority Notification Expiration	300 This specifies how many seconds the notifications will continue to be retried (every retry seconds) for Emergency Priority notifications until the notification is acknowledged. This parameter must have a maximum value of at most 10800 seconds (3 hours). Default is 5 minutes.
Test Pushover Settings	Test Pushover Settings A test notification will be sent even if the service is not enabled. The last SAVED values will be used, not necessarily the values displayed here.

Pushover Section of System / Advanced / Miscellaneous Page

- **Enable Pushover:** Check this option to enable Pushover notifications

An API key will need to be created and entered along with the Pushover account user key. [API Documentation](#)

- **API Key:** Enter the API key required to authenticate with the Pushover API server

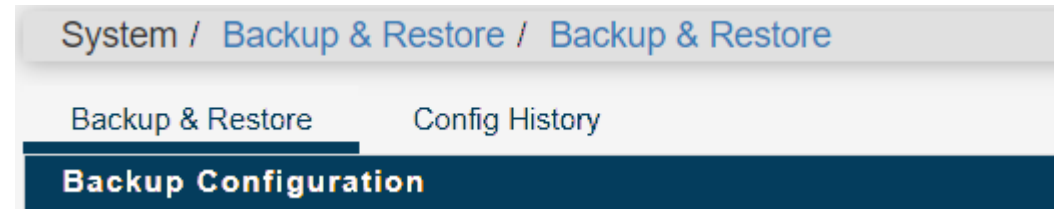
An [API Key](#) is required for this

- **User Key:** Enter the user key of the Pushover account
- **Notification Sound:** Use the dropdown to select a [Notification Sound](#)
- **Message Priority:** Use the dropdown to select the [Message Priority](#)
- **Emergency Priority Notification Retry Interval:** Specifies how often (in seconds) the Pushover servers will send the same notification for Emergency Priority notifications until the notification is acknowledged. This parameter must have a value of at least 30 seconds between retries. The default is 1 minute
- **Emergency Priority Notification Expiration:** Specifies how many seconds the notifications will continue to be retried (every retry seconds) for Emergency Priority notifications until the notification is acknowledged. This parameter must have a maximum value of at most 10800 seconds (3 hours). The default is 5 minutes
- **Test Pushover Settings:** Use the **Test Pushover Settings** button to send a test notification even if the service is not enabled

The last SAVED values will be used for the test notification, not necessarily the values entered here

Backup & Restore

Overview



System / Backup & Restore / Backup & Restore Page

The section shows how an Anybus Defender can have its configuration backed up to an external destination or restored from an external source

The **System / Backup & Restore/ Config History** page is divided into three sections:

Backup Configuration

Backup Configuration	
Backup area	All
Skip packages	☐ Do not backup package information.
Skip RRD data	☒ Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)
Include extra data	☐ Backup extra data. Backup extra data files for some services.
Encryption	☐ Encrypt this configuration file.
Download configuration as XML Save configuration to USB Format & Save configuration to USB	

Backup Configuration Section of System / Backup & Restore/ Backup & Restore Page

- **Backup area:** Which area of the Anybus Defender to include in the backup

When All is selected, it is still possible to restore a section of the backup in the **Restore area** explained below

- **Skip packages:** Check this box to exclude any package information
- **Skip RRD data:** Check this box to skip backing up any Round Robin Data (RRD)

RRD Data can consume 4+ megabytes of config.xml space

- **Include extra data:** Check this box to include extra data for some of the services in use like Captive portal or DHCP
- **Encryption:** Encrypt the backup file to be unreadable when opened in a text editor
- **Download configuration as XML:** Click this button to download an XML backup file to a desired location
- **Save configuration to USB:** Click the button to store an XML backup file to an external drive plugged into the USB port of the Anybus Defender
- **Format & Save configuration to USB:** Click this button to format the external USB storage device, then save the backup XML file to that drive

Using this option will erase any existing data on the external drive

Restore Backup

Restore Backup

Open a Anybus Defender configuration XML file and click the button below to restore the configuration.

Restore area

All

Configuration file

Choose File

No file chosen

Encryption

☐ Configuration file is encrypted.

Restore Configuration

The firewall will reboot after restoring the configuration.

Restore Backup Section of System / Backup & Restore/ Backup & Restore Page

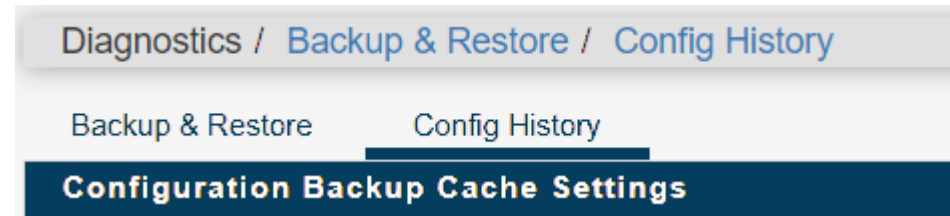
- Restore area:** Select the Area(s) of an Anybus Defender backup to restore to the current unit
- i** If **All** was selected for the backup, it is still possible to restore a section of the backup in the **Restore area** by just selecting the appropriate item
- Configuration File:** Use the **Choose File** button to select the file to be restored
 - Encryption:** If the back was done with encryption, this needs to be selected for the restore operation to work
 - Restore Configuration:** Click this button to restore the loaded configuration file to the Anybus Defender
- i** After the restore operation is complete, the unit will be rebooted

Package Functions

- Reinstall Packages:** Click this button to reinstall all system packages
- i** This may take a significant period of time

Config History

Overview



System / Backup & Restore / Config History Page

The section shows a list of the last 20 automated backups on the Anybus Defender. These backups are done any time a configuration change is applied or saved. The list allows for several operations to inspect, revert, and delete previous automated backups

Configuration Backup Cache Settings

To view the differences between an older configuration and a newer configuration, select the older configuration using the left column of radio options and select the newer configuration in the right column, then press the "Diff" button.

Diff	Date	Version	Size	Configuration Change	Actions
☐	2/12/24 10:01:36	21.7	29 KiB	admin@192.168.200.222 (Local Database): User Manager Settings saved	Current configuration
☐	1/30/24 14:09:06	21.7	29 KiB	admin@192.168.200.222 (Local Database): Widget configuration has been changed.	
☐	1/30/24 14:09:03	21.7	29 KiB	admin@192.168.200.222 (Local Database): Updated traffic graphs widget settings via dashboard.	
☐	1/30/24 14:08:58	21.7	29 KiB	admin@192.168.200.222 (Local Database): Updated traffic graphs widget settings via dashboard.	
☐	1/30/24 14:08:12	21.7	29 KiB	admin@192.168.200.222 (Local Database): Updated traffic graphs widget settings via dashboard.	
☐	1/30/24 14:07:16	21.7	29 KiB	admin@192.168.200.222 (Local Database): Updated traffic graphs widget settings via dashboard.	
☐	1/30/24 14:06:53	21.7	29 KiB	admin@192.168.200.222 (Local Database): Updated traffic graphs widget settings via dashboard.	

Differences Table Section of System / Backup & Restore/ Config History Page

This table allows several operations to be performed with current and previous backups:

- Diff

button: use the radio buttons below this button to select any 2 backups from the list. When this button is clicked, a list of all changes performed will be shown on an embedded XML viewer:

Backup & Restore	Config History
Configuration Diff from 1/30/24 14:00:31 to 2/12/24 10:01:36	
--- /conf/backup/config-1706641231.xml	2024-01-30 14:03:02.425833000 -0500
+++ /conf/config.xml	2024-02-12 10:01:36.462030000 -0500
@@ -41,6 +41,8 @@	
<pre> <max_procs>2</max_procs> <loginautocomplete bool="true"/> <dashboardcolumns>2</dashboardcolumns> + <session_timeout>0</session_timeout> + <authmode>Local Database</authmode> </webgui> <maximumtableentries>400000</maximumtableentries> <disablenatreflection>yes</disablenatreflection> </pre>	
@@ -286,7 +288,7 @@	
<pre> <enable/> </rrd> <widgets> - <sequence>system_information:col1:open:0,thermal_sensors:col2:open:0,interfaces:col2:open:1,traffic_graphs:col2:open:0</sequence> + <sequence>system_information:col1:open:0,thermal_sensors:col2:open:0,interfaces:col2:open:1</sequence> </log> <descr><![CDATA[Firewall Logs]]></descr> <filterlogentries>5</filterlogentries> </pre>	
@@ -321,8 +323,8 @@	
<pre> <traffic_graphs> <refreshinterval>1</refreshinterval> <invert>>false</invert> - <backgroundupdate>true</backgroundupdate> - <smoothfactor>0</smoothfactor> + <backgroundupdate>>false</backgroundupdate> + <smoothfactor>1</smoothfactor> <size>1</size> <filter/> </traffic_graphs> </pre>	
@@ -366,8 +368,8 @@	
<pre> <dnssecstripped/> </unbound> <revision> - <time>1706641231</time> - <description><![CDATA[admin@192.168.200.222 (Local Database): Updated traffic graphs widget settings via dashboard.]]></description> + <time>1707750096</time> + <description><![CDATA[admin@192.168.200.222 (Local Database): User Manager Settings saved]]></description> <username>admin@192.168.200.222 (Local Database)</username> </revision> </ppps> </pre>	

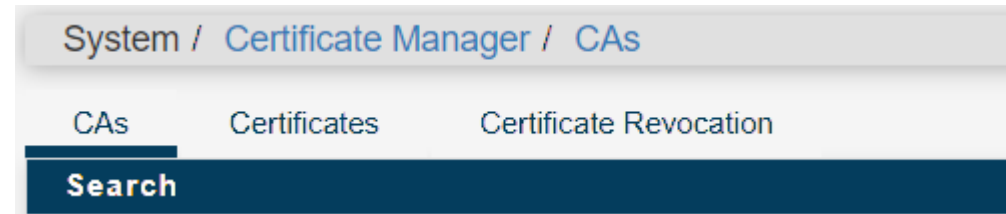
XML Viewer Showing Color-Coded Differences

Any rows highlighted in color represent differences between the two backups:

- **Red Highlight:** Removed Entry
- **Green Highlight:** Added Entry
- **Gray Highlight:** Changed Entry
- **Information Columns:** Each row contains info on Date, Firmware Version, File Size, and Configuration Change(s)
- **Actions Column:** The **Actions** column has three buttons    to revert to the selected config, download that config, or delete that config respectively

CAs

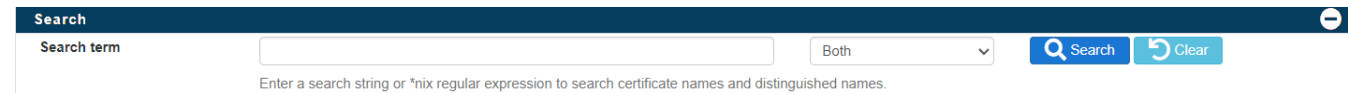
Overview



System / Certificate Manager/ CAs Page

The section has settings for all the Certificate Authorities used in the Anybus Defender The **System / Certificate Manager/ CAs** page is divided into two sections:

Search



Search Section of System / Certificate Manager/ CAs Page

- **Search term:** Enter a search string to use in searching the Certificate Authorities table below
- **Search Name Type:** To the right of the search term entry is a dropdown to select which names will be searched. Options are:
 - **Distinguished Name:** Searches just the text in the **Distinguished Name** column of the Certificate Authorities
 - **Name:** Searches just the **Name** of the Certificate Authorities
 - **Both:** Searches both the CA Name and the Distinguished Name
- **Search button** Click to execute the search. The results will show in the **Certificate Authorities** table below
- **Clear button** Click to clear the search term text and show all the Certificate Authorities

Certificate Authorities

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA_ACME	✓	self-signed	1	ST=Michigan, O=ACME Co, L=Ann Arbor, CN=CA_ACME, C=US Valid From: Mon, 29 Jan 2024 14:46:14 -0500 Valid Until: Thu, 26 Jan 2034 14:46:14 -0500	OpenVPN Server	   

Certificate Authorities of System / Certificate Manager/ CAs Page

This is a table of all Certificate Authorities used in the Anybus Defender. Each row in this table has these columns:

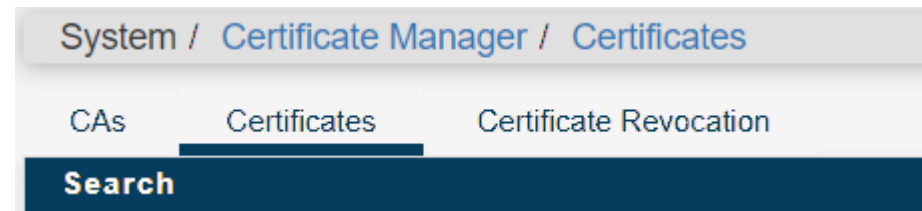
- **Name:** Name of the CA
- **Internal:** Depending on the CA [method used] to create it, this will be checked if an internal CA was created
- **Issuer:** Usually self-signed where certificates will "sign themselves" using the given certificate's private key
- **Certificates:** Count of how many certificates are using this CA

- **Distinguished Name:** Detailed information on the CA. The information can be expanded by using the  button
- **In Use:** List of which service(s) is using this CA
- **Action buttons:** A series of buttons  to edit, export, key export, or reissue/renew the CA

Below the CA table is an + **ADD** button to [Create a New Certificate Authority](#)

Certificates

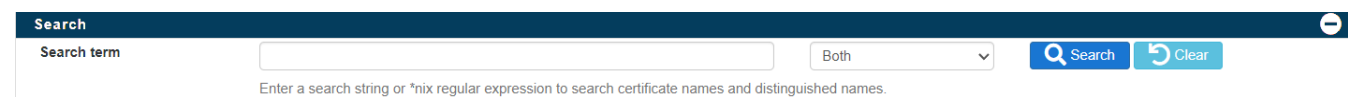
Overview



System / Certificate Manager/ Certificates Page

The section has settings for all the certificates used in the Anybus Defender The **System / Certificate Manager/ Certificates** page is divided into two sections:

Search



Search Section of System / Certificate Manager/ Certificates Page

- **Search term:** Enter a search string to use in searching the Certificates table below
- **Search Name Type:** To the right of the search term entry is a dropdown to select which names will be searched. Options are:
 - **Distinguished Name:** Searches just the text in the **Distinguished Name** column of the Certificates
 - **Name:** Searches just the **Name** of the Certificates
 - **Both:** Searches both the Certificate Name and the Distinguished Name
- **Search button** Click to execute the search. The results will show in the **Certificates** table below
- **Clear button** Click to clear the search term text and show all the Certificates

Certificates

Certificates				
Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (65b0eb1f85376) Server Certificate CA: No Server: Yes	self-signed	O=ICS360.Defender webConfigurator Self-Signed Certificate, CN=ICS360-Defender-65b0eb1f85376  Valid From: Wed, 24 Jan 2024 05:49:03 -0500 Valid Until: Tue, 25 Feb 2025 05:49:03 -0500	webConfigurator	   
SC_ACME Server Certificate CA: No Server: Yes	CA_ACME	ST=Michigan, O=ACME Co, L=Ann Arbor, CN=SC_ACME, C=US  Valid From: Mon, 29 Jan 2024 14:46:14 -0500 Valid Until: Sun, 02 Mar 2025 14:46:14 -0500	OpenVPN Server	   

Certificates of System / Certificate Manager/ Certificates Page

This is a table of all Certificates used in the Anybus Defender. Each row in this table has these columns:

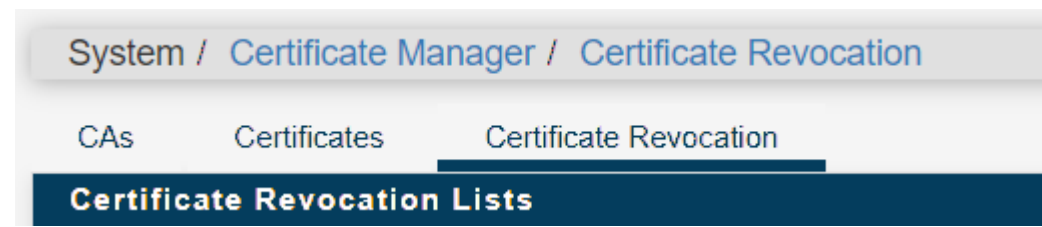
- **Name:** Name of the Certificate
- **Issuer:** The CA who issues the Certificate. Self-signed certificates will "sign themselves" using the given certificate's private key

- **Distinguished Name:** Detailed information on the Certificate. The information can be expanded by using the  button
- **In Use:** List of which service(s) is using this Certificate
- **Action buttons:** A series of buttons  to edit, export, key export, or reissue/renew the Certificate

Below the Certificate table is an **+ ADD** button to [Create a New Certificate](#)

Certificate Revocation

Overview



System / Certificate Manager/ Certificate Revocation

The section shows all the Revoked certificates in the Anybus Defender as well as the ability to add new revocations. The **System / Certificate Manager/ Certificate Revocation** page is divided into two sections:

Certificate Revocation Lists

Certificate Revocation Lists					
CA	Name	Internal	Certificates	In Use	Actions
CA_ACME	Sample Revoke Item	✓	0	✗	  

Certificate Revocation List of System / Certificate Manager/ Certificate Revocation Page

This is a table of all Certificate Revocations used in the Anybus Defender. Each row in this table has these columns:

- **CA:** Name of the [Certificate Authority](#) for this revocation
- **Name:** Descriptive name of the revocation
- **Internal:** Checked if applied to an internal CA
- **Certificates:** number of certificates affect by this revocation
- **In Use:** Indicator to show if the revocation is currently in use
- **Actions Buttons:** A series of buttons    to export, edit, or delete the revocation

Create or Import a New Certificate Revocation List



Create or Import a New Certificate Revocation List of System / Certificate Manager/ Certificate Revocation Page

The dropdown selector allows CA selection for a new revocation to be created

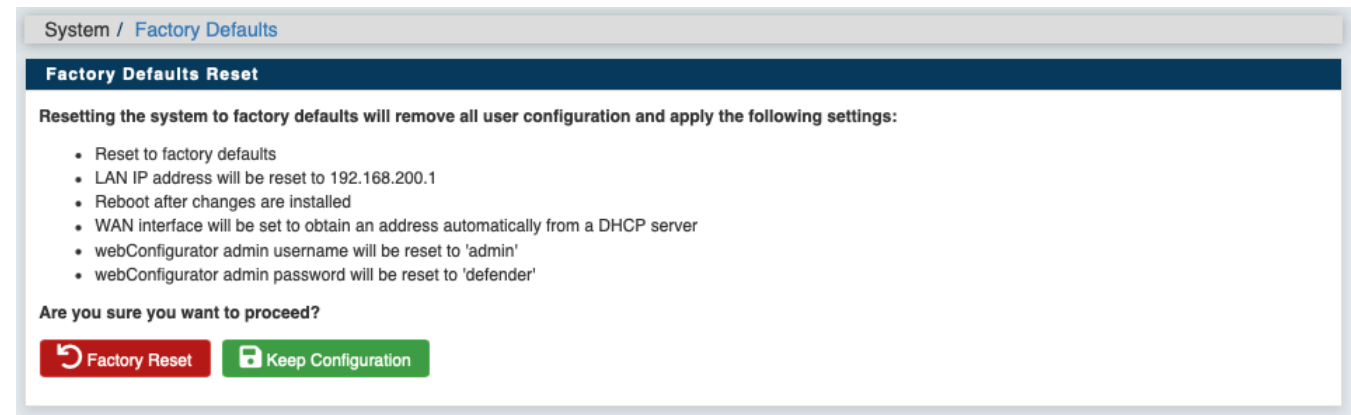
To the right of the dropdown is an **+ Add or Import CRL** button to import or create a new **Certificate Revocation List**

Factory Defaults

Overview



Factory Defaults Reset



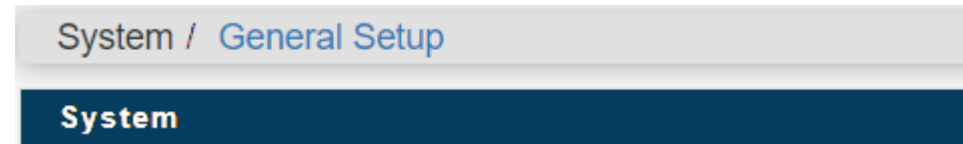
Factory Defaults Reset of System / Factory Defaults Page

Use the **Factory Reset** button to restore the Anybus Defender to its original factory state. After the reset, the unit will automatically reboot.

⊗ This is a destructive operation and will erase all user-created configurations on the device. Be sure to back up the device first if any or all configurations are needed in the future

General Setup

Overview



System / General Setup

The section has general setup settings in the Anybus Defender The **System / General Setup** page is divided into four sections:

System

System	
Hostname	ICS360-Defender Name of the firewall host, without domain part
Domain	localdomain Do not end the domain name with '.local' as the final part (Top Level Domain, TLD), The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternative TLDs such as 'local.lan' or 'mylocal' are safe.

System of System / General Setup Page

- **Hostname:** User-changeable Name of the Anybus Defender host without any domain info
- **Domain:** User-changeable Domain name of the Anybus Defender

ⓘ Do not end the domain name with '.local' as the final part (Top Level Domain, TLD), The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternative TLDs such as 'local.lan' or 'mylocal' are safe

DNS Server Settings

DNS Server Settings	
DNS Servers	DNS Server Address Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled. DNS Hostname Hostname Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).
Add DNS Server	+ Add DNS Server
DNS Server Override	☒ Allow DNS server list to be overridden by DHCP/PPP on WAN If this option is set, ICS360.Defender will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.
DNS Resolution Behavior	Use local DNS (127.0.0.1), fall back to remote DNS Servers (Default) ▼ By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.

DNS Server Settings of System / General Setup Page

- **DNS Servers:** Enter the DNS IP address or optional DNS hostname. More than one DNS Servers can be created by clicking the **+ Add DNS Server** below

i When using IP addresses it can be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled

- **Add DNS Server:** Use the **+ Add DNS Server** to add new rows to the **DNS Servers** list above
- **DNS Server Override:** Check this box to allow a DHCP/PP on the WAN interface to override the DNS server list above
- **DNS Resolution Behavior:** The dropdown will set the priority of the different DNS servers that may be available. Options are:
 - **Use local DNS (127.0.0.1), fall back to remote DNS Servers:** The Firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, then fall back to any remote DNS servers
 - **Use local DNS (127.0.0.1), ignore remote DNS Servers:** The Firewall will ONLY use local DNS service (127.0.0.1, DNS Resolver or Forwarder) and ignore any remote DNS servers
 - **Use remote DNS Servers, ignore local DNS:** The Firewall will ONLY use remote DNS servers and ignore the local DNS

Localization

Localization	
Timezone	US/Eastern Select a geographic region name (Continent/Location) to determine the timezone for the firewall. Choose a special or "Etc" zone only in cases where the geographic zones do not properly handle the clock offset required for this firewall.
Timeservers	pool.ntp.org Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!
Sync time to PC	Sync time to PC Will sync time of ICS360.Defender to your browser.
Language	English Choose a language for the webConfigurator

Localization of System / General Setup Page

- **Timezone:** Use the dropdown selector to choose the geographic region name (Continent/Location) to determine the timezone for the Anybus Defender

i Choose a special or "Etc" zone only in cases where the geographic zones do not properly handle the clock offset required for this device

- **Timeservers:** Enter a server host location to get the accurate time. Use spaces in between hosts if needed
- **Sync time to PC:** Click the **Sync time to PC** to sync the current time in the Anybus Defender to the PC connected to it
- **Language:** Use the dropdown selector to choose the language used by the WebGUI

WebConfigurator

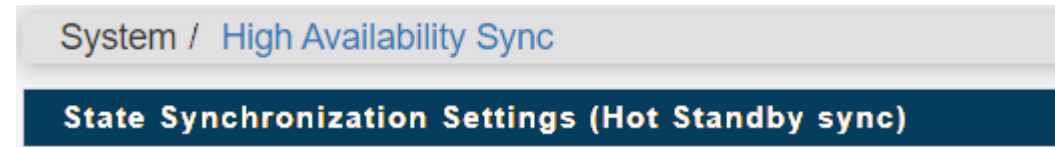
webConfigurator				
Top Navigation	Fixed (Remains visible at top of page) ▼ The fixed option is intended for large screens only.			
Dashboard Columns	2			
Interfaces Sort	☐ Sort Alphabetically If selected, lists of interfaces will be sorted by description, otherwise they are listed wan,lan,optn...			
Associated Panels Show/Hide	☐ Available Widgets Show the Available Widgets panel on the Dashboard.	☐ Log Filter Show the Log Filter panel in System Logs.	☐ Manage Log Show the Manage Log panel in System Logs.	☐ Monitoring Settings Show the Settings panel in Status Monitoring.
Require State Filter	☐ Do not display state table without a filter By default, the entire state table is displayed when entering Diagnostics > States. This option requires a filter to be entered before the states are displayed. Useful for systems with large state tables.			
Left Column Labels	☐ Active If selected, clicking a label in the left column will select/toggle the first item of the group.			
Alias Popups	☐ Disable details in alias popups If selected, the details in alias popups will not be shown, just the alias description (e.g. in Firewall Rules).			
Disable dragging	☐ Disable dragging of firewall/NAT rules Disables dragging rows to allow selecting and copying row contents and avoid accidental changes.			
Login hostname	☒ Show hostname on login banner			

webConfigurator of System / General Setup

- **Top Navigation:** Drop down to select the behavior of the top menu visibility. When using the **Fixed** option, the top menu always remains on top. Using the **Scrolls with page** option, the top menu will scroll out of view if the page is vertically long
- **Dashboard Columns:** Enter the number of columns that will be used on the [Dashboard Page](#) for widget display. The range is between 1 and 6 columns
- **Interfaces Sort:** Click this box to sort the interfaces by description. Otherwise, they are listed in WAN, LAN, and OPT groups
- **Associate Panels Show/Hide:** Check this series of checkboxes to toggle visibility on these panels:
 - **Available Widgets:** Show the Available Widgets panel on the [Dashboard](#)
 - **Log Filter:** Show the Log Filter panel in the System Logs
 - **Manage Log:** Show the Manage Log panel in System Logs
 - **Monitoring Settings:** Show the Settings panel in Status Monitoring
- **Require State Filter:** By default, the entire state table is displayed when entering Diagnostics > States. This option requires a filter to be entered before the states are displayed. Useful for systems with large state tables
- **Left Column Labels:** Check this box to allow clicking a label in the left column that will select/toggle the first item of the group
- **Alias Popups:** Check this box to disable any details of an alias popup and only show alias description
- **Disable dragging:** Check this box to prevent any drag-and-drop or copy/paste operations on any table rows
- **Login hostname:** Check this box to show the hostname on the Anybus Defender login page

High Availability Sync

Overview



System / High Availability Sync

This section has [Top Banner Buttons](#)

The section has synchronization settings for states and others in the Anybus Defender The **System / High Availability Sync** page is divided into two sections:

State Synchronization Settings (Hot Standby sync)

State Synchronization Settings (Hot Standby sync)	
Synchronize states	☐ Hot Standby sync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the Hot Standby sync protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)
Synchronize Interface	WAN If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.
Hot Standby sync Synchronize Peer IP	IP Address Setting this option will force Hot Standby sync to synchronize its state table to this IP address. The default is directed multicast.

State Synchronization Settings (Hot Standby sync) of System / High Availability Sync Page

- **Synchronization States:** Check this box to enable hot standby sync transfers state insertion, update, and deletion messages between firewalls

Each firewall sends these messages out via multicast on a specified interface, using the Hot Standby sync protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking the **Save** button will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

- **Synchronize Interface:** Use the dropdown to select which interface will be used for state synchronization

It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes

- **Hot Standby sync Synchronize Peer IP:** Setting this option will force Hot Standby sync to synchronize its state table to this IP address

If left blank, the default is directed multicast

Configuration Synchronization Settings (XMLRPC Sync)

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP

IP Address

Enter the IP address of the firewall to which the selected configuration sections should be synchronized.

XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username

Enter the webConfigurator username of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password

Remote System Password

Remote System Password

Enter the webConfigurator password of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and password option on backup cluster members!

Confirm

Synchronize admin

☐ synchronize admin accounts and autoupdate sync password.

By default, the admin account does not synchronize, and each node may have a different admin password.
This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

Select options to sync

☐ User manager users and groups
☐ Authentication servers (e.g. LDAP, RADIUS)
☐ Certificate Authorities, Certificates, and Certificate Revocation Lists
☐ Firewall rules
☐ Firewall schedules
☐ Firewall aliases
☐ NAT configuration
☐ IPsec configuration
☐ OpenVPN configuration (Implies CA/Cert/CRL Sync)
☐ DHCP Server settings
☐ WoL Server settings
☐ Static Route configuration
☐ Virtual IPs
☐ Traffic Shaper configuration
☐ Traffic Shaper Limiters configuration
☐ DNS Forwarder and DNS Resolver configurations
☐ Captive Portal
☐ Industrial Protocol

☒ Toggle All

Configuration Synchronization Settings (XMLRPC Sync) of System / High Availability Sync

- Synchronize Config to IP:** Enter the IP address of the firewall to which the selected configuration sections should be synchronized

ⓘ XMLRPC sync is currently only supported over connections using the same protocol and port as this system. Make sure the remote system's port and protocol are set accordingly! Do not use the Synchronize Config to IP and password option on backup cluster members!
- Remote System Username:** Enter the WebGUI username of the system entered above for synchronizing the configuration

ⓘ Do not use the Synchronize Config to IP and username option on backup cluster members!
- Remote System Password:** Enter the WebGUI password of the system entered above for synchronizing the configuration

ⓘ Do not use the Synchronize Config to IP and password option on backup cluster members!
- Synchronize admin:** Check this box to automatically synchronize the sync passwords with admin passwords. This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account
- Select options to sync:** A list of checkboxes to select which options in the Anybus Defender will be synchronized. Use the **Toggle All** button to select/deselect all options

License

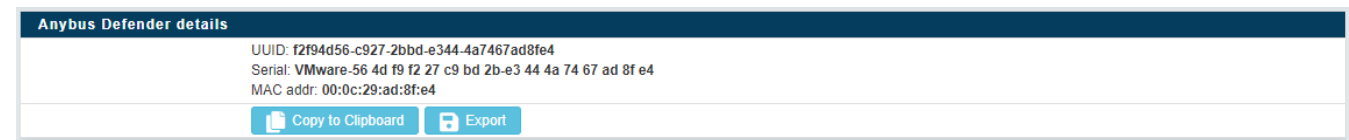
Overview



System / License

The section has settings for exporting and uploading licenses in the Anybus Defender The **System / License** page is divided into three sections:

Anybus Defender details



ICS360.Defender details of System / License Page

- **UUID:** The Universal Unique Identifier (UUID) for this Anybus Defender
- **Serial:** Serial number of the unit
- **MAC addr:** The MAC address of WAN interface
- **Copy to Clipboard Button:** Click this to copy the above UUID, Serial, and MAC to the computer's clipboard which can then be pasted into a text editor, email message, etc
- **Export:** Click this to create a file with the UUID, Serial, and MAC information

i This information is needed for any Anybus Defender license upgrades. Contact sales@hms-networks.com for more information on licensing upgrade pricing and procedures

License Information



License Information of System / License Page

- **Identifier:** Unique ID for the license installed
- **Variant** The License type (3-letter abbreviation) as described in the [Licensing Section](#)
- **Features:** List of features activated based on the current license variant. The [Licensing Section](#) also lists these features

Logout

Overview

This option will log the current user out of the Anybus Defender and load the WebGUI login screen

❗ The logout is immediately done when selecting this menu option

Package Manager

Overview

System / Package Manager / Installed Packages

Installed Packages	Available Packages			
Installed Packages				
Name	Category	Version	Description	Actions
✓ API	sysutils	1.3.4_1	Provide modular RESTful APIs for use by a remote server.	
✓ AssetMgmt	sysutils	1.0.1_6	A package to scan hosts on the network and identify OS and/or Industrial Protocol information.	
✓ RemoteMgmt	sysutils	0.5.1	A package to integrate with a remote management server to allow remote control/visibility of this instance	

= Update = Current
 = Remove = Information = Reinstall
Newer version available
Package is configured but not (fully) installed or deprecated

System / Package Manager Showing Installed Packages

The Package Manager allows [Packages](#) to be viewed, installed, uninstalled, or upgraded. There are two tabs used for packages:

Installed Packages

This is a table of all the currently-installed packages in the Anybus Defender. The table columns are:

- Status Icons:** To the left of the package name is an icon indicator to show if the package is the current one or has an update available
- Name:** The package name
- Category:** The category of the package. The [Packages](#) has a list of the categories used
- Version:** The version of the installed package
- Description:** A brief description of the package
- Actions:** Two buttons allow for removing or reinstalling the package

Below the table is a legend showing the button icon meanings explained above. There is also text coding, where any yellow-colored table entries represent a new package version is available or red represents deprecated or improperly installed package

Available Packages

Installed Packages

Available Packages

Search

Search term

Both

Search

Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Name	Version	Description	
Acme	0.6.11	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates.	+ Install
Apcupsd	0.3.92_10	"apcupsd" can be used for controlling all APC UPS models It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN	+ Install
Arping	1.2.3_2	Broadcasts a who-has ARP packet on the network and prints answers.	+ Install
Arpwatch	0.2.1_6	This package contains tools that monitors ethernet activity and maintains a database of ethernet/ip address pairings. It also reports certain changes via email.	+ Install
Bandwidthd	0.7.5_5	BandwidthD tracks usage of TCP/IP network subnets and builds html files with graphs to display utilization. Charts are built by individual IPs, and by default display utilization over 2 day, 8 day, 40 day, and 400 day periods. Furthermore, each IP address's utilization can be logged out in CDF format, or to a backend database server. HTTP, TCP, UDP, ICMP, VPN, and P2P traffic are color coded.	+ Install
Bind	9.16.1_11	ICS360 Defender GUI for BIND DNS server	+ Install
Freeradius3	0.15.8_32	A free implementation of the RADIUS protocol. Supports MySQL, PostgreSQL, LDAP, Kerberos.	+ Install
Ftp client proxy	0.3.1_7	Basic FTP Client Proxy using ftp-proxy from FreeBSD.	+ Install
Haproxy	0.61.1_3	The Reliable, High Performance TCP/HTTP(S) Load Balancer. This package implements the TCP, HTTP and HTTPS balancing features from haproxy. Supports ACLs for smart backend switching.	+ Install
Haproxy devel	0.62.1_4	The Reliable, High Performance TCP/HTTP(S) Load Balancer. This package implements the TCP, HTTP and HTTPS balancing features from haproxy. Supports ACLs for smart backend switching.	+ Install
Iperf	3.0.3_5	Iperf is a tool for testing network throughput, loss, and jitter.	+ Install
Ladvd	1.2.3_2	Send and decode link layer advertisements. Support for LLDP (Link Layer Discovery Protocol), CDP (Cisco Discovery Protocol), EDP (Extreme Discovery Protocol) and NDP (Nortel Discovery Protocol).	+ Install

System / Package Manager showing Available Packages

This tab shows all the available [Packages](#) that can be installed in the Anybus Defender

❗ To install packages, an internet connection is required on the Anybus Defender

The **System / Package Manager / Available packages** page is divided into two sections:

Search

Search

Search term

Both

Search

Clear

Enter a search string or *nix regular expression to search package names and descriptions.

System / Package Manager showing Available Packages

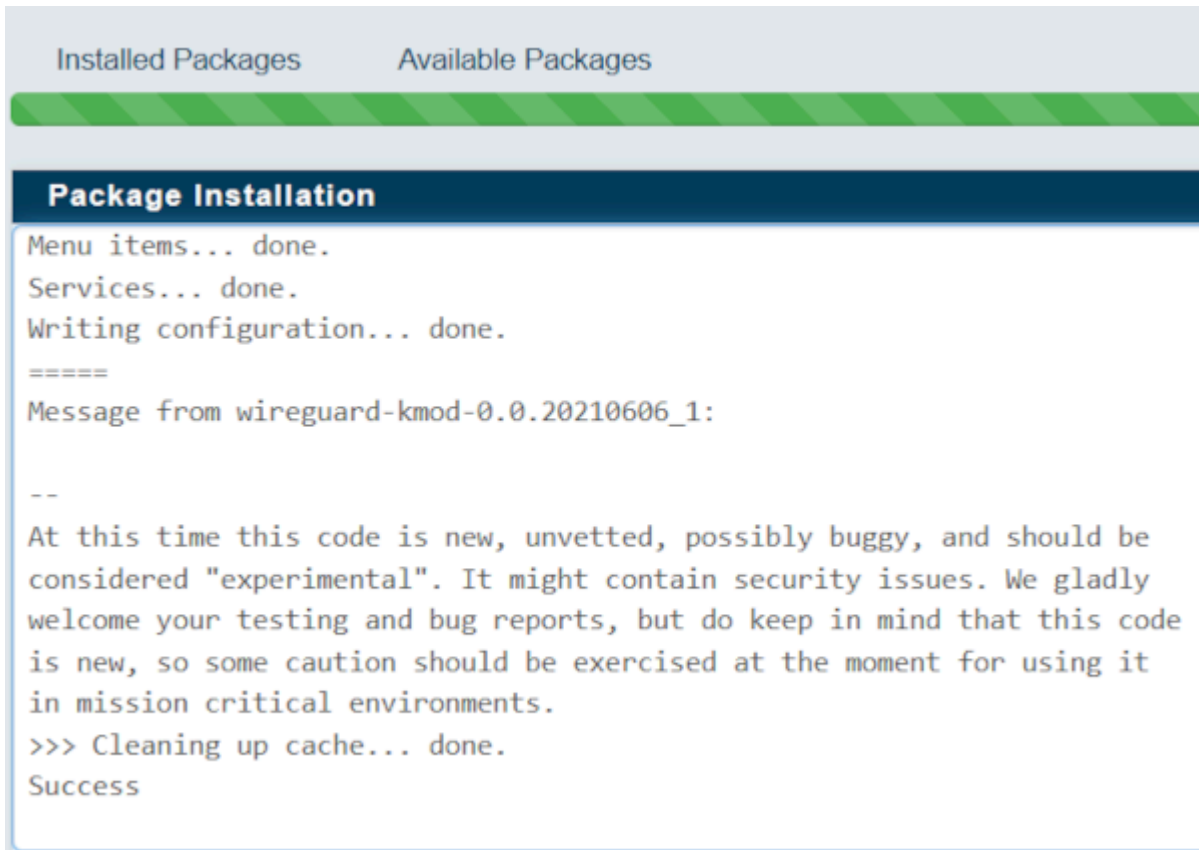
- **Search term:** Enter a search string to use in searching the Packages table below
- **Search Name Type:** To the right of the search term entry is a dropdown to select which names will be searched. Options are:
 - **Name:** Searches just the **Name** of the **Packages** table
 - **Description:** Searches just the **Description** of the **Packages** table
 - **Both:** Searches both the **Name** and the **Description** of the **Packages** table
- **Search button** Click to execute the search. The results will appear in the **Packages** table below
- **Clear button** Click to clear the search term text and show all the **Packages** table

Packages

This is a table of all the currently available packages for the Anybus Defender. The table columns are:

- **Name:** The package name
- **Version:** The current version of the package
- **Description:** A brief description of the package
- **Install button:** Click to install the package. After clicking the **Install** button, click the **Confirm** button to begin the installation

During installation, a command window will appear with a horizontal progress bar:



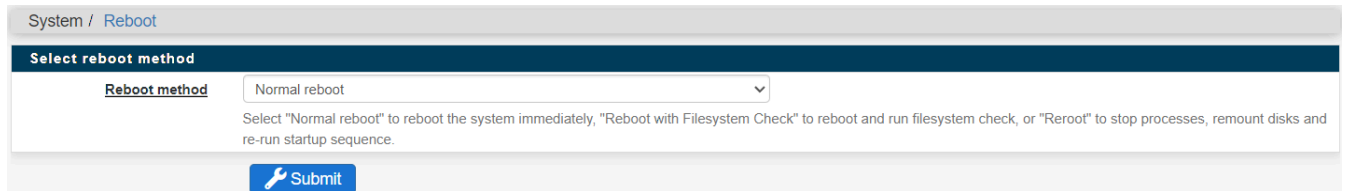
```
Menu items... done.
Services... done.
Writing configuration... done.
====
Message from wireguard-kmod-0.0.20210606_1:
--
At this time this code is new, unvetted, possibly buggy, and should be
considered "experimental". It might contain security issues. We gladly
welcome your testing and bug reports, but do keep in mind that this code
is new, so some caution should be exercised at the moment for using it
in mission critical environments.
>>> Cleaning up cache... done.
Success
```

System / Package Manager showing Available Packages

⚠ Wait until the **Success** message appears on the installation command window before doing any other operation in the WebGUI

Reboot

Overview

A screenshot of a web interface for rebooting a system. At the top, there is a breadcrumb trail 'System / Reboot'. Below this is a section titled 'Select reboot method'. Inside this section, there is a label 'Reboot method' followed by a dropdown menu currently showing 'Normal reboot'. Below the dropdown, there is a text instruction: 'Select "Normal reboot" to reboot the system immediately, "Reboot with Filesystem Check" to reboot and run filesystem check, or "Reroot" to stop processes, remount disks and re-run startup sequence.' At the bottom of the section is a blue button with a wrench icon and the text 'Submit'.

System / Reboot

The Reboot page allows the reboot of the Anybus Defender using various methods:

Select Reboot method

Within the **Select Reboot method** section are these options:

- **Reboot method:** use the dropdown to select a reboot type:
 - **Normal reboot:** Reboots the system immediately
 - **Reboot with Filesystem Check:** Reboots the system and runs a filesystem check
 - **Fast reboot:** Stops all processes, remounts the disks, and re-runs the startup sequence without doing a complete device restart
- **Submit Button:** Click this button to reboot the Anybus Defender with the selected Reboot method

Remote Management Integration

Overview

Package / System: Remote Management

General Options

Package / System: Remote Management

General Options

General Options

Enable

☐ Enable Remote Management

This allows for management of some parts of this units configuration by a remote server.

Adoption File

Choose File

No file chosen

 Save

General Options of Package / System: Remote Management Page

- Enable:** Check this box to allow Anybus ACC and the Anybus Defender to interact
- Adoption File:** Use the **Choose File** button to load the required adoption file

 Adoption files are created on a licensed Anybus ACC application

Gateways

Overview

System / Routing / Gateways

Gateways

Static Routes

Gateway Groups

Gateways

System / Routing / Gateways Page

This section has [Top Banner Buttons](#)

This page has settings related to gateway routings in the Anybus Defender. The **System / Routing / Gateways** page is divided into two sections:

Gateways

Gateways							
Name	Default	Interface	Gateway	Monitor IP	Description	Actions	
☒ WAN_DHCP 		WAN	192.168.68.1	192.168.68.1	Interface WAN_DHCP Gateway	 	 Save  Add

Gateways Section of Routing / Gateways Page

This table lists all the **Gateways** configured in this device. Each row in this table has these columns:

- Enabled/Disabled Status:** The icon indicator to the left of the gateway name shows whether the gateway is currently enabled  or disabled 

i When a gateway is disabled, the text will change from black to a lighter gray color

- Name:** The gateway name
- Default:** Indicates whether this is the default gateway as described below
- Interface:** The interface used in this gateway
- Gateway:** IP address assigned to this gateway
- Monitor IP:** An alternative address here to be used to monitor the link
- Description:** Brief description of the gateway
- Actions:** A series of buttons     to edit, duplicate, disable/enable, or delete the gateway

On the lower right of the table are two buttons  Save  Add to **Save Gateway settings** and [Add New Gateways](#)

i While a gateway is in a group it cannot be disabled. To disable the gateway, remove it from all groups

Default gateway

Default gateway

Default gateway IPv4

Automatic

Select a gateway or failover gateway group to use as the default gateway.

Default gateway IPv6

Automatic

Select a gateway or failover gateway group to use as the default gateway.

Save

Gateways Section of Routing / Gateways Page

- **Default gateway IPv4:** When using IPv4 addressing, the dropdown can be used to select which gateway or failover gateway group will be used as the default gateway. Options for **Automatic** and **None** are also available
- **Default gateway IPv6:** When using IPv6 addressing, the dropdown can be used to select which gateway or failover gateway group will be used as the default gateway. Options for **Automatic** and **None** are also available
- **Save Button:** After setting either default gateway, click this button to update the device

 On the lower right of this page is a  button can be toggled to show/hide legend information about the various indicators used on this page



The current default route as present in the current routing table of the operating system



Gateway is inactive, interface is missing



Gateway disabled



Gateway enabled

Gateway Icon Indicator Legend

Static Routes

Overview

System / Routing / Static Routes

Gateways

Static Routes

Gateway Groups

Static Routes				
Network	Gateway	Interface	Description	Actions
☒ 192.168.68.99/32	WAN_DHCP - 192.168.68.1	WAN	Sample Static Route	

+ Add

System / Routing / Static Routes Page

This section has [Top Banner Buttons](#)

This page has settings related to static routes in the Anybus Defender

Static Routes

This table lists all the **Static Routes** configured in this device. Each row in this table has these columns:

- Enabled/Disabled Status:** The icon indicator to the left of the route Network shows whether the route is currently enabled  or disabled 

i When a route is disabled, the text will change from black to a lighter gray color

- Network:** The IPaddress and Subnet mask of the static route target
- Gateway:** The [Gateway](#) used for the static route
- Interface:** The interface used in this static route
- Description:** Brief description of the gateway
- Actions:** A series of buttons     to edit, duplicate, disable/enable, or delete the route

On the lower right of the table is an **+ Add** button to add a new **Static Route**

i On the lower right of this page is a  button can be toggled to show/hide legend information about the various indicators used on this page



Route is inactive, gateway interface is missing



Route disabled



Route enabled

Gateway Icon Indicator Legend

Overview

System / Routing / Gateway Groups Page

This page has settings related to gateway groups in the Anybus Defender

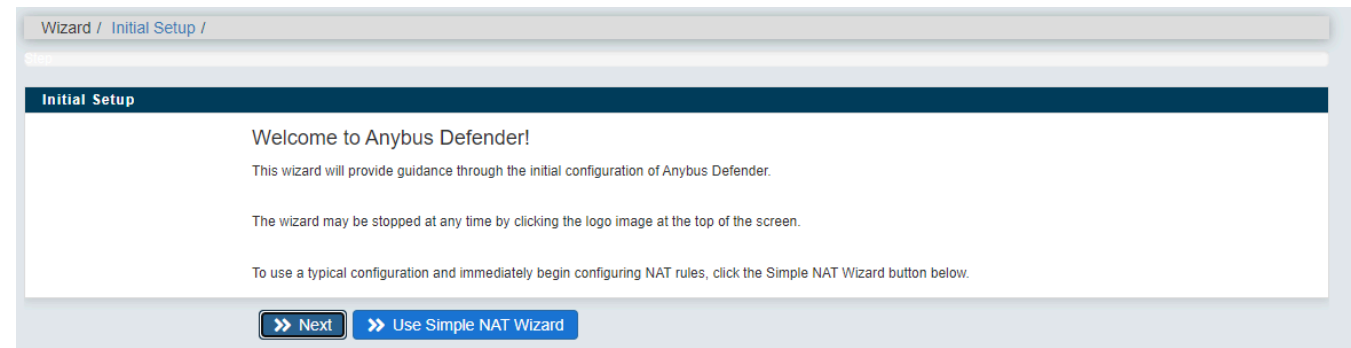
This table lists all the **Gateway Groups** configured in this device. Each row in this table has these columns:

- On the lower right of the table is a button to [Add New Gateway Group](#).

❶ As mentioned when toggling on  button on the lower left of the page, remember to use these Gateway Groups in firewall rules in order to enable load balancing, failover, or policy-based routing. Without rules directing traffic into the Gateway Groups, they will not be used

Setup Wizard

Overview



System / Setup Wizard

The Setup Wizard page allows for a guided wizard to be used to set up the Anybus Defender for standard functionality. It also has a more basic [Simple NAT Wizard](#) for basic WAN access and NAT communication

Wizard Selection

From the two buttons on this page, the >> **Next** button will begin the standard setup wizard. The >> **Use Simple NAT Wizard** will begin the [Simple NAT Wizard explained here](#)

Standard Setup Wizard

Clicking the >> **Next** button will start the standard setup wizard with these steos:

Step 1 of 8: General Information

General Information	
On this screen the general Anybus Defender parameters will be set.	
Hostname	Anybus-Defender EXAMPLE: myserver
Domain	localdomain EXAMPLE: mydomain.com
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.	
Primary DNS Server	
Secondary DNS Server	
Override DNS	☒
Allow DNS servers to be overridden by DHCP/PPP on WAN	
>> Next	

General Information Page

This is general Anybus Defender settings including:

- **Hostname:** Name of this Anybus Defender. The default name can be changed
- **Domain:** Domain name used. By default, **localhost** is used
- **Primary DNS Server:** If DNS is used, the primary DNS can be entered here

- **Secondary DNS Server:** If DNS is used, the secondary DNS can be entered here

❗ The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use these manually configured DNS servers for client queries, visit [Services > DNS Resolver](#) and enable **DNS Query Forwarding** after completing this wizard

- **Override DNS:** Check this box to have DNS settings overridden by any DHCP/PP on the WAN

Click the >> **Next** button to continue to the next step

Step 2 of 8: Time Server Information

Time Server Information	
Please enter the time, date and time zone.	
Time server hostname	pool.ntp.org
Enter the hostname (FQDN) of the time server.	
Timezone	US/Eastern
» Next	

Time Server Page

- **Time server hostname:** Enter a Network Time Protocol (NTP) hostname that will synchronize with the system clock to the Anybus Defender

❗ It is recommended to use the default NTP hostname already set here

- **Timezone:** Use the dropdown to select the proper geographic location of the Anybus Defender to adjust the system clock to the proper time zone

Click the >> **Next** button to continue to the next step

Step 3 of 8: Configure WAN Interface

This step sets up the Wide Area Network (WAN)

Configure WAN Interface	
On this screen the Wide Area Network information will be configured.	
Selected Type	Static

Configure WAN Interface

- **SelectedType:** Use the dropdown selector to set the type of configuration to use. Options are:
 - **Static:** Manual entry of the WAN gateway IP address, subnet, and upstream gateway. Selecting this option enables the **Static IP Configuration** explained below and disables the **DHCP Hostname** also explained below
 - **DHCP:** Allows automatic IP address, subnet, and upstream gateway by use of a DHCP server on the WAN. Selecting this option disables the **Static IP Configuration** explained below but enables the **DHCP Hostname** also explained below
 - **PPPoE:** Allows the use of Point-to-Point Protocol over Ethernet (PPPoE) WAN type that may be required by the ISP. Selecting this option disables the **Static IP Configuration** and **DHCP Hostname** sections and enables the **PPPoE configuration:** explained below
 - **PPTP:** Allows the use of Point-to-Point Tunneling Protocol (PPTP) WAN type that may be required by the ISP. Selecting this option disables the **Static IP Configuration**, **DHCP Hostname**, and **PPPoE configuration** sections and enables the **PPTP configuration** explained below

General configuration	
MAC Address	 This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU	 Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.
MSS	 If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

General configuration

- **MAC Address:** Allows modification of the MAC address of the WAN network (called "spoofing")

❗ The MAC address format needs to be xx:xx:xx:xx:xx:xx

- **MTU:** Overrides the Maximum Transmission Unit (MTU) for packet sizes in bytes if required. If left blank, the default will be 1492 bytes for PPPoE or 1500 bytes for all others
- **MSS:** Overrides the Maximum Segment Size (MSS) for packet sizes in bytes if required. If left blank, the default will be 1492 bytes for PPPoE or 1500 bytes for all others

i The MSS should match the MTU setting in most cases

Static IP Configuration	
IP Address	192.168.68.55
Subnet Mask	24
Upstream Gateway	192.168.68.1

Static IP Configuration

❗ The settings are only available when the **Static** Type is set above

- **IP Address:** The WAN IP address
- **Subnet Mask:** The subnet mask of the WAN
- **Upstream Gateway:** If the WAN is connected to an upstream network, the gateway IP address can be entered here

DHCP client configuration	
DHCP Hostname	 The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

DHCP client configuration

❗ The settings are only available when the **DHCP** Type is set above

- **DHCP Hostname:** For some ISPs, a DHCP client identifier and hostname may be required when requesting a DHCP lease. Enter that information here

PPPoE configuration	
PPPoE Username	
PPPoE Password	
Show PPPoE password	☐ Reveal password characters
PPPoE Service name	 Hint: this field can usually be left empty
PPPoE Dial on demand	☐ Enable Dial-On-Demand mode This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.
PPPoE Idle timeout	 If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

PPPoE configuration

❗ The settings are only available when the **PPPoE** Type is set above

- **PPPoE Username:** Enter the login name for the PPPoE
- **PPPoE Password:** Enter the login password for the PPPoE
- **Show PPPoE password:** Check this box to see the **PPPoE Password** above in a human-readable form
- **PPPoE Service name:** If required, the PPPoE service name can be entered
- **PPPoE Dial on demand:** Check this box to enable the Dial-On-Demand mode. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected
- **PPPoE idle timeout:** Enter timeout in seconds when no qualifying outgoing packets are transmitted. Setting this to 0 disables this feature

PPTP configuration	
PPTP Username	
PPTP Password	
Show PPTP password	☐ Reveal password characters
PPTP Local IP Address	
pptpllocalsubnet	32
PPTP Remote IP Address	
PPTP Dial on demand	☐ Enable Dial-On-Demand mode This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.
PPTP Idle timeout	

If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

PPTP configuration

❗ The settings are only available when the **PPTP** Type is set above

- **PPTP Username:** Enter the login name for the PPTP
- **PPTP Password:** Enter the login password for the PPTP
- **Show PPTP password:** Check this box to see the **PPTP Password** above in a human-readable form
- **PPTP Local IP Address:** Enter the local address used by the Anybus Defender for the PPTP connection
- **pptpllocalsubnet:** Dropdown selector for the subnet mask of the local connection
- **PPTP Remote IP Address:** Enter the PPTP server IP Address. This uses the same subnet as the local IP address
- **PPTP Dial on demand:** Check this box to enable the Dial-On-Demand mode. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected
- **PPTP idle timeout:** Enter timeout in seconds when no qualifying outgoing packets are transmitted. Setting this to 0 disables this feature

RFC1918 Networks	
Block RFC1918 Private Networks	☐ Block private networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

RFC1918 Networks

- **Block RFC1918 Private Networks:** Check this box to block traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8)

❗ This option should generally be left turned on unless the WAN network is within a private address space as well

Block bogon networks	
Block bogon networks	☐ Block non-Internet routed networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.
>> Next	

Block bogon networks

- **Block RFC1918 Private Networks:** Check this box to blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA

❗ Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received

Click the >> **Next** button to continue to the next step

Step 4 of 8: Configure LAN Interface

This step sets up the Local Area Network (LAN)

Configure LAN Interface	
On this screen the Local Area Network information will be configured.	
LAN IP Address	192.168.200.2 Type dhcp if this interface uses DHCP to obtain its IP address.
Subnet Mask	24
>> Next	

Configure LAN Interface

- **LAN IP Address:** Enter the IP address of the LAN
- **Subnet Mask:** Use the dropdown to select the Subnet Mask of the LAN

Click the >> **Next** button to continue to the next step

Step 5 of 8: Set Admin WebGUI Password

This step sets up the Admin user password

❗ This password should be changed immediately because the same default password is used for ALL Anybus Defender devices

Set Admin WebGUI Password	
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.	
Admin Password	
Admin Password AGAIN	

Set Admin WebGUI Password

- **Admin Password:** Enter a new admin password
- **Admin Password AGAIN:** Re-enter the same password

Click the >> **Next** button to continue to the next step

Step 6 of 8: Reload configuration

Reload configuration
Click 'Reload' to reload Anybus Defender with new changes.
>> Reload

Reload configuration

Click the >> **Reload** button to reload the Anybus Defender

Step 7 of 8: Reload configuration

Reload in progress

A reload is now in progress. Please wait.

The wizard will redirect to the next step once the reload is completed.

Reload in progress

A **Reload in progress** page will appear. No user input is required here

Step 8 of 8: Reload configuration

Wizard completed.

Congratulations! Anybus Defender is now configured.

We recommend that you check to see if there are any software updates available if you are connected to internet. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

Check for updates

Finish

Wizard completed

A **Wizard complete** page will appear. From here, the **Check for updates** button can be clicked to check if there are any software updates for the Anybus Defender or just the **Finish** button to be redirected to the [Main dashboard page](#)

Shutdown System

Overview

System / [Shutdown System](#)

System Halt Confirmation

Click "Shutdown" to shutdown the system immediately, or "Cancel" to go to the system dashboard. (There will be a brief delay before the dashboard appears.)

 Shutdown

 Cancel

System / Shutdown System

The Shutdown System page allows for the shutdown of the Anybus Defender. Either click the **Shutdown** button to commence shutdown or the **Cancel** button to be returned to the [Main dashboard page](#)

System Update

Overview

The screenshot shows the 'System Update' page. At the top, there is a breadcrumb trail: 'System / Update / System Update'. Below this, there are two tabs: 'System Update' (which is active) and 'Update Settings'. A dark blue banner reads 'Confirmation Required to update Anybus Defender system.' Below the banner, there are two rows of information: 'Current Base System' with the value '2.5.2-2024043016', and 'Latest Base System' with the value 'Retrieving' and a yellow gear icon.

System / Update / System Update	
System Update	Update Settings
Confirmation Required to update Anybus Defender system.	
Current Base System	2.5.2-2024043016
Latest Base System	Retrieving

System / Update / System Update

- ❗ Checking and updating the system OS usually requires an internet connection to the device. There is an option to allow Offline updates but will require an external drive with the system OS on it

The Update page allows for checking and updating the system OS in the Anybus Defender. The two tabs on this page are:

System Update

As shown in the image above, the **System Update** tab has these readouts:

- **Current Base System:** The OS version currently in the device
- **Latest Base System:** The latest OS version for the Anybus Defender
- **Status:** Depending on the current and latest OS versions and the internet connectivity, these messages may appear:
 - **Update to date.**
 - **Update available** When this appears an **Update** button will appear to allow updating the system OS to the latest version

- **Any system OS updates will require the device to be taken offline and restarted. Also, be sure to back up the device configuration before updating**

- **Unable to check for updates** This usually happens when there is not an internet connection to the device

Update Settings

The screenshot shows the 'Update Settings' page. At the top, there is a breadcrumb trail: 'System Update / Update Settings'. Below this, there are two tabs: 'System Update' and 'Update Settings' (which is active). Below the tabs, there is a section titled 'Updates'. It contains two settings: 'Dashboard check' with a checked checkbox and the text 'Disable the Dashboard auto-update check', and 'Enable Offline Upgrades' with an unchecked checkbox and the text 'Enable Offline Firmware Upgrades from removable storage i.e. USB sticks'. At the bottom of the settings section, there is a blue 'Save' button with a floppy disk icon.

System Update / Update Settings	
System Update	Update Settings
Updates	
Dashboard check	☒ Disable the Dashboard auto-update check
Enable Offline Upgrades	☐ Enable Offline Firmware Upgrades from removable storage i.e. USB sticks

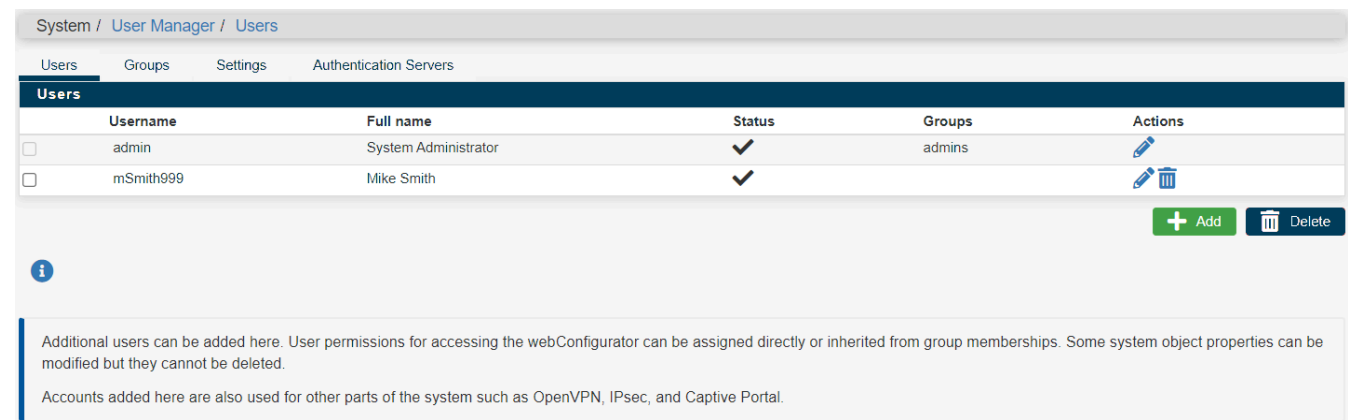
System / Update / Update Settings

- **Dashboard check:** Check this box to prevent the Main dashboard from automatically checking for system updates
- **Enable Offline Upgrades:** Check this box to allow system updates from external drives (USB sticks, etc)

Click the **Save** button if any changes are made

Users

Overview



System / User Manager / Users

The **Users** tab of the User Manager page allows for viewing, adding, editing, and deleting users in the Anybus Defender. These users can be used to manage the Anybus Defender, [OpenVPN](#), IPsec, and [Captive Portal](#)

Users

As shown in the image above, the **Users** tab show a table of users with these columns:

- **Selection Checkbox:** To the left of the Username, is a checkbox that can be used for bulk operations (delete, for example)
- **Username:** The username of the user
- **Full Name:** The user's full name
- **Status:** An indicator to show whether the user is enabled  or disabled 
- **Groups:** Which group(s) the user is a member of
- **Actions:** Two buttons   for editing or deleting the user

 The default admin user cannot be removed so it will not show the delete button

On the lower-right of the Users table, are two buttons to [Add a New User](#) and **Delete** a user

 As mentioned when toggling on  button on the lower left of the page, User permissions for accessing the WebGUI can be assigned directly or inherited from [Group Memberships](#). Some system object properties can be modified but they cannot be deleted.

Groups

Overview

System / [User Manager](#) / [Groups](#)

Users **Groups** Settings Authentication Servers

Groups			
Group name	Description	Member Count	Actions
admins	System Administrators	1	
all	All Users	2	
engineers		1	 

 Add

System / User Manager / Groups

The **Groups** tab of the User Manager page allows for viewing, adding, editing, and deleting user groups in the Anybus Defender. User groups allow grouping users according to their role and the permissions allowed to them

Groups

As shown in the image above, the **Groups** tab show a table of user groups with these columns:

- **Group name:** The name of the user group
- **Description:** Short description of the user group
- **Member Count:** Number of users that are a member of the user group
- **Actions:** Two buttons   for editing or deleting the user groups

 The default **admins** and **All Users** groups cannot be removed so it will not show the delete button

On the lower-left of the user groups table, are two buttons to [Add a New User Group](#) and **Delete** a user group

Settings

Overview

System / User Manager / Settings

UsersGroupsSettingsAuthentication Servers

Settings

Session timeout

30

Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to never expire sessions. NOTE: This is a security risk!

Authentication Server

Local Database

Shell Authentication

☐ Use Authentication Server for Shell Authentication

If RADIUS or LDAP server is selected it is used for console and SSH authentication. Otherwise, the Local Database is used.
To allow logins with RADIUS credentials, equivalent local users with the expected privileges must be created first.
To allow logins with LDAP credentials, Shell Authentication Group DN must be specified on the LDAP server configuration page.

Auth Refresh Time

Time in seconds to cache authentication results. The default is 30 seconds, maximum 3600 (one hour). Shorter times result in more frequent queries to authentication servers.

Save

Save & Test

System / User Manager / Settings

The **Settings** tab of the User Manager page has various settings related to the User Manager

Settings

As shown in the image above, the **Settings** tab has these options:

- Session Timeout:** The length of inactivity time in minutes before the current user is locked out. If left blank, the default time is 4 hours (240 minutes)

ⓘ A value of 0 can be used to disable any timeout, but this is a security risk!

- Authentication Server:** Use the dropdown selector to choose the user authentication server type. This is usually set to **Local Database** unless RADIUS or LDAP is used

ⓘ If RADIUS or LDAP server is selected it is used for console and SSH authentication. Otherwise, the Local Database is used. To allow logins with RADIUS credentials, equivalent local users with the expected privileges must be created first. To allow logins with LDAP credentials, Shell Authentication Group DN must be specified on the LDAP server configuration page

- Auto Refresh Time:** Enter a number in seconds to cache authentication results. If left blank, the default will be 30 seconds. The maximum is 3600 seconds (1 hour)

ⓘ Shorter times result in more frequent queries to authentication servers

Authentication Servers

Overview

System / [User Manager](#) / [Authentication Servers](#)

Authentication Servers			
Server Name	Type	Host Name	Actions
Test	LDAP	199.99.99.99	  
Local Database		Anybus-Defender	

 Add

System / User Manager / Authentication Servers

The **Authentication Servers** tab of the User Manager page shows a table of servers used for authentication. An authentication server is a centralized system that verifies the identity of users attempting to access a network or service by validating their credentials. The **Local Database** is built-in and is used for all [Users](#)

 The **Local Database** server cannot be deleted or altered

Authentication Servers

As shown in the image above, the **Authentication Servers** tab shows a table of servers with these columns:

- **Server Name:** Name of the server
- **Type:** The server type, either **LDAP** or **RADIUS**
- **Host Name:** Host name or IP address of the server
- **Actions:** A series of buttons    to edit, duplicate, or delete the server

On the lower-left of the Users table, is a button to [Add a New Authentication Server](#)

Interface Assignments

Overview

Interfaces / Interface Assignments

Interface Assignments

Interface Groups

VLANs

PPPs

GREs

GIFs

Bridges

LAGGs

Interface / Interface Assignments

This section has [Top Banner Buttons](#)

This page has settings related to interfaces and their port assignment in the Anybus Defender. The **Interface / Interface Assignments** page is divided into these sections:

Interface - Network port Table

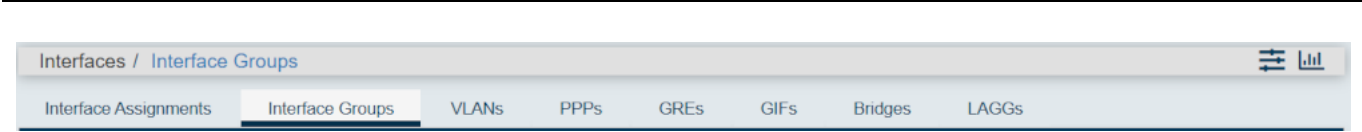
Interface	Network port
WAN	vmx0 (00:0c:29:80:39:1c)
LAN	vmx1 (00:0c:29:80:39:26)
Available network ports:	ovpns1 ()
Save Delete Add	

Interfaces and their Port Assignments

- Interface:** Shows currently assigned interfaces. At the bottom of the table, an **Available network ports:** row allows the selection of unassigned physical ports and virtual interfaces
 - Network port:** Shows the network port currently assigned to each interface. At the bottom of the table is a dropdown list of all remaining unassigned ports. The **+ Add** button allows for the port to be assigned an interface name and added as an assigned port.
 - Delete Button:** To the right of assigned interfaces, except the **WAN** interface which cannot be deleted, is a **Delete** button that will revert the network port to an unassigned port
- Below this table is a **Save** button to save the interface assignment changes

Interface Groups

Overview



Interface / Interface Groups

This section has [Top Banner Buttons](#)

Interface Groups allow setting up rules for multiple interfaces without duplicating the rules. If members are removed from an interface group, the group rules are no longer applicable to that interface

This page has settings related to interfaces and their port assignment in the Anybus Defender. The **Interface / Interface Groups** page is divided into these sections:

Interface Groups

Interface Assignments			
Interface Groups			
Interface Groups			
Name	Members	Description	Actions
WAN_LAN	WAN, LAN		 
			 Add

Interface Groups Section of the Interface / Interface Groups Page

This is a table of all Interface Groups used in the Anybus Defender. Each row in this table has these columns:

- **Name:** The name of the Interface Group
- **Members:** The interfaces assigned to this group
- **Description:** Optional description of this group
- **Actions:** Two buttons   for editing or deleting the group

On the lower-right of the Interface Groups table is an [Add a New Interface Group](#) button

VLANs

Overview

Interfaces / VLANs

Interface Assignments

Interface Groups

VLANs

PPPs

GREs

GIFs

Bridges

LAGGs

Interface / VLANs

This section has [Top Banner Buttons](#)

VLANs, or Virtual Local Area Networks, segment a physical network into multiple virtual networks, enhancing security, flexibility, and efficiency by isolating traffic between different groups of devices

This page has settings related to interfaces and their port assignment in the Anybus Defender. The **Interface / VLANs** page is divided into these sections:

VLAN Interfaces

Interface Assignments	Interface Groups	VLANs	PPPs	GREs	GIFs	Bridges	LAGGs
VLAN Interfaces							
Interface	VLAN tag	Priority	Description	Actions			
vmx0 (wan)	1		Zone 5	 			
							+ Add

VLAN Interfaces Section of the Interface / VLANs Page

- This is a table of all VLAN Interfaces used in the Anybus Defender. Each row in this table has these columns:
- Interface:** The interface the VLAN is using
 - VLAN tag:** Identifiers added to network packets to segregate and manage traffic. The value must be between 1 and 4094
 - VLAN Priority:** value assigned to network packets within a VLAN to prioritize their transmission, ensuring certain types of traffic receive preferential treatment over others. The value must be between 0 and 7, with 0 being the lowest priority traffic and 7 being the highest
 - Description:** Optional description of this VLAN interface
 - Actions:** Two buttons   for editing or deleting the VLAN interface

On the lower-right of the Interface Groups table is an [Add a New VLAN Interface](#) button

ⓘ Not all drivers/NICs support 802.1Q VLAN tagging properly. On cards that do not explicitly support it, VLAN tagging will still work, but the reduced MTU may cause problems

Bridges

Overview

Interfaces / Bridges							
Interface Assignments	Interface Groups	VLANs	PPPs	GREs	GIFs	Bridges	LAGGs

Interface / Bridges

This section has [Top Banner Buttons](#)

A bridge interface connects two ports directly, much like a switch or hub, allowing them to be managed as a single interface for routing and firewall capabilities and passing traffic between them

This page has settings related to interfaces and their port assignment in the Anybus Defender. The **Interface / Bridges** page is divided into these sections:

Bridge Interfaces

Interface Assignments	Interface Groups	VLANs	PPPs	GREs	GIFs	Bridges	LAGGs
Bridge Interfaces							
Interface	Members	Description				Actions	
BRIDGE0	WAN					 	
							 Add

Bridges Section of the Interface / Bridges Page

This is a table of all bridge interfaces used in the Anybus Defender. Each row in this table has these columns:

- **Interface:** Bridge interface name

 The bridge interface name is created automatically beginning with word **BRIDGE** followed by an indexing number

- **Members:** List of all the interfaces assigned to this bridge
- **Description:** Optional description of this bridge interface
- **Actions:** Two buttons   for editing or deleting the bridge interface

On the lower-right of the Interface Groups table is an [Add a New Bridge Interface](#) button

Overview

Overview

Firewall aliases make it easy to use semantic names for devices. This allows for devices to be added or changed later. Aliases can be created for these types:

1. [IP Address](#)
2. [Ports](#)
3. [URLs](#)
4. [All](#)

❗ If an alias cannot be resolved (e.g. because it was deleted), the corresponding element (e.g. filter/NAT/shaper rule) will be considered invalid and skipped

IP

Overview



Firewall / Aliases / IP Page

This section has [Top Banner Buttons](#)

This section is used for managing and organizing IP addresses or ranges within the Anybus Defender configuration

The **Firewall / Aliases / IP** page only has one section:

Firewall Aliases IP

IP

Ports

URLs

All

Firewall Aliases IP

Name	Values	Description	Actions
All_Rockwell	Rockwell_HMI, Rockwell_PLC		  
Rockwell_HMI	192.168.200.121/32, 192.168.200.123/32, 192.168.200.125/32		  
Rockwell_PLC	192.168.2.122, 192.168.2.124, 192.168.124.126		  

 Add

 Import

IP Table of Firewall / Aliases / IP Page

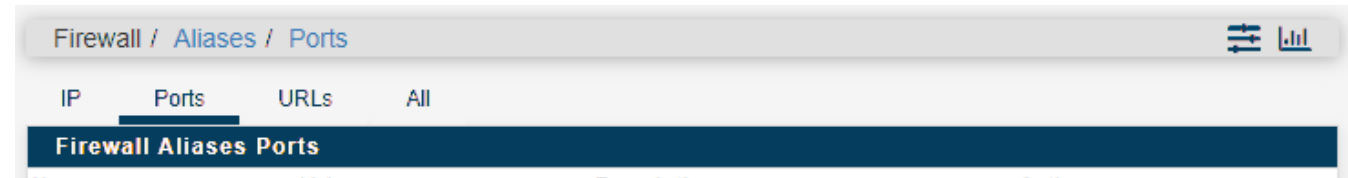
- **Name:** Name of the alias
- **Values:** The specific IP address or addresses associated with this alias
- **Description:** Optional description not used by the Anybus Defender
- **Actions:** The **Actions** column has three buttons    to edit, duplicate, or delete that alias IP respectively

Below the **Firewall Aliases IP** table are these buttons:

- **+ Add:** Sets the properties and host(s) for a new alias IP entry
- **📁 Import:** Imports from a text-based list of aliases

Ports

Overview



Firewall / Aliases / Ports Page

This section has [Top Banner Buttons](#)

This section is used for managing and organizing port numbers within a firewall's configuration

The **Firewall / Aliases / Ports** page only has one section:

Firewall Aliases Ports

A screenshot of the "Firewall Aliases Ports" table. The table has a dark blue header with the text "Firewall Aliases Ports". Below the header is a table with four columns: "Name", "Values", "Description", and "Actions". The first row of data has the following values: "Port_Sample", "44818", an empty cell, and three icons (edit, duplicate, delete). At the bottom right of the table are two buttons: a green "+ Add" button and a blue "Import" button with an upload icon.

Firewall Aliases Ports			
Name	Values	Description	Actions
Port_Sample	44818		  

Ports Table of Firewall / Aliases / IP Page

- **Name:** Name of the alias
- **Values:** The Ports and Port ranges associated with this alias
- **Description:** Optional description not used by the Anybus Defender
- **Actions:** This column has three buttons    to edit, duplicate, or delete the alias port respectively

Below the **Firewall Aliases Ports** table are these buttons:

- **+ Add:** Sets the properties and ports for a new alias port entry
- **⬆️ Import:** Imports from a text-based list of aliases

URLs

Overview



Firewall / Aliases / URLs Page

This section has [Top Banner Buttons](#)

This section is used for managing and organizing URLs or domain names within a firewall's configuration. The URL aliases are mostly useful for public blocklists and locations where you want to dynamically grab a list of IPs or hosts to block

The **Firewall / Aliases / URLs** page only has one section:

Firewall Aliases URLs

IP	Ports	URLs	All
Firewall Aliases URLs			
Name	Values	Description	Actions
+ Add			

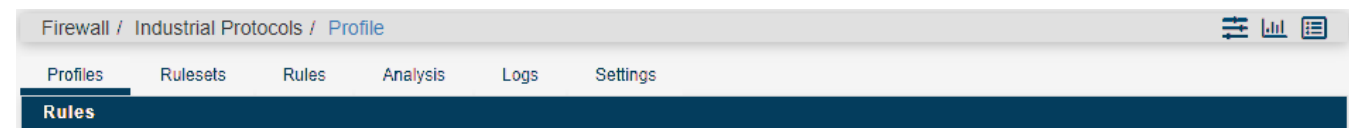
URLs Table of Firewall / Aliases / IP Page

- **Name:** Name of the alias
- **Values:** The specific URL numbers or URL ranges associated with a particular URL alias
- **Description:** Optional description not used by the Anybus Defender
- **Actions:** This column has three buttons    to edit, duplicate, or delete the alias port respectively

Below the **Firewall Aliases URLs** table, there is the + **Add** button to set the properties and URLs for a new alias URL entry

Profiles

Overview



Firewall / Industrial Protocols / Profile Page

This section has [Top Banner Buttons](#)

Industrial Profiles allow granular control over operations of some control devices. Currently, these industrial protocols are supported:

- Ethernet/IP
- Modbus TCP
- S7 Classic and S7 Plus

These protocols are filtered with an inline deep packet inspection engine which is unequalled in the industry for speed and accuracy. The Anybus Defender allows for manual creation of [Rules](#), or can learn network traffic via [Packet Capture](#) and generate a set of rules. The learned rules can be applied via either a block or pass, essentially creating a traffic whitelist with little effort

Rules can be grouped into [Rulesets](#) and then one or more Rulesets can be applied to profiles. Once a profile is created, the profile can be applied to firewall rules on any [Interface](#) configured in the Anybus Defender

❗ Rules can also be applied directly to profiles, though it is highly recommended to only apply rules to a Ruleset. Rulesets allow import/export of rules so they can be easily moved from one Anybus Defender to another

The **Firewall / Industrial Protocols / Profile** page only has one section:

Rules

Profiles Rulesets Rules Analysis Logs Settings					
Rules					
	Action	Name	Description		
☐	×	Rockwell_OnlineOnly			
☐	×	ModBusLimited			
☐	×	S7_Plus_Online_Only			

Profile Rules Table of the Firewall / Industrial Protocols / Profile Page

- **Selection:** This is a checkbox to select the accompanying row

❗ The **Select All** checkbox on the upper left of the table can be used to select all rows

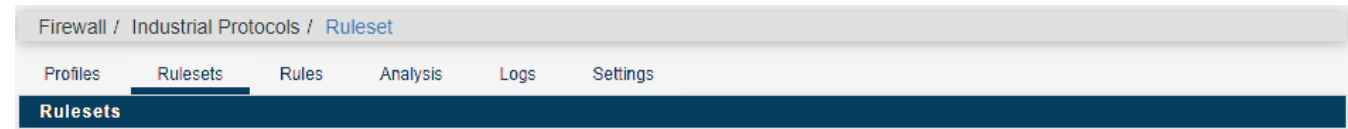
- **Action:** Whether this is passing (whitelist) or blocking (blacklist) packets
- **Name:** Name of the Industrial Profile
- **Description:** Optional description not used by the Anybus Defender
- **Actions:** This column has four buttons to edit, delete, copy, or test that profile respectively

Below the **Rules** table are these buttons:

- **Add New Profile:** Creates a new profile while setting the options and rules
- **Delete Selected Profiles:** Removes rules from the table

Rulesets

Overview



Firewall / Industrial Protocols / Rulesets Page

Rulesets are created by importing pre-created rulesets, or those exported from another Anybus Defender. They can also be created and rules can be added one at a time to the ruleset. After creating or importing a ruleset, the available rulesets are listed in the table explained below

The **Firewall / Industrial Protocols / Rulesets** page only has one section:

Rules

Profiles	Rulesets	Rules	Analysis	Logs	Settings
Rulesets					
Select All ☐					
Name		Description			
☐	ModbusCoilReg				
☐	Logix5000_Controller_v28_ReadOnly	Go Online and Allow Read Only			
☐	Logix5000_Controller_v28_Upload	Upload Controller into a Project File			
☐	Logix5000_Controller_v28_RunMode	Change the Controller to Run Mode			
☐	Logix5000_Controller_v28_ReadOnly_imported	Go Online and Allow Read Only			
☐	Logix5000_Controller_v28_Upload_imported	Upload Controller into a Project File			
☐	Logix5000_Controller_v28_RunMode_imported	Change the Controller to Run Mode			
☐	Logix5000_Controller_v28_EnableDisableMinorFaults	Change Controller Properties Advanced Settings and Run-Prog-Test Modes			
☐	Logix5000_Controller_v28_ProgramMode	Change the Controller to Program Mode			
☐	Logix5000_Controller_v28_TestMode	Change the Controller to Test Mode			
☐	Logix5000_Controller_v28_InhibitAutoFirmwareUpdate	Inhibit Automatic Firmware Updates			
☐	Logix5000_Controller_v28_RestrictCommsThroughSlot	Restrict Communications Through Specified Comm. Slot			
☐	Logix5000_Controller_v28_Time	Change Time and Time Sync in Controller Properties			
☐	Logix5000_Controller_v28_TimeSynch	Enable and Disable Time Synchronization			
☐	Logix5000_Controller_v28_CreateUDT	Create a User Defined Data Type while Online			
☐	Logix5000_Controller_v28_DeleteUDT	Delete and existing unused User Defined Data Type			
☐	Logix5000_Controller_v28_CreateRoutine	Create a routine in the controller			
☐	Logix5000_Controller_v28_TimeSyncAdvanced	View Advanced Time Synch Settings			
☐	Logix5000_Controller_v28_DeviceLevelRing	Controller Device Level Ring Properties			
☐	Logix5000_Controller_v28_ResetMemoryMax	Reset Maximum Memory used in Controller Properties			
☐	RSLinx_Controller_ChangeIPAddress	Change the IP Address Settings			
☐	S7_Online_Only				
Add New Ruleset Merge Selected Rulesets Delete Selected Rulesets Save Separator Import/Export Selected Rulesets					

Ruleset Table of the Firewall / Industrial Protocols / Rulesets Page

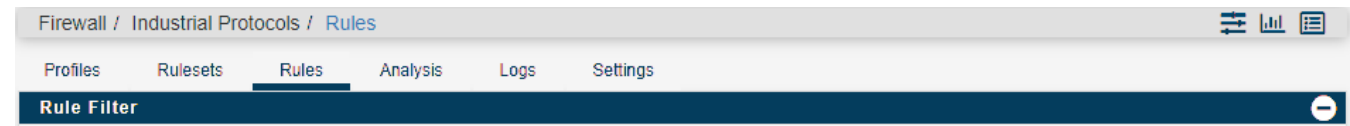
- Selection:** This is a checkbox to select the accompanying row
- The Select All checkbox** on the upper left of the table can be used to select all rows
- Name:** Name of the ruleset
- Description:** Optional description not used by the Anybus Defender
- Action:** This column has four buttons to edit , delete, delete with all linked rules, or duplicate the ruleset respectively

Below the **Rules** table, there are these six buttons:

- **Add New Ruleset:** Creates a new ruleset while setting the profile options and group rules
- **Merge Selected Rulesets:** Combines two or more rulesets
- **Delete Selected Rulesets:** Removes selected ruleset(s)
- **Save:** Commits any changes made to the selected rulesets
- **Separator:** Adds separator between rows. This allows rules to have section headers
- **Import/Export Selected Ruleset:** Opens two additional sections on a new page export or import ruleset(s) as XML. Encryption options are available for each

Rules

Overview



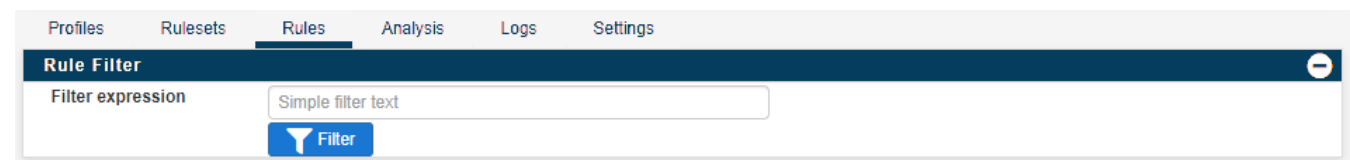
Firewall / Industrial Protocols / Rules Page

This section has [Top Banner Buttons](#)

Rules for the [Industrial Profile](#) represent the specific device functionality to affect. Each rule will have a protocol, and protocol packet type that can be blocked or allowed

The **Firewall / Industrial Protocols / Rules** page is divided into two sections:

Rules Filter



Rules Table of the Firewall / Industrial Protocols / Rules Page

- **Filter Expression:** Text field to filter the Rule table results
- **Filter:** Button to initiate the filter based on the **Filter Expression**

Below the **Rules Filter** table are these buttons:

- **Add New Rule:** Create a new rule
- **Delete Selected Rules:** Deletes all selected rules
- **Delete All Rules:*** Deletes all rules regardless of selection

Rules

Rules				
Select All ☐	Proto	Proto info	Description	
☐ 0	MODBUS	ADDR:1, FUNC: 6, REG: 1	Sample Register	 
☐ 1	MODBUS	ADDR:1, FUNC: 5, REG: 1	Sample Coil	 
☐ 2	MODBUS	ADDR:1, FUNC: 3, REG: 1	Reg 1 Read	 
☐ 3	CIP	Execute PCCC Service (0x4b) Class:0x64 Instance:0x1	Multi Use - Go Online - Read Only - Upload v28	 
☐ 4	CIP	Other(0x54) Class:0x6 Instance:0x1	Multi Use - Go Online - Read Only - Upload v28	 
☐ 5	CIP	RMW (Read/Modify/Write) Service (0x4e) Class:0x6 Instance:0x1	Multi Use - Go Online - Read Only - Upload v28	 
☐ 6	CIP	Set Attribute List (0x4) Class:0xac Instance:0x1	Multi Use - Go Online - Read Only - Upload v28	 
☐ 7	CIP	Other(0x54) Class:0x6 Instance:0x1	Multi Use - Go Online - Read Only - Upload v28	 
☐ 8	CIP	RMW (Read/Modify/Write) Service (0x4e) Class:0x6 Instance:0x1	Multi Use - Go Online - Read Only - Upload v28	 
☐ 9	CIP	Execute PCCC Service (0x4b) Class:0x64 Instance:0x1	Multi Use - Go Online - Read Only - Upload v28	 
☐ 10	CIP	Set Attribute List (0x4) Class:0xac Instance:0x1	Multi Use - Go Online - Read Only - Upload v28	 
☐ 11	CIP	Get Attribute List (0x3)	Multi Use - Go Online - Read Only - Upload v28	 
☐ 12	S7COMM_PLUS	AckData (0x03) OpCode: Response (0x32) Func: SetMultiVariables (0x0542)	(1) packets matched with this S7COMM PLUS data. (from packetcapture(6).pcap)	 
☐ 13	S7COMM_PLUS	AckData (0x03) OpCode: Request (0x31) Func: SetMultiVariables (0x0542)	(1) packets matched with this S7COMM PLUS data. (from packetcapture(6).pcap)	 
☐ 14	S7COMM_PLUS	AckData (0x03) OpCode: Response (0x32) Func: GetMultiVariables (0x054C)	(10) packets matched with this S7COMM PLUS data. (from packetcapture(6).pcap)	 
☐ 15	S7COMM_PLUS	AckData (0x03) OpCode: Request (0x31) Func: GetMultiVariables (0x054C)	(10) packets matched with this S7COMM PLUS data. (from packetcapture(6).pcap)	 
☐ 16	S7COMM_PLUS	AckData (0x03) OpCode: Response (0x32) Func: GetLink (0x0524)	(2) packets matched with this S7COMM PLUS data. (from packetcapture(6).pcap)	 
☐ 17	S7COMM_PLUS	AckData (0x03) OpCode: Request (0x31) Func: GetLink (0x0524)	(2) packets matched with this S7COMM PLUS data. (from packetcapture(6).pcap)	 
☐ 18	S7COMM_PLUS	AckData (0x03) OpCode: Response (0x32) Func: Invoke (0x056B)	(1) packets matched with this S7COMM PLUS data. (from packetcapture(6).pcap)	 
☐ 19	S7COMM_PLUS	AckData (0x03) OpCode: Request (0x31) Func: Invoke (0x056B)	(1) packets matched with this S7COMM PLUS data. (from packetcapture(6).pcap)	 

Rules Table of the Firewall / Industrial Protocols / Rules Page

- **Selection:** This is a checkbox to select the accompanying row
- **Proto:** Short for protocol. Displays which is used for the rule
- **Proto Info:** Short for protocol Information. Uses a **Class** and **Instance** designation for the specific traffic packet
- **Description:** Optional description not used by the Anybus Defender
- **Action:** This column has two buttons   to edit or delete the selected rule

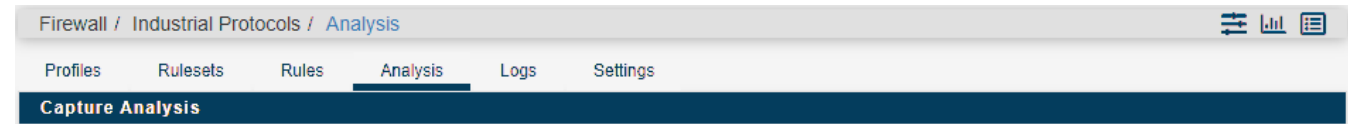
• If the rule count goes above 25 rows, page numbers will appear below the table (see image above)

Below the **Rules Filter** table are these buttons:

- **Add New Rule:** Creates a new rule
- **Delete Selected Rules:** Deletes all selected rules
- **Delete All Rules:** Deletes all rules regardless of selection

Analysis

Overview



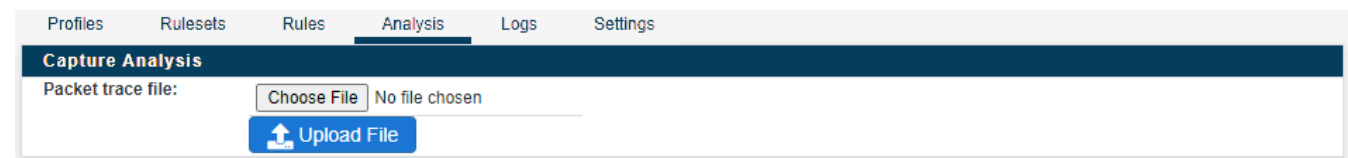
Firewall / Industrial Protocols / Analysis Page

This section has [Top Banner Buttons](#)

This section is for loading packet capture files and analyzing network packets for network troubleshooting, security analysis, performance monitoring, and protocol analysis

The **Firewall / Industrial Protocols / Analysis** page only has one section:

Capture Analysis



Capture Analysis Table of the Firewall / Industrial Protocols / Analysis Page

- **Packet Trace File:** Button used to set a network pathway upload to the capture analysis file
- **Upload File:** Button to initiate the file load from the specified network location

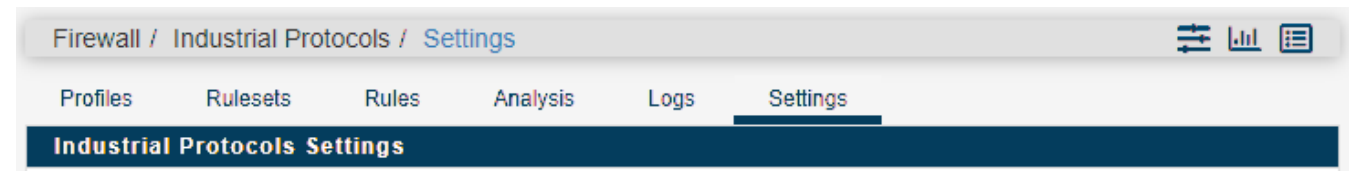
Logs

Overview

❗ Refer to the linked [Dashboard Overview](#) page for more information

Settings

Overview



Firewall / Industrial Protocols / Settings Page

This section is used to configure and customize various aspects of the protocol behavior, functionality, and integration within an industrial environment

The **Firewall / Industrial Protocols / Settings** page is divided into three sections:

Industrial Protocols Settings

Profiles	Rulesets	Rules	Analysis	Logs	Settings
Industrial Protocols Settings					
Enable blocking unknown traffic	☐ Enable blocking of unknown Industrial Protocols or other traffic Drop traffic that is not a known Industrial Protocol or other type of protocol.				
Enable sending a TCP RST	☐ Enable sending a TCP RST when a packet is blocked to reset the session on TCP Send a TCP RST packet to the host which packet got blocked to enable fast recovery on it!				
Enable debug logging	☐ Enable debugging of Industrial Protocols Enable functionality to enable verbose logging from the Industrial Protocols inspection.				

Industrial Protocol Settings Table of the Firewall / Industrial Protocols / Settings Page

- **Enabled Blocking Unknown Traffic:** A default off checkbox that, when enabled, drops traffic that is not a known Industrial Protocol or other type of protocol
- **Enable Sending a TCP RST:** A default off checkbox that, when enabled, sends a TCP RST packet to the host which packet got blocked to enable fast recovery reset the session on TCP
- **Enable Debug Logging:** A default off checkbox that, when enabled, allows functionality to enable verbose logging from the Industrial Protocols inspection

PCAP Blocked Packets

PCAP blocked packets	
Enable logging blocked traffic to PCAP	☐ Enable Industrial Protocols logging of blocked traffic Enable functionality to enable verbose logging from the Industrial Protocols inspection
PCAP log files	(No pcap logfile currently exists.)

PCAP Blocked Packets Table of the Firewall / Industrial Protocols / Settings Page

- **Enabled Logging Blocked Traffic to PCAP:** A default off checkbox that when enabled, allows functionality to enable verbose logging from the Industrial Protocols inspection
- **PCAP Log Files:** These files serve as a fundamental resource for capturing, storing, and analyzing network traffic data, providing detailed insights into network behavior, performance, security, and protocol interactions

PCAP Captured Packets

PCAP captured packets	
Enable capture of traffic to PCAP	☐ Enable Industrial Protocols capture of all traffic Enable functionality to capture all traffic going through the Industrial Protocols inspection
Captured PCAP files	(No pcap capture currently exists.)

 Save

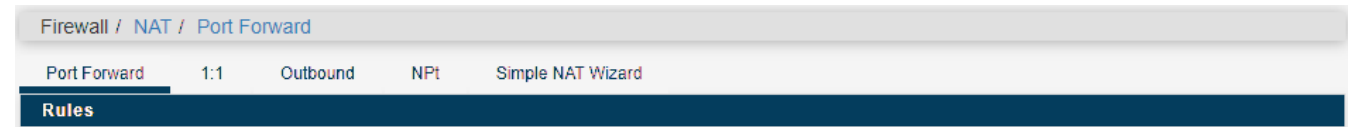
PCAP Captured Packets Table of the Firewall / Industrial Protocols / Settings Page

- **Enable Capture of Traffic to PCAP:** A default off checkbox that when enabled, allows functionality to capture all traffic going through the Industrial Protocols inspection
- **Captured PCAP Files:** These files are commonly used for network analysis, troubleshooting, security monitoring, protocol analysis, and forensic investigations

Below these three tables, there is a **Save:** button to confirm all selected changes and make them permanent

Port Forward

Overview

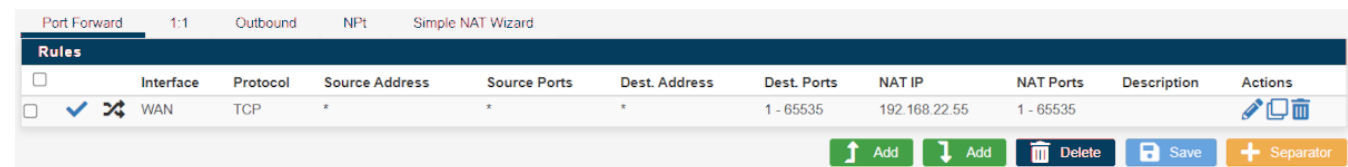


Firewall / NAT / Port Forward Page

This section provides a way to manage and configure the redirection of traffic within a network, facilitating efficient communication between internal devices and external networks or devices

The **Firewall / NAT / Port Forward** page only has one section:

Port Forward



Port Forward Rules Table of the Firewall / NAT / Port Forward Page

- **Selection:** This is a checkbox to select the accompanying row

i The checkbox on the upper left of the table can be used to select all rows

- ✓ **Enable/Disable:** Toggles enabling/disabling the row
- **Pass or Linked:** Indicator to show **Pass** ▶ or a **Linked Rule** ⚡

i This indicator is affected by the **Filter rule association** setting in the **Port Forward Edit Page**

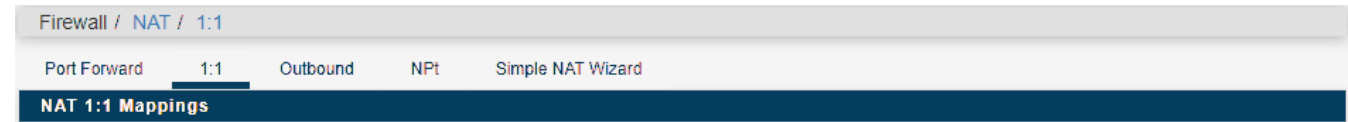
- **Interface:** The physical or logical connection point through which a device communicates with other devices or networks and is used to specify the source and destination of the forwarded traffic
- **Protocol:** The specific rules and format for communication between devices or applications
- **Source Address:** The IP address or range of IP addresses from which incoming traffic originates
- **Source Ports:** The port numbers from which incoming traffic originates
- **Dest. Address:** The IP address or network interface to which the forwarded traffic is directed
- **Dest. Ports:** The port numbers on the destination device or server to which incoming traffic is forwarded
- **NAT IP:** An IP address assigned to a device within a private network that is undergoing NAT (Network Address Translation) allowing multiple devices within that local network to share a single public IP address when accessing resources on the internet
- **NAT Ports:** The port numbers used in conjunction with NAT to manage the translation of IP addresses and port numbers between devices within a local network and external networks, typically the internet
- **Description:** This provides a human-readable label or description for the port forwarding rule
- **Actions:** This column has three buttons    to edit, duplicate, or delete the Port Forwards respectively

Below the Port Forward Rules table are these buttons:

- **Add Above:** Adds another rule above the selected row
- **Add Below:** Adds another rule below the selected row
- **Delete:** Removes the selected row
- **Save:** Saves the current rule order
- **Separator** Adds a visual separator on the **Port Forward** table with optional text

1:1

Overview

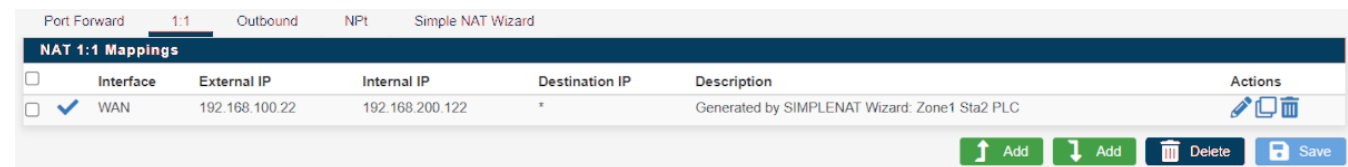


Firewall / NAT / 1:1 Page

This section is used in network address translation (NAT) configurations to establish a direct correspondence between public and private IP addresses. This mapping ensures that all traffic destined for a specific public IP address is directed to the corresponding private IP address, and vice versa

The **Firewall / NAT / 1:1** page only has one section:

NAT 1:1 Mappings



NAT 1:1 Mappings Table of the Firewall / NAT / 1:1 Page

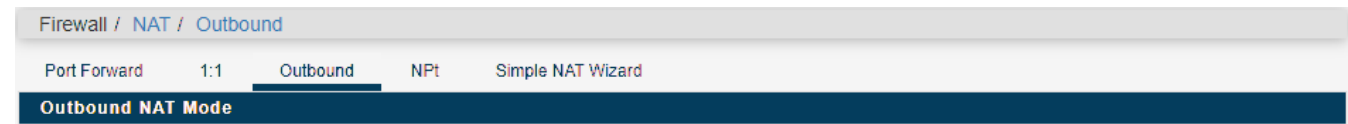
- **Selection:** This is a checkbox to select the accompanying row
- **Interface:** The [Interface](#) use for this mapping
- **External IP:** The external IP address
- **Internal IP:** The internal IP address
- **Description:** Optional description not used by the Anybus Defender
- **Actions:** This column has three buttons    to edit , copy, or delete the selected mapping respectively

Below the NAT 1:1 Mappings table as these buttons:

- **Add Above:** Adds another rule above the selected row
- **Add Below:** Adds another rule below the selected row
- **Delete:** Removes the selected row
- **Save:** Saves the mapping order of the rows

Outbound

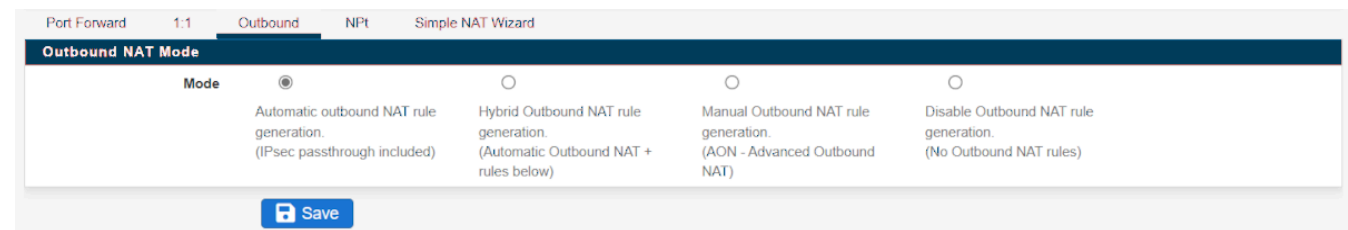
Overview



Firewall / NAT / Outbound Page

This section is used in network devices such as routers or firewalls to configure how outgoing traffic from the internal network is translated when it passes through the NAT device and reaches the external network. The **Firewall / NAT / Outbound** page is divided into three sections:

Outbound NAT Mode



Outbound NAT Mode Table of the Firewall / NAT / Outbound Page

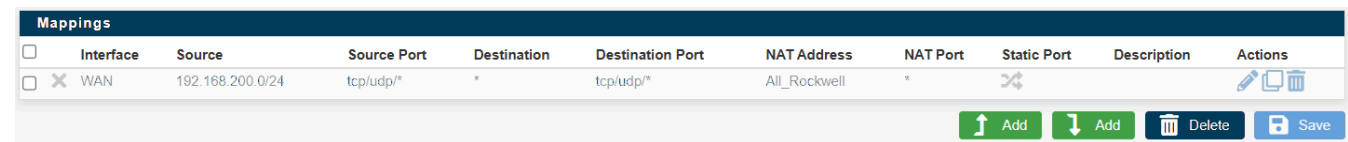
- **Mode:** This determines how a NAT-enabled router or firewall translates internal private IP addresses to external public IP addresses when devices within the local network initiate outbound connections to destinations on the internet

The four mode options are:

1. Automatic Outbound NAT rule generation
2. Hybrid Outbound NAT rule generation
3. Manual Outbound NAT rule generation
4. Disable Outbound NAT rule generation.

Below the NAT 1:1 Mapping table, there is a **Save** button to commit any changes made to the Outbound NAT Mode.

Mappings



Mapping Table of the Firewall / NAT / Outbound Page

- **Selection:** This is a checkbox to select the accompanying row

i The checkbox on the upper left of the table can be used to select all rows

- **Interface:** The [Interface](#) used in this mapping

- **Source:** The source network with subnet range
- **Source Port:** The source port or port range assigned
- **Destination:** The destination network
- **Destination Port:** The destination port or port range assigned
- **NAT Address:** The IP address that has been translated or modified by a NAT (Network Address Translation) device as part of the NAT process
- **NAT Port:** The port or port range used by the NAT translation
- **Static Port:** Flag for whether a port that is statically assigned
- **Description:** Optional description not used by the Anybus Defender
- **Actions:** The **Actions** column has three buttons    to edit the selected mapping, copy the selected mapping, or delete the selected mapping respectively

Below the Mappings table are these buttons:

- **Add Above:** Adds another rule above the selected row
- **Add Below:** Adds another rule below the selected row
- **Delete** Removes the selected row
- **Save:** Saves the mapping order of this table

Automatic Rules

Automatic Rules:								
Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description

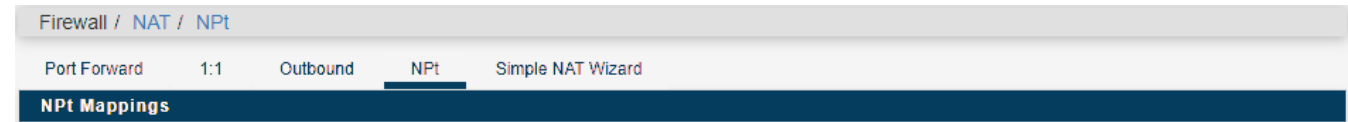
Automatic Rules Table of the Firewall / NAT / Outbound Page

- **Interface:** The [Interface](#) used in this mapping
- **Source:** The source network with subnet range
- **Source Port:** The source port or port range assigned
- **Destination:** The destination network
- **Destination Port:** The destination port or port range assigned
- **NAT Address:** The IP address that has been translated or modified by a NAT (Network Address Translation) device as part of the NAT process
- **NAT Port:** The port or port range used by the NAT translation
- **Static Port:** Flag for whether a port that is statically assigned
- **Description:** Optional description not used by the Anybus Defender

i If automatic outbound NAT is selected, a mapping is automatically generated for each interface's subnet (except WAN-type connections) and the rules on the "Mappings" section of this page are ignored. If manual outbound NAT is selected, outbound NAT rules will not be automatically generated and only the mappings specified on this page will be used. If hybrid outbound NAT is selected, mappings specified on this page will be used, followed by the automatically generated ones. If disable outbound NAT is selected, no rules will be used. If a target address other than an interface's IP address is used, then depending on the way the WAN connection is setup, a Virtual IP may also be required.

NPt

Overview

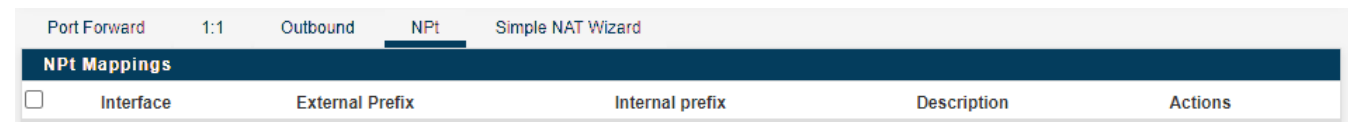


Firewall / NAT / NPt Page

This section is used for translating IP addresses and network prefixes to enable seamless communication between networks with different addressing schemes, facilitate IPv6 transition, and provide security and accessibility features such as port forwarding.

The **Firewall / NAT / NPt** page only has one section:

NPt Mappings



NPt Mappings of the Firewall / NAT / NPt

- **Selection:** This is a checkbox to select the accompanying row
- **External Prefix:** This refers to the range of external or public IP addresses to which internal or private IP addresses are translated
- **Internal Prefix:** refers to the range of internal or private IP addresses that are subject to translation when communicating with external networks
- **Description:** This provides a human-readable label or annotation for each mapping entry and aids in managing, organizing, and troubleshooting the NPt configuration
- **Actions:** This column has three buttons    to edit , copy, or delete the selected rule respectively

Below the NPt Mappings table, there are these four buttons:

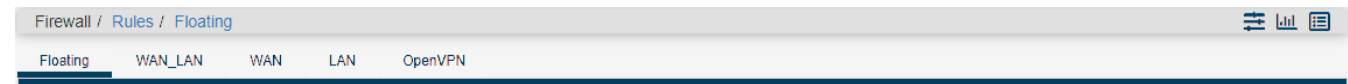
- **Add Above** button to [Add an NPt Rule](#) above the selected row
- **Add Below** button to [Add an NPt Rule](#) below the selected row
- **Delete** button to remove the selected row
- **Save** button to keep any changes made to the NPt list

Simple NAT Wizard

❗ Refer to the [Simple NAT Wizard](#) page in the **Getting Started** for more information

Floating

Overview



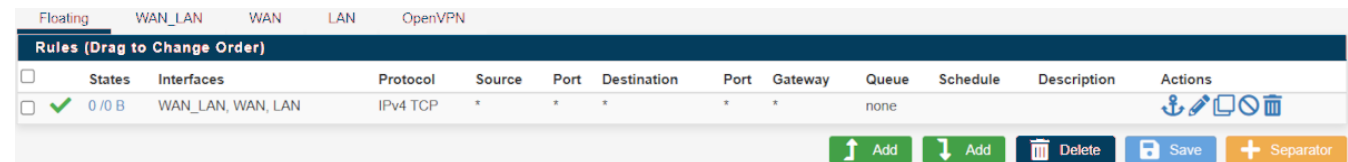
Firewall / Rules / Floating Page

This section has [Top Banner Buttons](#)

This section in a firewall is used for defining rules that have higher priority than the standard rules in the firewall's rule set. These rules are typically evaluated before the regular rules and can apply to multiple interfaces or zones

The **Firewall / Rules / Floating** page only has one section:

Floating Rules



Rules Table of the Firewall / Rules / Floating Page

- **Selection:** This is a checkbox to select the accompanying row
- **States:** This field will contain an expanded window showing the tracking ID, the evaluations, packets, bytes, the number of states, and the number of state creations
- **Interface:** The [Interfaces](#) used in this rule
- **Protocol:** The network protocol or communication protocol that the rule applies to. * signifies any protocol
- **Source:** The source type used. Can be **any** (uses * character), **single host**, **alias**, **network**, etc. See the [Add Interface Rule Procedure](#) for more details
- **Port:** The source port or port range used. * signifies any port
- **Destination:** The destination type used. Can be **any** (uses * character), **single host**, **alias**, **network**, etc. See the [Add Interface Rule Procedure](#) for more details
- **Port:** The destination port or port range used. * signifies any port
- **Gateway:** The router through which traffic matching the rule will be forwarded. * signifies any gateway
- **Queue:** Shows Acknowledge Queue if there is a selected queue
- **Schedule:** This specifies a time-based schedule or timetable that determines when the rule is active or enforced, which allows administrators to define specific periods during which the rule should be applied
- **Description:** Optional description not used by the Anybus Defender
- **Actions:** This column has five buttons  to either **move** the selected floating rules up or down, edit, copy, disable, or delete the rules respectively

Below the Floating Rules table are these buttons:

- **Add Above:** Adds another rule above the selected row
- **Add Below:** Adds another rule below the selected row

- **Save:** Keeps any changes made to the selected row
- **Separator:** to set a visual element to distinguish between different sections or groups.

WAN_LAN

Overview



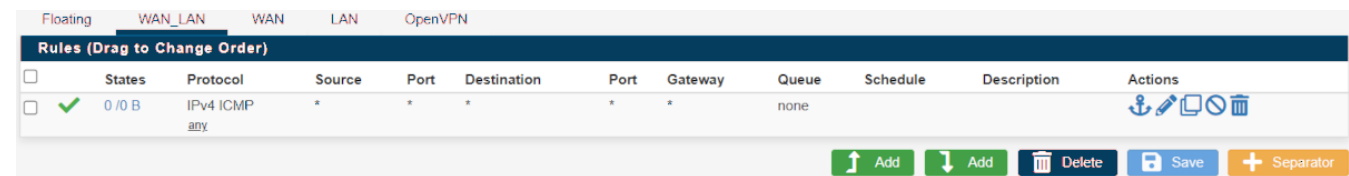
Firewall / Rules / WAN_LAN Page

This section has [Top Banner Buttons](#)

This section in a firewall is used for defining rules that are evaluated on both the WAN and LAN side interfaces

The **Firewall / Rules / WAN_LAN** page only has one section:

WAN_LAN Rules



Rules Table of the Firewall / Rules / WAN_LAN Page

- **Selection:** This is a checkbox to select the accompanying row
- i** The checkbox on the upper left of the table can be used to select all rows
- **States:** This field will contain an expanded window showing the tracking ID, the evaluations, packets, bytes, the number of states, and the number of state creations
 - **Protocol:** The network protocol or communication protocol that the rule applies to. * signifies any protocol
 - **Source:** The source type used. Can be **any** (uses * character), **single host**, **alias**, **network**, etc. See the [Add Interface Rule Procedure](#) for more details
 - **Port:** The source port or port range used. * signifies any port
 - **Destination:** The destination type used. Can be **any** (uses * character), **single host**, **alias**, **network**, etc. See the [Add Interface Rule Procedure](#) for more details
 - **Port:** The destination port or port range used. * signifies any port
 - **Gateway:** The router through which traffic matching the rule will be forwarded. * signifies any gateway
 - **Queue:** Shows Acknowledge Queue if there is a selected queue
 - **Schedule:** This specifies a time-based schedule or timetable that determines when the rule is active or enforced, which allows administrators to define specific periods during which the rule should be applied
 - **Description:** Optional description not used by the Anybus Defender
 - **Actions:** This column has five buttons  to either **move** the selected rules up or down, edit, copy, disable, or delete the rules respectively

Below the **WAN_LAN** Rules table are these buttons:

- **Add Above:** Adds another rule above the selected row
- **Add Below:** Adds another rule below the selected row
- **Delete** Removes the selected row
- **Save:** Keeps any changes made to the selected row.
- **Separator:** to set a visual element to distinguish between different sections or groups

WAN

Overview

Floating	WAN_LAN	WAN	LAN	OpenVPN							
Rules (Drag to Change Order)											
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓ 0 / 0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN wizard	
☐	✓	IPv4 TCP	*	*	This Firewall	443 (HTTPS)	*	none		Allow WAN management	
☐	✓	IPv4 ICMP	*	*	This Firewall	*	*	none		Allow WAN pings	
☐	✓	IPv4 *	*	*	192.168.200.122	*	*	none		Generated by SIMPLenAT Wizard: Zone1 Sta2 PLC	
Add Add Delete Save Separator											

Firewall / Rules / WAN Page

This section has [Top Banner Buttons](#)

This section has sets of rules or configurations within the firewall that specifically govern traffic entering or exiting the Wide Area Network (WAN) interface

The **Firewall / Rules / WAN** page only has one section:

WAN Rules

Floating	WAN_LAN	WAN	LAN	OpenVPN							
Rules (Drag to Change Order)											
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✔ 0 / 0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN wizard	   
☐	✔	IPv4 TCP	*	*	This Firewall	443 (HTTPS)	*	none		Allow WAN management	   
☐	✔	IPv4 ICMP	*	*	This Firewall	*	*	none		Allow WAN pings	   
☐	✔	IPv4 *	*	*	192.168.200.122	*	*	none		Generated by SIMPLenAT Wizard: Zone1 Sta2 PLC	   

Rules Table of the Firewall / Rules / WAN Page

- **Selection:** This is a checkbox to select the accompanying row

The checkbox on the upper left of the table can be used to select all rows

- **States:** This field will contain an expanded window showing the tracking ID, the evaluations, packets, bytes, the number of states, and the number of state creations
- **Protocol:** The network protocol or communication protocol that the rule applies to. * signifies any protocol
- **Source:** The source type used. Can be **any** (uses * character), **single host**, **alias**, **network**, etc. See the [Add Interface Rule Procedure](#) for more details
- **Port:** The source port or port range used. * signifies any port
- **Destination:** The destination type used. Can be **any** (uses * character), **single host**, **alias**, **network**, etc. See the [Add Interface Rule Procedure](#) for more details
- **Port:** The destination port or port range used. * signifies any port
- **Gateway:** The router through which traffic matching the rule will be forwarded. * signifies any gateway
- **Queue:** Shows Acknowledge Queue if there is a selected queue
- **Schedule:** This specifies a time-based schedule or timetable that determines when the rule is active or enforced, which allows administrators to define specific periods during which the rule should be applied
- **Description:** Optional description not used by the Anybus Defender

- **Actions:** This column has five buttons  to either **move** the selected rules up or down, edit, copy, disable, or delete the rules respectively

Below the **WAN** Rules table are these buttons:

- **Add Above:** Adds another rule above the selected row
- **Add Below:** Adds another rule below the selected row
- **Delete** Removes the selected row
- **Save:** Keeps any changes made to the selected row.
- **Separator:** to set a visual element to distinguish between different sections or groups

LAN

Overview



Firewall / Rules / LAN Page

This section has [Top Banner Buttons](#)

This section has sets of rules or configurations within the firewall that specifically govern traffic flow within the Local Area Network (LAN) segment

The **Firewall / Rules / LAN** page only has one section:

LAN Rules

Floating	WAN_LAN	WAN	LAN	OpenVPN							
Rules (Drag to Change Order)											
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	1 / 2.93 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
☐	0 / 36 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
☐	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	
☐		IPv4 *	192.168.200.122	*	*	*	*	none		Generated by SIMPLenAT Wizard: Zone1 Sta2 PLC	
Add Add Delete Save Separator											

Rules Table of the Firewall / Rules / LAN Page

- **Selection:** This is a checkbox to select the accompanying row

The checkbox on the upper left of the table can be used to select all rows

- **States:** This field will contain an expanded window showing the tracking ID, the evaluations, packets, bytes, the number of states, and the number of state creations
- **Protocol:** The network protocol or communication protocol that the rule applies to. * signifies any protocol
- **Source:** The source type used. Can be **any** (uses * character), **single host**, **alias**, **network**, etc. See the [Add Interface Rule Procedure](#) for more details
- **Port:** The source port or port range used. * signifies any port
- **Destination:** The destination type used. Can be **any** (uses * character), **single host**, **alias**, **network**, etc. See the [Add Interface Rule Procedure](#) for more details
- **Port:** The destination port or port range used. * signifies any port
- **Gateway:** The router through which traffic matching the rule will be forwarded. * signifies any gateway
- **Queue:** Shows Acknowledge Queue if there is a selected queue
- **Schedule:** This specifies a time-based schedule or timetable that determines when the rule is active or enforced, which allows administrators to define specific periods during which the rule should be applied
- **Description:** Optional description not used by the Anybus Defender
- **Actions:** This column has five buttons to either **move** the selected rules up or down, edit, copy, disable, or delete the rules respectively

Below the **LAN Rules** table are these buttons:

- **Add Above:** Adds another rule above the selected row
- **Add Below:** Adds another rule below the selected row
- **Delete** Removes the selected row
- **Save:** Keeps any changes made to the selected row.
- **Separator:** to set a visual element to distinguish between different sections or groups

OpenVPN

Overview



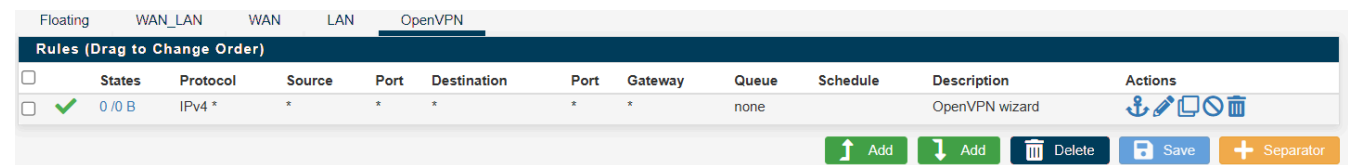
Firewall / Rules / OpenVPN Page

This section has [Top Banner Buttons](#)

This section has sets of rules or configurations within the firewall that are specifically related to managing OpenVPN connections

The **Firewall / Rules / OpenVPN** page only has one section:

OpenVPN Rules



Rules Table of the Firewall / Rules / OpenVPN Page

- **Selection:** This is a checkbox to select the accompanying row
- i** The checkbox on the upper left of the table can be used to select all rows
- **States:** This field will contain an expanded window showing the tracking ID, the evaluations, packets, bytes, the number of states, and the number of state creations
 - **Protocol:** The network protocol or communication protocol that the rule applies to. * signifies any protocol
 - **Source:** The source type used. Can be **any** (uses * character), **single host**, **alias**, **network**, etc. See the [Add Interface Rule Procedure](#) for more details
 - **Port:** The source port or port range used. * signifies any port
 - **Destination:** The destination type used. Can be **any** (uses * character), **single host**, **alias**, **network**, etc. See the [Add Interface Rule Procedure](#) for more details
 - **Port:** The destination port or port range used. * signifies any port
 - **Gateway:** The router through which traffic matching the rule will be forwarded. * signifies any gateway
 - **Queue:** Shows Acknowledge Queue if there is a selected queue
 - **Schedule:** This specifies a time-based schedule or timetable that determines when the rule is active or enforced, which allows administrators to define specific periods during which the rule should be applied
 - **Description:** Optional description not used by the Anybus Defender
 - **Actions:** This column has five buttons  to either **move** the selected rules up or down, edit, copy, disable, or delete the rules respectively

Below the **OpenVPN** Rules table are these buttons:

- **Add Above:** Adds another rule above the selected row
- **Add Below:** Adds another rule below the selected row
- **Delete** Removes the selected row
- **Save:** Keeps any changes made to the selected row.
- **Separator:** to set a visual element to distinguish between different sections or groups

Schedules

Overview

Firewall / Schedules

Schedules

Firewall / Schedules / Schedules Page

This section is used for defining time-based schedules or timetables that determine when specific firewall rules or policies should be active or enforced

The **Firewall / Schedules / Schedules** page only has one section:

Schedules

Schedules			
Name	Range: Date / Times / Name	Description	Actions
Maint	April 30; 1:00-10:59		 
			 Add

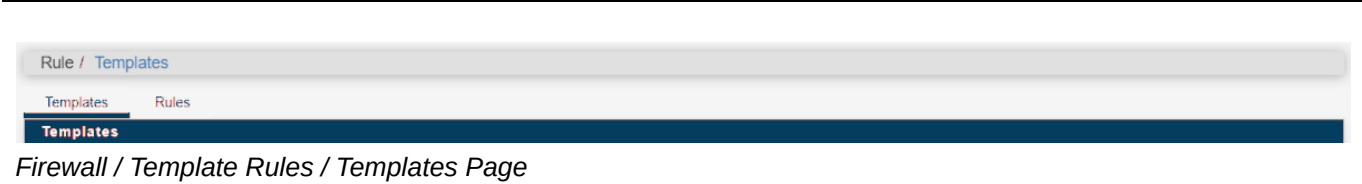
Schedules Table of the Firewall / Rules / Schedules Page

- **Name:** This field serves to provide a human-readable label or reference for each schedule, making it easier for administrators to identify and manage schedules effectively
- **Range: Date/Times/Name:** This field provides the date, time, and name for each scheduling event
- **Description:** This field provides a textual explanation for each scheduling event
- **Actions:** The **Actions** button has two buttons   to either edit the selected schedule or delete the selected schedule respectively

Below the **Schedules** table, there is the **Save:** button to confirm all selected changes and make them permanent

Templates

Overview



This section provides pre-configured firewall rule sets that users can apply to their firewall configurations

The **Firewall / Template Rules / Templates** page only has one section:

Templates



Templates Table of the Firewall / Template Rules / Template Page

- **Selection:** This is a checkbox to select the accompanying row
- **Name:** A user-defined label or identifier assigned to a template rule on the templates table
- **Description:** This refers to a field that provides additional information or context about each template on the templates table
- **Actions:** The **Actions** column has four buttons  to edit the selected template, delete the selected template, delete the selected template with all linked rules, and copy the selected template respectively

Below the **Template** table are these buttons:

- **Add New Template:** Sets template options and rules for a new entry on the table
- **Delete Selected Templates:** Removes a selected template

Rules

Overview

📌 This navigates directly to the [Rules Section](#) page

By Interface

Overview

Firewall / Traffic Shaper / By Interface

By Interface

By Queue

Limiters

Wizards

Firewall / Traffic Shaper / By Interface Page

This section has [Top Banner Buttons](#)

This section has a bandwidth management system to define and enforce traffic shaping policies organized by the interface type. The **Firewall / Traffic Shaper / By Interface** page only has one section:

By Interface

By Interface

By Queue

Limiters

Wizards

WAN

LAN

OPT1

By Interface Table of the Firewall / Traffic Shaper / By Interface Page

- **WAN:** This stands for Wide Area Network and refers to a network that connects devices over a broad geographical area
- **LAN:** This stands for Local Area Network and refers to a network that connects devices within a limited geographic area
- **OPT1:** This refers to an optional network interface in networking configurations

By Interface

By Queue

Limiters

Wizards

WAN

LAN

OPT1

Enable/Disable

☐ Enable/disable discipline and its children

Name

wan

Scheduler Type

HFSC

Changing this changes all child queues! Beware information can be lost.

Bandwidth

Mbit/s

Queue Limit

TBR Size

Adjusts the size, in bytes, of the token bucket regulator. If not specified, heuristics based on the interface bandwidth are used to determine the size.

Save

Add new Queue

Disable shaper on interface

WAN Interface Table of the Firewall / Traffic Shaper / By Interface Page

- **Enable/Disable:** A default off checkbox that when checked enables the discipline and its children
- **Name:** This refers to the specific interface type and will be either WAN, LAN, or OPT1 depending on the selected section on the left
- **Scheduler Type:** A dropdown box allowing changes to the type of scheduler
 - **HFSC:** Hierarchical Fair Service Curve
 - **CBQ:** Class Based Queueing
 - **FAIRQ:** Fair Queueing
 - **CODELQ:** Controlled Delay Queue
 - **PRIQ:** Priority Queueing

⚠ Changing the scheduler type changes all child queues! Information can be lost!

- **Bandwidth:** A numerical text field used to set the maximum data transfer rate of the network connection
- **Unit of Measure:** A dropdown box to set the unit size for the data transfer value
- **Queue Limit:** A numerical text field to set the maximum limit
- **TBR Size:** The Token Bucket Rate refers to the capacity of the token bucket, which is a fundamental component of token bucket algorithms used in traffic shaping and policing.

Below the select Interface Table are these buttons:

- **Save:** Keeps any changes made to the selected row
- **Add New Queue:** Creates a new Queue entry
- **Disable Shaper on Interface:** Suspends the traffic shaper for this interface type.

❗ The tree on the left navigates through the queues. Buttons at the bottom represent queue actions and are activated accordingly

By Queue

Overview

Firewall / Traffic Shaper / By Queue

By Interface

By Queue

Limiters

Wizards

Firewall / Traffic Shaper / By Queue Page

This section has [Top Banner Buttons](#)

This section has a bandwidth management system to define and enforce traffic shaping policies organized by queue type. The **Firewall / Traffic Shaper / By Queue** page only has one section:

By Queue

By Interface

By Queue

Limiters

Wizards

No Queue Configured/Selected

By Queue Table of the Firewall / Traffic Shaper / By Queue Page

Limiters

Overview

Firewall / Traffic Shaper / Limiters

By Interface

By Queue

Limiters

Wizards

Firewall / Traffic Shaper / Limiters Page

This section has [Top Banner Buttons](#)

This section has options to control and manage the bandwidth of network traffic to meet specific requirements and priorities The **Firewall / Traffic Shaper / Limiters** page only has one section:

Limiters

By Interface

By Queue

Limiters

Wizards

+ New Limiter

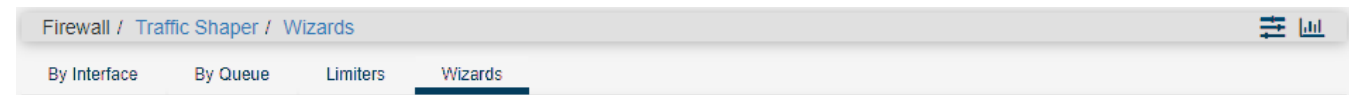
Below the **Limiters** table is the **New Limiter** button to set the limiter and queue options as well as the set advanced options.

❗ The tree on the left navigates through the limiters. Buttons at the bottom represent limiter actions and are activated accordingly.

Wizards

Overview

This wizard will provide guidance through [Setting up the Traffic Shaper](#) for the Anybus Defender



Firewall / Traffic Shaper / Wizards Page

This section has [Top Banner Buttons](#)

This section has tools within a traffic shaping configuration interface that guide users through the process of setting up traffic shaping policies and configurations.

The **Firewall / Traffic Shaper / Wizards** page only has one section:

Wizards

By Interface	By Queue	Limiters	Wizards
Traffic Shaper Wizards			
Multiple Lan/Wan	traffic_shaper_wizard_multi_all.xml		
Dedicated Links	traffic_shaper_wizard_dedicated.xml		

Virtual IPs

Overview

Firewall / Virtual IPs

Virtual IP Address

Firewall / Virtual IPs / Virtual IP Address Page

The **Firewall / Virtual IPs / Virtual IP Address** page only has one section:

Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
192.168.100.22/32	WAN	IP Alias	Generated by SIMPLENAT Wizard: Zone1 Sta2 PLC	 
				 Add

Virtual IP Address Table of the Firewall / Virtual IPs / Template Page

- **Virtual IP Address:** This is an IP address that is not associated with a specific physical network interface but instead is mapped to a virtual resource, such as a virtual server, a cluster of servers, or a network service
- **Interface:** This field indicates the network interface or network adapter with which the virtual IP address is associated or bound
- **Type:** This refers to the type or purpose of the virtual IP address
- **Description:** This refers to a field that provides additional information or context about each virtual IP on the virtual IP table
- **Actions:** The **Actions** column has two buttons   to either edit the selected template or delete the selected template respectively

Below the **Virtual IPs** table is the + **Add** button to configure the next virtual IP to be added to the table.

❗ The virtual IP addresses defined on this page may be used in NAT mappings. Check the status of Hot Standby Virtual IPs and interfaces here.

Services Overview

Overview

Services are functionality essential to the Anybus Defender. They include:

- [Asset Management](#)
- [Captive Portal](#)
- [DHCP Server](#)
- [DNS Forwarder](#)
- [DNS Resolver](#)
- [IGMP Proxy](#)
- [NTP](#)
- [SNMP](#)

Detected Assets

Overview

Package / Asset Detection

Detected Assets Saved Assets Settings

	Interface	MAC	MAC Vendor	IP	Description
0	LAN	00:0C:29:31:9A:4C	VMware, Inc.	192.168.200.2	
1	LAN	00:1D:9C:C7:83:7B	Rockwell Automation	192.168.200.202	Vendor: Rockwell Automation/Allen-Bradley (1) Product Name: 1756-EN2T/D Serial Number: 0x00afd21f Device Type: Communications Adapter (12) Product Code: 166 Revision: 11.2 Device IP: 192.168.200.202
2	LAN	00:0E:C6:CA:D6:75	ASIX ELECTRONICS CORP.	192.168.200.222	Guess accuracy: 85% Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2
3	LAN	70:B3:D5:B5:E0:17	Dynics Inc.	192.168.200.1	2.3.4-RELEASE

Services / Asset Management / Detected Assets Showing Detected Devices

Asset Management scans hosts on the network and identifies OS and/or Industrial Protocol information. The **Detected Assets** tab is a table of all detected assets for an interface(s) defined in the [Settings](#) tab

By default, the **Asset Management** is not installed on the Anybus Defender. Use the [Package Manager](#) to install the **AssetMgmt** package

Asset Table

On top left of the **Detected Assets** table, are these buttons:

- **(Add Refresh Icon):** Re-scans the configured interface(s) adding or removing devices based on detected changes
- **(Add Save Icon):** Saves a snapshot of the detected assets. The snap shot can be downloaded and more in the [Save Assets](#) tab

Within the **Detected Assets** table, the information displayed is as follows:

- **Interface:** The interface of this devices
- **MAC:** MAC address of devices
- **MAC Vendor:** Vendor information if available
- **IP:** IP address of the device
- **Description:** Specific information about the device if available

Saved Assets

Overview

Package / Asset Detection

Detected Assets Saved Assets Settings



	Interface	MAC	MAC vendor	IP	Description
0	LAN	00:0C:29:31:9A:4C	VMware, Inc.	192.168.200.2	
1	LAN	00:1D:9C:C7:83:7B	Rockwell Automation	192.168.200.202	Guess accuracy: 94% TP-LINK TL-R478+ router
2	LAN	00:0E:C6:CA:D6:75	ASIX ELECTRONICS CORP.	192.168.200.222	Guess accuracy: 85% Microsoft Windows XP SP2
3	LAN	70:B3:D5:B5:E0:17	Dynics Inc.	192.168.200.1	2.3.4-RELEASE

Services / Asset Management / Saved Assets Showing Saved Devices

Asset Management scans hosts on the network and identifies OS and/or Industrial Protocol information. The **Saved Assets** tab is a table of all saved assets for an interface(s). Saving assets is done in the [Detected Assets](#) tab when the **Save** operation is performed

❗ By default, the **Asset Management** is not installed on the Anybus Defender. Use the [Package Manager](#) to install the **AssetMgmt** package

Asset Table

On top left of the **Saved Assets** table, are these buttons:

- **(Add Clear Icon):** Clears all currently saved assets
- **(Add Download Icon):** Downloads the ALL saved assets as an xml file
- **(Add circle with down arrow icon):** Downloads only newly-discovered assets
- **(Add circle with up arrow icon):** Checks the Asset storage database for proper functionality

Within the **Saved Assets** table, the information displayed is as follows:

- **Interface:** The interface of this devices
- **MAC:** MAC address of devices
- **MAC Vendor:** Vendor information if available
- **IP:** IP address of the device
- **Description:** Specific information about the device if available

❗ Guess accuracy may appear here if the detect algorithm cannot get 100% accuracy on the device detected. Increasing the [Scan Speed in the [Settings](#) tab can help increase accuracy

Settings

Overview

Package / Asset Detection Settings

Detected Assets

Saved Assets

Settings

AssetsForm

Enable

☒ Enable Asset scanning...

Interface

WAN

LAN

Extra Scans

Specify any extra subnet you want included in the scan. Host responding to ICMP ECHO will be considered only. NOTE: These entries add overhead since every iteration they will be scanned.

Exclude hosts

Comma separated list of hosts to exclude from scan on the selected network interface.

Advanced

Scan speed

Fast

How thorough should the asset scan be.

Period

Number of minutes to elapse before re-scanning for assets. Default interval is: 30

Save

Services / Asset Management / Settings

These are the settings used for [Detected Asset](#) and [Saved Asset](#) devices

❗ By default, the **Asset Management** is not installed on the Anybus Defender. Use the [Package Manager](#) to install the **AssetMgmt** package

The **Services / Asset Management / Settings** page is divided into these sections:

AssetsForm

- **Enable:** Enables/Disables actively scanning for assets
- **Interface:** Selects the interface to scan for devices

❗ Use the **Ctrl** to select multiple individual or the **Shift** key for a range of interfaces

- **Extra Scans:** Allows specifying an extra subnet to include in the scan

❗ Host responding to ICMP ECHO will be considered only

❗ These entries add overhead since every iteration they will be scanned

- **Exclude hosts:** A comma-separated list of hosts to exclude from the scan

Advanced

- **Scan speed:** Dropdown to set how thorough the asset scan will be: **Fast**, **Medium**, or **Slow**

❗ Slower scans will increase the scan time but increase the accuracy percentage of device information shown on the [Saved Assets](#)

- **Period:** Number of minutes between asset scans. If left blank, 30 minutes will be used

Captive Portal

Overview

Services / [Captive Portal](#)

Zone	Interfaces	Number of users	Description	Actions
Acme_Login		0		 

 Add

Services / Captive Showing Portal Zone

This section has [Top Banner Buttons](#)

Captive Portal creates authentication requirements for users to access the internet. Authentication can be user/password, a voucher, or click-through agreement

The **Services / Captive Portal** page is divided into these sections:

Captive Portal Zones

Within the **Captive Portal Zones** table, the information displayed is as follows:

- **Zone:** Name of the captive portal zone
- **Interfaces:** Which interface(s) the portal is active on
- **Number of users:** Total count of users configured to access the portal
- **Description:** Specific information about the portal zone if available
- **Actions:** Buttons for:
 - **(Pencil icon):** Edit the portal zone
 - **(garbage icon):** Delete the portal zone The **Add** button allows for creation and [Configuring](#) a portal zone

Configuration

Overview

Services / Captive Portal / Acme_Login / Configuration

ConfigurationMACsAllowed IP AddressesAllowed HostnamesVouchersHigh AvailabilityFile Manager

Captive Portal Configuration

Enable

☐ Enable Captive Portal

Description

A description may be entered here for administrative reference (not parsed).

Save

Don't forget to enable the DHCP server on the captive portal interface! Make sure that the default/maximum DHCP lease time is higher than the hard timeout entered on this page. Also, the DNS Forwarder or Resolver must be enabled for DNS lookups by unauthenticated clients to work.

Services / Captive Portal / Configuration

This section has [Top Banner Buttons](#)

Captive Portal configuration allows to enable/disable the captive portal zone and add an option description

ⓘ Remember to enable the DHCP server on the captive portal interface. Make sure that the default/maximum [DHCP Lease Time](#) is higher than the hard timeout entered on this page. Also, the DNS Forwarder or [Resolver](#) must be enabled for DNS lookups by unauthenticated clients to work

MACs

Overview

Services / Captive Portal / Acme_Login / MACs

Configuration	MACs	Allowed IP Addresses	Allowed Hostnames	Vouchers	High Availability	File Manager
Action	MAC address				Description	Actions
✓ Pass	00:0e:c6: [mask icon]				JJone_PC	[pencil icon] [trash icon]
						+ Add

Services / Captive Portal/ MACs Showing Sample MAC Device

This section has [Top Banner Buttons](#)

Adding MAC addresses here allows them to be **bypassed** from the captive portal automatically

❗ These MACs can also be blocked from ANY access as explained below

MACs Table

Within the **MACs** table, the information displayed is as follows:

- **Action:** Can be set to **Pass** or **Block** packets from the MAC
- **MAC Address:** The MAC of the device

❗ It is also possible to add a mask value (/24 for example) to allow all phones of a certain manufacturer to bypass the portal

- **Description:** Specific optional information about the MAC
- **Actions:** Buttons for:
 - **(Pencil icon):** Edit the MAC
 - **(garbage icon):** Delete the MAC

Below the table is an **Add** button to add new MACs. The resulting MAC edit page will load:

Edit MAC Address Rules

Action	Pass	
Choose what to do with packets coming from this MAC address.		
MAC Address	00:0e:c6:bb:76:33	Copy My MAC
6 hex octets separated by colons ⓘ		
Description	AGibbs_PC	
A description may be entered here for administrative reference (not parsed)		
Bandwidth up	100	
Enter an upload limit to be enforced on this MAC in Kbit/s		
Bandwidth down	500	
Enter a download limit to be enforced on this MAC in Kbit/s		
Save		

Services / Captive Portal/ MACs / Edit Page

Edit MAC Address Rules

- **Action:** Set to **Pass** or **Block** packets from the MAC
- **MAC Address:** The 6 octet MAC address of the device. The **Copy MAC** button can paste in the current device's MAC automatically

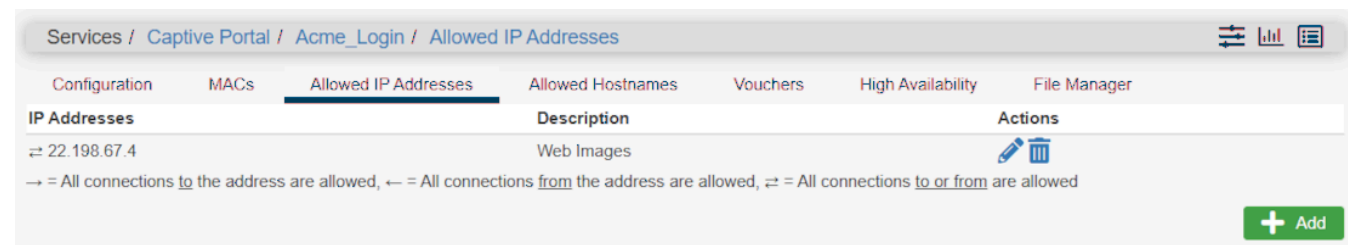
❗ Mask values (such a /24) can be used to allow all phones of a certain manufacturer to bypass the portal

- **Description:** Specific optional information about the MAC
- **Bandwidth up:** Allowed upload limit on this MAC device. If left blank, it will be unlimited
- **Bandwidth up:** Allowed download limit on this MAC device. If left blank, it will be unlimited

The **Save** button will save the current MAC address and add it to the **MACs** table

Allowed IPs

Overview



Services / Captive Portal/ Allowed IP Addresses Showing Sample IP Address

This section has [Top Banner Buttons](#)

Adding IP addresses here allows them to be **bypassed** from the captive portal automatically. This could be used when outside images or files are required on the captive portal web page

Allowed IP Addresses Table

Within this table, the information displayed is as follows:

- **IP Addresses:** The IP address(s) to be allowed. To the left of the IP address are arrows to signify:
 - **(Right Arrow icon):** All connections **to** the address are allowed
 - **(Left Arrow Icon):** All connections **from** the address are allowed
 - **(Left/Right Arrow Icon):** All connections **to** and **from** are allowed
- **Description:** Specific optional information about the IP address
- **Actions:** Buttons for:
 - **(Pencil icon):** Edit the IP addresses
 - **(garbage icon):** Delete the IP addresses

Below the table is an **Add** button to add new IPs. The resulting IP Address edit page will load:

A screenshot of the 'Edit Captive Portal IP Rule' form. The breadcrumb trail at the top reads 'Services / Captive Portal / Acme_Login / Allowed IP Addresses / Edit'. The form has a dark blue header with the title 'Edit Captive Portal IP Rule'. It contains several input fields: 'IP Address' with the value '22.198.67.4' and a dropdown menu set to '32'; 'Description' with the value 'Web Images' and a note 'Enter a description here for reference only. (Not parsed)'; 'Direction' with a dropdown menu set to 'Both' and a note 'Use "From" to always allow access to an address through the captive portal (without authentication). Use "To" to allow access from all clients (even non-authenticated ones) behind the portal to this IP.'; 'Bandwidth up' and 'Bandwidth down' fields with notes 'Enter an upload limit to be enforced on this address in Kbit/s' and 'Enter a download limit to be enforced on this address in Kbit/s' respectively. At the bottom of the form is a blue 'Save' button with a floppy disk icon.

Services / Captive Portal/ IP Address / Edit Page

Edit MAC Address Rules

- **IP Address:** The IP address

i to the right of the IP address is a drop down to select a subnet. This can be used to define a whole range of IP addresses

- **Description:** Specific optional information about the IP address
- **Direction:** Dropdown to select:
 - **Both:** Allows access **to** and **from** the IP address
 - **From:** Allows access to an address through the captive portal
 - **To:** Allow access from all clients (even non-authenticated ones) behind the portal to this IP
- **Bandwidth up:** Allowed upload limit on this IP address. If left blank, it will be unlimited
- **Bandwidth down:** Allowed download limit on this IP address. If left blank, it will be unlimited

The **Save** button will save the current MAC address and add it to the **Allowed IP Addresses** table

Allowed Hostnames

Overview

Services / Captive Portal / Acme_Login / Allowed Hostnames

Configuration

MACs

Allowed IP Addresses

Allowed Hostnames

Vouchers

High Availability

File Manager

Hostname	Description	Actions
⇄ acme_corp.com	ACME Corp Web Site	 
→ = All connections to the hostname are allowed, ← = All connections from the hostname are allowed, ⇄ = All connections to or from are allowed		

+ Add

Services / Captive Portal/ Allowed Hostnames Showing Sample Host Name

This section has [Top Banner Buttons](#)

Adding Hostnames here allows them to be **bypassed** from the captive portal automatically. This could be used when outside images or files are required on the captive portal web page. This could also allow a DNS on another network

Allowed Hostnames Table

Within this table, the information displayed is as follows:

- Hostname:** The hostname(s) to be allowed. To the left of the hostname are arrows to signify:
 - (Right Arrow icon):** All connections **to** the hostname are allowed
 - (Left Arrow Icon):** All connections **from** the hostname are allowed
 - (Left/Right Arrow Icon):** All connections **to** and **from** are allowed
- Description:** Specific optional information about the hostname
- Actions:** Buttons for:
 - (Pencil icon):** Edit the hostname
 - (garbage icon):** Delete the hostname

Below the table is an **Add** button to add new hostnames. The resulting Hostname Edit page will load:

Services / Captive Portal / Acme_Login / Allowed Hostnames / Edit

Captive Portal Hostname Settings

Direction

Both

Use "From" to always allow a Hostname through the captive portal (without authentication). Use "To" to allow access from all clients (even non-authenticated ones) behind the portal to this Hostname.

Hostname

acme_corp.com

Description

ACME Corp Web Site

A description may be entered here for administrative reference (not parsed).

Bandwidth up

Enter a upload limit to be enforced on this Hostname in Kbit/s

Bandwidth down

Enter a download limit to be enforced on this Hostname in Kbit/s

Save

Services / Captive Portal/ IP Address / Edit Page

Edit MAC Address Rules

- **Direction:** Dropdown to select:
 - **Both:** Allows access **to** and **from** the hostname
 - **From:** Allows access to a hostname through the captive portal
 - **To:** Allow access from all clients (even non-authenticated ones) behind the portal to this IP
- **Hostname:** The host name
- **Description:** Specific optional information about the hostname
- **Bandwidth up:** Allowed upload limit on this hostname. If left blank, it will be unlimited
- **Bandwidth down:** Allowed download limit on this hostname. If left blank, it will be unlimited

The **Save** button will save the current hostname and add it to the **Allowed Hostnames** table

Vouchers

Overview

Services / Captive Portal / Acme_Login / Vouchers

ConfigurationMACsAllowed IP AddressesAllowed HostnamesVouchersHigh AvailabilityFile Manager

Voucher Rolls

Roll #	Minutes/Ticket	# of Tickets	Comment	Actions
99	240	10	ACME Vender Voucher	

+ Add

Create, Generate and Activate Rolls with Vouchers

Enable

☒ Enable the creation, generation and activation of rolls with vouchers

Create, Generate and Activate Rolls with Vouchers

Voucher Public Key

-----BEGIN PUBLIC KEY-----
MCQwDQYJKoZIhvcNAQEBBQADAwEAIJAK8qJL/n4ixVAgMBAAE=
-----END PUBLIC KEY-----

Paste an RSA public key (64 Bit or smaller) in PEM format here. This key is used to decrypt vouchers.

Generate new keys

Voucher Private Key

-----BEGIN RSA PRIVATE KEY-----
MD4CAQACCQCtK1S/5+IsVQIDAQABAggnnB9BgF8WFQIFAP81CH8CBQCtvsErAgRM
oO+7AgRpSda/AgUAj3jcMQ==
-----END RSA PRIVATE KEY-----

Paste an RSA private key (64 Bit or smaller) in PEM format here. This key is only used to generate encrypted vouchers and doesn't need to be available if the vouchers have been generated offline.

Character set

2345678abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

Tickets are generated with the specified character set. It should contain printable characters (numbers, lower case and upper case letters) that are hard to confuse with others. Avoid e.g. 0/O and l/1.

of Roll bits

16

Reserves a range in each voucher to store the Roll # it belongs to. Allowed range: 1..31. Sum of Roll+Ticket+Checksum bits must be one Bit less than the RSA key size.

of Ticket bits

10

Reserves a range in each voucher to store the Ticket# it belongs to. Allowed range: 1..16. Using 16 bits allows a roll to have up to 65535 vouchers. A bit array, stored in RAM and in the config, is used to mark if a voucher has been used. A bit array for 65535 vouchers requires 8 KB of storage.

of Checksum bits

5

Reserves a range in each voucher to store a simple checksum over Roll # and Ticket#. Allowed range is 0..31.

Magic number

349790887

Magic number stored in every voucher. Verified during voucher check. Size depends on how many bits are left by Roll+Ticket+Checksum bits. If all bits are used, no magic number will be used and checked.

Invalid voucher message

Voucher invalid

Error message displayed for invalid vouchers on captive portal error page (\$PORTAL_MESSAGE\$).

Expired voucher message

Voucher expired

Error message displayed for expired vouchers on captive portal error page (\$PORTAL_MESSAGE\$).

Save

Services / Captive Portal / Vouchers Showing an Enabled Voucher

This section has [Top Banner Buttons](#)

Vouchers for a captive portal are unique codes or tokens that provide users access to a restricted network, typically after they log in or register

Voucher Rolls

Within this table, the information displayed is as follows:

- Roll #:** The roll number (0-65535) to be generated voucher
- Minutes/Ticket:** Defines the time in minutes that a user is allowed access. The clock starts ticking the first time a voucher is used for authentication

- **# of Ticket:** The number of vouchers (1-1023) found on top of the generated voucher

❗ Changing this number for an existing Roll will mark all vouchers as unused again

- **Comment:** Optional description of the voucher
- **Actions:** Buttons for:
 - **(Pencil icon):** Edit the voucher roll
 - **(garbage icon):** Delete the voucher roll
 - **(page with X icon):** Export voucher roll to a .CSV file

Below the table is an **Add** button to add new voucher roles. The resulting Vouchers Edit page will load with the options explained above :

Services / Captive Portal / Acme_Login / Vouchers / Edit 

Voucher Rolls	
Roll #	 Enter the Roll# (0..65535) found on top of the generated/printed vouchers
Minutes per ticket	 Defines the time in minutes that a user is allowed access. The clock starts ticking the first time a voucher is used for authentication.
Count	 Enter the number of vouchers (1..1023) found on top of the generated/printed vouchers. WARNING: Changing this number for an existing Roll will mark all vouchers as unused again
Comment	 Can be used to further identify this roll. Ignored by the system.

 Save

Services / Captive Portal / Vouchers / Edit Page

Create, Generate and Activate Rolls with Vouchers Section

- **Enabled:** Checkbox to enable the creation, generation and activation of rolls with vouchers
- **Voucher Public Key:** A pasted or generated public key (64-bit or smaller in PEM format). To generate new Public and Private voucher keys, use the **Generate new keys** button
- **Voucher Private Key:** A pasted or generated private key (64-bit or smaller in PEM format). To generate new Public and Private voucher keys, use the **Generate new keys** button
- **Character set:** Tickets to be generated with the specified character set

❗ It should contain printable characters (numbers, lower case and upper case letters) that are hard to confuse with others. For example, avoid using zero (0) and the letter O and one (1) and the letter l

- **# of Roll bits:** Reserves a range (1-31) in each voucher to store the Roll # it belongs to

❗ The sum of Roll+Ticket+Checksum bits must be one Bit less than the RSA key size

- **# of Ticket bits:** Reserves a range (1-16) in each voucher to store the Ticket# it belongs to

❗ Using 16 bits allows a roll to have up to 65535 vouchers. A bit array, stored in RAM and in the config, is used to mark if a voucher has been used. A bit array for 65535 vouchers requires 8 KB of storage

- **Magic number:** Number stored in every voucher. It is used to verify during a voucher check

❗ Size depends on how many bits are left by Roll+Ticket+Checksum bits. If all bits are used, no magic number will be used and checked

- **Invalid voucher message:** Error message displayed for invalid vouchers on captive portal error page
- **Expired voucher message:** Error message displayed for expired vouchers on captive portal error page

The **Save** button will save the current hostname and add it to the **Allowed Hostnames** table

High Availability

Overview

Services / Captive Portal / Acme_Login / High Availability

ConfigurationMACsAllowed IP AddressesAllowed HostnamesVouchersHigh AvailabilityFile Manager

Secondary to Primary node Synchronization

Enable

☒ Enable backward High Availability Sync for connected users and used vouchers

The XMLRPC sync provided by ICS360.Defender in [High Availability](#) settings only synchronize a secondary node to its primary node. This checkbox enable a backward sync from the secondary to the primary, in order to have a bi-directional synchronization. ICS360.DefenderThe purpose of this feature is to keep connected users synchronized between servers even if a node does down, thus providing redundancy for the captive portal zone.

Important: these settings should be set on the secondary node only ! Do not update these settings if this ICS360.Defender is the primary node !

Primary node IP

22.33.65.122

Please fill here the IP address of the primary node.

Primary node username

ACME_Secondary

Please enter the username of the primary node that the secondary node will use for backward sync. This could be any ICS360.Defender user on the primary node with "System - HA node sync" privileges.

Primary node password

Please enter the password associated to this user.

Confirm

Save

It is recommended to configure XMLRPC sync on the primary node before configuring backward synchronization for captive portal.

Services / Captive Portal / High Availability

ⓘ These settings should be set on the secondary node only. Do not update these settings if this Anybus Defender is the primary node

Secondary to Primary node Synchronization

- **Enable backward High Availability Sync for connected users and used vouchers:** Enable for [High Availability](#)

ⓘ The XMLRPC sync provided by the Anybus Defender in [High Availability](#) settings only synchronize a secondary node to its primary node. This checkbox enables a backward sync from the secondary to the primary in order to have a bi-directional synchronization. The purpose of this feature is to keep connected users synchronized between servers even if a node goes down

When this is enabled, the items can be configured:

- **Primary node IP:** IP address of the primary node
- **Primary node username:** The username of the primary node that the secondary node will use for backward sync. This could be any Anybus Defender user on the primary node with "System - HA node sync" privileges.

Below the table is a **Save** button save the settings

ⓘ It is recommended to configure XMLRPC sync on the primary node before configuring backward synchronization for captive portal

File Manager

Overview

Services / Captive Portal / Acme_Login / File Manager

ConfigurationMACsAllowed IP AddressesAllowed HostnamesVouchersHigh AvailabilityFile Manager

Installed Files

Name	Size	Actions
captiveportal-company_logo.png	43 KiB	
Total	43 KiB	

+ Add

Services / Captive Portal / File Manager Showing Installed File

This section has [Top Banner Buttons](#)

The file manager allows for files (images, scripts, etc.) to be added to the root directory of the captive portal server

Any files that are uploaded here with the filename prefix of **captiveportal-** will be made available in the root directory of the captive portal HTTP(S) server. An icon file named **favicon.ico** may also be uploaded and will remain without prefix

Installed Files Table

Within this table, the information displayed is as follows:

- Name:** Name of the file
- Size:** File size
- Actions:** (trash can icon) Removes the file from the list

Clicking the (blue i icon) will display the **Notes** section with information explained above

Examples

Using the sample image above, HTML code to access it would be:

```

```

To link to a script file, this could be used:

```
<a href="/captiveportal-acme-aup.php?zone=$PORTAL_ZONE&redirurl=$PORTAL_REDIRURL">Acceptable usage policy</a>
```

DHCP Server

Overview

Services / DHCP Server / LAN

LAN

General Options

Enable

☒ Enable DHCP server on LAN interface

BOOTP

☐ Ignore BOOTP queries

Deny unknown clients

Allow all clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.

Ignore denied clients

☐ Denied clients will be ignored rather than rejected.
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers

☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet

192.168.200.0

Subnet mask

255.255.255.0

Available range

192.168.200.1 - 192.168.200.254

Range

From

To

Services / DHCP Server / LAN

This section has [Top Banner Buttons](#)

DHCP Server is for the alternate (usually the LAN) interface of the Anybus Defender

i For DHCP on the WAN is done on the [WAN Interfaces](#) page

The **Services / DHCP Server / LAN** page is divided into these sections:

General Options

- **Enable:** Enables the DHCP server on the LAN interface
- **BootP:** If enabled, any BOOTP queries will be ignored
- **Deny unknown clients:** Dropdown for denying unknown clients
 - **Allow all clients:** Any DHCP client will get an IP address within this scope/range on this interface
 - **Allow known clients from any interface:** Any DHCP client with a MAC address listed on **ANY** scope(s)/interface(s) will get an IP address
 - **Allow known clients from only this interface:** Only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range
- **Ignore denied clients:** Checkbox to ignore (not logged) rather than reject (logged) clients

i This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured

- **Ignore client identifiers:** Checkbox to not record the clients UID (Unique Identifier) in a DHCP request

i This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification

- **Subnet:** This is a read-only field showing the interface's subnet
- **Subnet mask:** This is a read-only field showing the interface's subnet mask
- **Available range:** Shows the current range allowed by the Subnet and Subnet Mask settings shown above
- **Range:** Allows for an override of the **From** and **To** ranges for IP addresses assignment

Additional Pools

Additional Pools			
Add		+ Add pool	
If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.			
Pool Start	Pool End	Description	Actions

Additional Pools Section

This allows for additional pools of addresses are needed inside of this subnet outside the above Range set above. Use the **Add pool** button to add pools as needed

Servers

Servers	
WINS servers	WINS Server 1
	WINS Server 2
DNS servers	DNS Server 1
	DNS Server 2
	DNS Server 3
	DNS Server 4
Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.	

WINS and DNS Section

If WINS and/or DNS are needed, enter them here

OMAPI

OMAPI	
OMAPI Port	OMAPI Port
Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable. Only the first OMAPI configuration is used.	
OMAPI Key	OMAPI Key
Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint.	
☐ Generate New Key Generate a new key based on the selected algorithm.	
Key Algorithm	HMAC-SHA256 (current bind9 default)
Set the algorithm that OMAPI key will use.	

WINS and DNS Section

For the OMAPI (Open Mobile Application Platform Interface) protocol, configure these options:

- **OMAPI Port:** Port (default is 7911) that OMAPI will listen on. If left blank, OMAPI will be disabled

- **OMAPI Key:** The key using the **Key Algorithm** explained below
- **Key Algorithm:** Dropdown to select the key algorithm. Options are:
 - **HMAC-MD5 (legacy default)**
 - **HMAC-SHA1**
 - **HMAC-SHA224**
 - **HMAC-SHA256 (current bind9 default)**
 - **HMAC-SHA384**
 - **HMAC-SHA512 (most secure)**

Other Options

Other Options

Gateway

The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.

Domain name

The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.

Domain search list

The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.

Default lease time

This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.

Maximum lease time

This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.

Failover peer IP

Leave blank to disable. Enter the interface IP address of the other machine. Machines must be using Hot Standby. Interface's advskew determines whether the DHCPd process is Primary or Secondary. Ensure one machine's advskew < 20 (and the other is > 20).

Static ARP

☐ Enable Static ARP entries

This option persists even if DHCP server is disabled. Only the machines listed below will be able to communicate with the firewall on this interface.

Time format change

☐ Change DHCP display lease time from UTC to local time

By default DHCP leases are displayed in UTC time. By checking this box DHCP lease time will be displayed in local time and set to the time zone selected. This will be used for all DHCP interfaces lease time.

Statistics graphs

☐ Enable RRD statistics graphs

Enable this to add DHCP leases statistics to the RRD graphs. Disabled by default.

Ping check

☐ Disable ping check

When enabled dhcpd sends a ping to the address being assigned, and if no response has been heard, it assigns the address. Enabled by default.

Dynamic DNS

⚙

Display Advanced

MAC address control

⚙

Display Advanced

NTP

⚙

Display Advanced

TFTP

⚙

Display Advanced

LDAP

⚙

Display Advanced

Network Booting

⚙

Display Advanced

Additional BOOTP/DHCP Options

⚙

Display Advanced

Save

Other Options Section

If required these options are available to further customize the DHCP server:

- **Gateway:** Enter a gateway address if the default interface IP address will not be used

ⓘ

Type **none** for no gateway assignment

- **Domain name:** Enter a domain name if the system name will not be used
- **Domain search list:** Optional domain search list. Use the semicolon character to separate these terms
- **Default lease time:** Enter a specific expiration time for client that do not ask for it. The default is 7200 seconds
- **Maximum lease time:** Enter a specific maximum lease time for client that ask for it. The default is 86400 seconds
- **Failover peer IP:** Enter the IP of the failover peer (disabled if left blank). Devices must be in **Hot Standby** mode
- **Static ARP:** Checkbox to enable Static Arp entries even if the DHCP server is disabled
- **Time format change:** Checkbox change lease time from UTC to the local time
- **Statistics graphs:** Checkbox to enabled RRD (Round Robin Database) for lease Statistics
- **Ping check:** Checkbox to disable ping check

Advanced options are available by clicking these buttons:

- (cog wheel icon) **Dynamic DNS**
- (cog wheel icon) **MAC address control**
- (cog wheel icon) **NTP**
- (cog wheel icon) **TFTP**
- (cog wheel icon) **LDAP**
- (cog wheel icon) **Network**
- (cog wheel icon) **Additional BOOTP/DHCP Options**

Below this section is a **Save** button to save the DHCP Server settings

DHCP Static Mappings for this Interface

DHCP Static Mappings for this Interface				
Static ARP	MAC address	IP address	Hostname	Description
				+ Add

DHCP Static Mappings for this Interface Section

For devices identified by MAC, specific IP, WINS, DNS, Gateway, etc. can be configured by clicking the **Add** button for each device

DNS Forwarder

Overview

Services / DNS Forwarder

General DNS Forwarder Options

Enable

☐ Enable DNS forwarder

DHCP Registration

☐ Register DHCP leases in DNS forwarder

If this option is set machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. The domain in [System: General Setup](#) should also be set to the proper value.

Static DHCP

☐ Register DHCP static mappings in DNS forwarder

If this option is set, IPv4 DHCP static mappings will be registered in the DNS forwarder so that their name can be resolved. The domain in [System: General Setup](#) should also be set to the proper value.

Prefer DHCP

☐ Resolve DHCP mappings first

If this option is set DHCP mappings will be resolved before the manual list of names below. This only affects the name given for a reverse lookup (PTR).

DNS Query Forwarding

☐ Query DNS servers sequentially

☐ Require domain

☐ Do not forward private reverse lookups

If this option is set ICS360.Defender DNS Forwarder (dnsmasq) will query the DNS servers sequentially in the order specified ([System - General Setup - DNS Servers](#)), rather than all at once in parallel.

If this option is set ICS360.Defender DNS Forwarder (dnsmasq) will not forward A or AAAA queries for plain names, without dots or domain parts, to upstream name servers. If the name is not known from `/etc/hosts` or DHCP then a "not found" answer is returned.

If this option is set ICS360.Defender DNS Forwarder (dnsmasq) will not forward reverse DNS lookups (PTR) for private addresses (RFC 1918) to upstream name servers. Any entries in the Domain Overrides section forwarding private "n.n.n.in-addr.arpa" names to a specific server are still forwarded. If the IP to name is not known from `/etc/hosts`, DHCP or a specific domain override then a "not found" answer is immediately returned.

Listen Port

The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

Interfaces

All

WAN

LAN

WAN IPv6 Link-Local

Interface IPs used by the DNS Forwarder for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected below are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.

Strict binding

☐ Strict interface binding

If this option is set, the DNS forwarder will only bind to the interfaces containing the IP addresses selected above, rather than binding to all interfaces and discarding queries to other addresses.

This option does NOT work with IPv6. If set, dnsmasq will not bind to IPv6 addresses.

Custom options

Enter any additional options to add to the dnsmasq configuration here, separated by a space or newline.

Save

Services / DNS Forwarder

This section has [Top Banner Buttons](#)

The DNS forwarder service in the Anybus Defender allows the firewall to forward DNS (Domain Name System) queries from clients to external or internal DNS servers for resolution

If the DNS forwarder is enabled, the [DHCP Service](#) (if enabled) will automatically serve the LAN IP address as a DNS server to DHCP clients so they will use the forwarder. The DNS forwarder will use the DNS servers entered in [System > General Setup](#) or those obtained via DHCP or PPP on WAN if **Allow DNS server list to be overridden by DHCP/PPP on WAN** is checked. If that option is not used (or if a static IP address is used on WAN), at least one DNS server must be manually specified on the [System > General Setup](#) page

The **Services / DNS Forwarder** page is divided into these sections:

General DNS Forwarder Options

- **Enable:** Enables the DNS forwarder
- **DHCP Registration:** If enabled, devices that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved

❗ The domain in the [System > General Setup](#) is required for this checkbox to be selectable

- **Static DHCP:** If enabled, IPv4 DHCP static mappings will be registered in the DNS forwarder so that their name can be resolved

❗ The domain in the [System > General Setup](#) is required for this checkbox to be selectable

- **Prefer DHCP:** If enabled, DHCP mappings will be resolved before the manual list of names below

i This only affects the name given for a reverse lookup (PTR)

- **DNS Query Forwarding:** A series of checkboxes for:
 - **Query DNS servers sequentially:** The DNS Forwarder (dnsmasq) will not forward **A** or **AAAA** queries for plain names, without dots or domain parts, to upstream name servers. If the name is not known from **/etc/hosts** or DHCP then a **not found** answer is returned
 - **Require domain:** The DNS Forwarder (dnsmasq) will query the DNS servers sequentially in the order specified (System - General Setup - DNS Servers), rather than all at once in parallel
 - **Do not forward private reverse lookups:** The DNS Forwarder (dnsmasq) will not forward reverse DNS lookups (PTR) for private addresses (RFC 1918) to upstream name servers. Any entries in the **Domain Overrides** section below forwarding private **n.n.n.in-addr.arpa** names to a specific server are still forwarded. If the IP to name is not known from **/etc/hosts**, DHCP or a specific domain override then a **not found** answer is immediately returned
- **Listen Port:** The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53
- **Interfaces:** Interface IPs used by the DNS Forwarder for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected below are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address
- **Strict Binding:** If enabled, the DNS forwarder will only bind to the interfaces containing the IP addresses selected above, rather than binding to all interfaces and discarding queries to other addresses

❗ This option does NOT work with IPv6. If set, dnsmasq will not bind to IPv6 addresses

- **Custom Options:** Enter any additional options to add to the dnsmasq configuration here, separated by a space or newline

Below this section is a **Save** button to save the DNS Forwarder settings

Host Overrides

Host Overrides				
Host	Domain	IP	Description	Actions
				+ Add

Host Overrides Section

This allows for additional custom DNS entries. Use the **Add** button to add Host Overrides as needed

Domain Overrides

Domain Overrides			
Domain	IP	Description	Actions
			+ Add

Domain Overrides Section

This allows for using an alternate DNS server used for resolving hosts within a specific domain. Use the **Add** button to add Domain Overrides as needed

General Settings

Overview

Services / DNS Resolver / General Settings

General Settings

Advanced Settings

Access Lists

General DNS Resolver Options

Enable

☒ Enable DNS resolver

Listen Port

53

The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

Enable SSL/TLS Service

☐ Respond to incoming SSL/TLS queries from local clients

Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.

SSL/TLS Certificate

webConfigurator default (6703cb518daa2)

The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.

SSL/TLS Listen Port

853

The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.

Network Interfaces

All

WAN

LAN

WAN IPv6 Link-Local

LAN IPv6 Link-Local

Interface IPs used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected below are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.

Outgoing Network Interfaces

All

WAN

LAN

WAN IPv6 Link-Local

LAN IPv6 Link-Local

Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.

System Domain Local Zone Type

Transparent

The local-zone type used for the ICS360.Defender system domain (System | General Setup | Domain). Transparent is the default. Local-Zone type descriptions are available in the unbound.conf(5) manual pages.

DNSSEC

☒ Enable DNSSEC Support

Python Module

☐ Enable Python Module

Enable the Python Module.

DNS Query Forwarding

☐ Enable Forwarding Mode

If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under System > General Setup or those obtained via DHCP/PPP on WAN (if DNS Server Override is enabled there).

☐ Use SSL/TLS for outgoing DNS Queries to Forwarding Servers

When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.

DHCP Registration

☐ Register DHCP leases in the DNS Resolver

If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. Note that this will cause the Resolver to reload and flush its resolution cache whenever a DHCP lease is issued. The domain in System > General Setup should also be set to the proper value.

Static DHCP

☐ Register DHCP static mappings in the DNS Resolver

If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in System > General Setup should also be set to the proper value.

OpenVPN Clients

☐ Register connected OpenVPN clients in the DNS Resolver

If this option is set, then the common name (CN) of connected OpenVPN clients will be registered in the DNS Resolver, so that their name can be resolved. This only works for OpenVPN servers (Remote Access SSL/TLS or User Auth with Username as Common Name option) operating in "tun" mode. The domain in System: General Setup should also be set to the proper value.

Display Custom Options

⚙️ Display Custom Options

Save

Services / DNS Resolver General Settings Tab

This section has [Top Banner Buttons](#)

A DNS resolver allows the firewall to resolve domain names (such as acme.corp.com) into IP addresses (like 192.200.2.1) using the Domain Name System (DNS)

❗ If the DNS Forwarder is enabled, the DHCP service (if enabled) will automatically serve the LAN IP address as a DNS server to DHCP clients so they will use the DNS Resolver. If Forwarding is enabled, the DNS Resolver will use the DNS servers entered in [System > General Setup](#) or those obtained via DHCP or PPP on WAN if **Allow DNS server list to be overridden by DHCP/PPP on WAN** is checked

The **Services / DNS Forwarder / General Settings** page is divided into these sections:

General DNS Resolver Options

- **Enable:** Enables the DNS resolver
- **Listen Port:** The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53
- **Enable SSL/TLS Service:** When checked, incoming SSL/TLS queries from local clients will be responded to

❗ Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings

- **SSL/TLS Certificate:** Dropdown to select the pre-configured SSL/TLS certificate
- **SSL/TLS Listen Port:** The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853
- **Network Interfaces:** Selection of interfaces to use in the DNS Resolver responder. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected below are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address
- **Outgoing Network Interfaces:** Selection of interfaces to use as outgoing destinations. Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used
- **System Domain Local Zone Type:** Dropdown to set the local-zone type used for the Anybus Defender's [System > General Setup > Domain](#). Options are:

- Deny
- Refuse
- Static
- Transparent is default
- Type Transparent
- Redirect
- Inform
- Inform Deny
- No Default

- **DNSSEC:** Enables (Domain Name System Security Extensions) support
- **Python Module:** Enables Python scripting support
- **DNS Query Forwarding:** If enabled, DNS queries will be forwarded to the upstream DNS servers defined under [System > General Setup](#) or those obtained via DHCP/PPP on WAN (if DNS Server Override is enabled there)
- **SSL/TLS for Outgoing DNS Queries:** If enabled, and used in conjunction with [DNS Query Forwarding](#), queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853

❗ ALL configured forwarding servers MUST support SSL/TLS queries on port 853

- **DHCP Registration:** If enabled, devices that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved

i This will cause the Resolver to reload and flush its resolution cache whenever a DHCP lease is issued. The domain in [System > General Setup](#) should also be set to the proper value

- **Static DHCP:** If enabled, DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved

i The domain in [System > General Setup](#) should also be set to the proper value

- **Open VPN Clients:** If enabled, the common name (CN) of connected [OpenVPN clients](#) will be registered in the DNS Resolver, so that their name can be resolved. This only works for [OpenVPN Servers](#) (the **Remote Access SSL/TLS** or the **User Auth with Username as Common Name** option) operating in **tun** mode.

i The domain in [System > General Setup](#) should also be set to the proper value

- **Display Custom Options:** By clicking the **(cog wheel icon) Display Custom Options** button toggles on a text entry that allows additional configuration parameters separated by new lines

Host Overrides

Host Overrides				
Host	Parent domain of host	IP to return for host	Description	Actions
Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'nas.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.				
				+ Add

Host Overrides Section

This allows for additional custom DNS entries. Use the **Add** button to add Host Overrides as needed

Domain Overrides

Domain Overrides			
Domain	Lookup Server IP Address	Description	Actions
Enter any domains for which the resolver's standard DNS lookup process should be overridden and a different (non-standard) lookup server should be queried instead. Non-standard, 'invalid' and local domains, and subdomains, can also be entered, such as 'test', 'nas.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. The IP address is treated as the authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried. If there are multiple authoritative DNS servers available for a domain then make a separate entry for each, using the same domain name.			
			+ Add

Domain Overrides Section

This allows for using an alternate DNS server used for resolving hosts within a specific domain. Use the **Add** button to add Domain Overrides as needed

Advanced Settings

Overview

Services / DNS Resolver / Advanced Settings		    
General Settings	Advanced Settings	Access Lists
Advanced Privacy Options		
Hide Identity	☒ id.server and hostname.bind queries are refused	
Hide Version	☒ version.server and version.bind queries are refused	
Query Name Minimization	☐ Send minimum amount of QNAME/QTYPE information to upstream servers to enhance privacy Only send minimum required labels of the QNAME and set QTYPE to A when possible. Best effort approach; full QNAME and original QTYPE will be sent when upstream replies with a RCODE other than NOERROR, except when receiving NXDOMAIN from a DNSSEC signed zone. Default is off. Refer to RFC 7816 for in-depth information on Query Name Minimization.	
Strict Query Name Minimization	☐ Do not fall-back to sending full QNAME to potentially broken DNS servers QNAME minimization in strict mode. A significant number of domains will fail to resolve when this option in enabled. Only use if you know what you are doing. This option only has effect when Query Name Minimization is enabled. Default is off.	

Services / DNS Resolver Advanced Settings Tab

This section has [Top Banner Buttons](#)

The **Services / DNS Forwarder / Advanced Settings** page is divided into these sections:

Advanced Privacy Options

- **Hide Identity:** If enabled, **id.server** and **hostname.bind** queries are refused
- **Hide Version:** If enabled, **version.server** and **version.bind** queries are refused
- **Query Name Minimization:** If enabled, only the minimum amount of **QNAME/QTYPE** information are sent to upstream servers to enhance privacy

i Best effort is for full **QNAME** and original **QTYPE** will be sent when upstream replies with a **RCODE** other than **NOERROR**, except when receiving **NXDOMAIN** from a **DNSSEC** signed zone

Refer to [RFC 7816](#) for in-depth information on Query Name Minimization

- **Strict Query Name Minimization:** If enabled, fall-back to sending full **QNAME** to potentially broken DNS servers is not done
- **Strict Query Name Minimization:** If enabled, fall-back to sending full **QNAME** to potentially broken DNS servers is not done

i This option only has effect when **Query Name Minimization** option above is enabled

i A significant number of domains will fail to resolve when this option in enabled. Only enable this for a specific purpose

Advanced Resolver Options

Advanced Resolver Options	
Prefetch Support	☐ Message cache elements are prefetched before they expire to help keep the cache up to date When enabled, this option can cause an increase of around 10% more DNS traffic and load on the server, but frequently requested items will not expire from the cache.
Prefetch DNS Key Support	☐ DNSKEYs are fetched earlier in the validation process when a Delegation signer is encountered This helps lower the latency of requests but does utilize a little more CPU. See: Wikipedia
Harden DNSSEC Data	☒ DNSSEC data is required for trust-anchored zones. If such data is absent, the zone becomes bogus. If Disabled and no DNSSEC data is received, then the zone is made insecure.
Serve Expired	☐ Serve cache records even with TTL of 0 When enabled, allows unbound to serve one query even with a TTL of 0, if TTL is 0 then new record will be requested in the background when the cache is served to ensure cache is updated without latency on service of the DNS request.
Aggressive NSEC	☐ Aggressive Use of DNSSEC-Validated Cache When enabled, unbound uses the DNSSEC NSEC chain to synthesize NXDOMAIN and other denials, using information from previous NXDOMAINs answers. It helps to reduce the query rate towards targets that get a very high nonexistent name lookup rate.
Message Cache Size	4 MB Size of the message cache. The message cache stores DNS response codes and validation statuses. The Resource Record Set (RRSet) cache will automatically be set to twice this amount. The RRSet cache contains the actual RR data. The default is 4 megabytes.
Outgoing TCP Buffers	10 The number of outgoing TCP buffers to allocate per thread. The default value is 10. If 0 is selected then TCP queries are not sent to authoritative servers.
Incoming TCP Buffers	10 The number of incoming TCP buffers to allocate per thread. The default value is 10. If 0 is selected then TCP queries are not accepted from clients.
EDNS Buffer Size	Automatic value based on active interface MTUs Number of bytes size to advertise as the EDNS reassembly buffer size. This is the value that is used in UDP datagrams sent to peers. Auto mode sets optimal buffer size by using the smallest MTU of active interfaces and subtracting the IPv4/IPv6 header size. If fragmentation reassemble problems occur, usually seen as timeouts, then a value of 1432 should help. The 512/1232 values bypasses most IPv4/IPv6 MTU path problems, but it can generate an excessive amount of TCP fallback.
Number of Queries per Thread	512 The number of queries that every thread will service simultaneously. If more queries arrive that need to be serviced, and no queries can be jostled, then these queries are dropped.
Jostle Timeout	200 This timeout is used for when the server is very busy. This protects against denial of service by slow queries or high query rates. The default value is 200 milliseconds.
Maximum TTL for RRsets and Messages	86400 The Maximum Time to Live for RRsets and messages in the cache. The default is 86400 seconds (1 day). When the internal TTL expires the cache item is expired. This can be configured to force the resolver to query for data more often and not trust (very large) TTL values.
Minimum TTL for RRsets and Messages	0 The Minimum Time to Live for RRsets and messages in the cache. The default is 0 seconds. If the minimum value kicks in, the data is cached for longer than the domain owner intended, and thus less queries are made to look up the data. The 0 value ensures the data in the cache is as the domain owner intended. High values can lead to trouble as the data in the cache might not match up with the actual data anymore.
TTL for Host Cache Entries	15 minutes Time to Live, in seconds, for entries in the infrastructure host cache. The infrastructure host cache contains round trip timing, lameness, and EDNS support information for DNS servers. The default value is 15 minutes.
Number of Hosts to Cache	10000 Number of infrastructure hosts for which information is cached. The default is 10,000.
Unwanted Reply Threshold	Disabled If enabled, a total number of unwanted replies is kept track of in every thread. When it reaches the threshold, a defensive action is taken and a warning is printed to the log file. This defensive action is to clear the RRSet and message caches, hopefully flushing away any poison. The default is disabled, but if enabled a value of 10 million is suggested.
Log Level	Level 1: Basic operational information Select the level of detail to be logged. Each level also includes the information from previous levels. The default is basic operational information (level 1)
Disable Auto-added Access Control	☐ Disable the automatically-added access control entries By default, IPv4 and IPv6 networks residing on internal interfaces of this system are permitted. Allowed networks must be manually configured on the Access Lists tab if the auto-added entries are disabled.
Disable Auto-added Host Entries	☐ Disable the automatically-added host entries By default, the primary IPv4 and IPv6 addresses of this firewall are added as records for the system domain of this firewall as configured in System: General Setup . This disables the auto generation of these entries.
Experimental Bit 0x20 Support	☐ Use 0x-20 encoded random bits in the DNS query to foil spoofing attempts. See the implementation draft dns-0x20 for more information.
DNS64 Support	☐ Enable DNS64 (RFC 6147)

 Save

Host Overrides Section

- **Prefetch Support:** If enabled, message cache elements are prefetched before they expire to help keep the cache up to date

❗ When enabled, this option can cause an increase of around 10% more DNS traffic and load on the server, but frequently requested items will not expire from the cache

- **Prefetch DNS Key Support:** If enabled, **DNSKEYs** are fetched earlier in the validation process when a Delegation signer is encountered. This helps lower the latency of requests but does utilize a little more CPU. [More Information on DNS Record Types](#)

- **Harden DNSSEC Data:** If enabled, DNSSEC data is required for trust-anchored zones. If disabled and no DNSSEC data is received, then the zone is made insecure

- **Serve Expired:** If enabled, this allows unbound to serve one query even with a TTL of 0, if TTL is 0 then new record will be requested in the background when the cache is served to ensure cache is updated without latency on service of the DNS request

- **Aggressive NSEC:** If enabled, unbound uses the **DNSSEC NSEC** chain to synthesize **NXDOMAIN** and other denials, using information from previous **NXDOMAINs** answers

- **Message Cache Size:** Dropdown to select the size of the message cache. The message cache stores DNS response codes and validation statuses. The Resource Record Set (RRSet) cache will automatically be set to twice this amount. Settings are 4MB (default), 10MB, 20MB, 50MB, 100MB, 250MB, and 512MB

- **Outgoing TCP Buffers:** Dropdown to select the number of outgoing TCP buffers to allocate per thread. Settings are , 0, 10 (default), 20, 30, 50

❗ If 0 is selected then TCP queries are not sent to authoritative servers

- **Incoming TCP Buffers:** Dropdown to select the number of incoming TCP buffers to allocate per thread. Settings are , 0, 10 (default), 20, 30, 50

❗ If 0 is selected then TCP queries are not accepted from clients

- **EDNS Buffer Size:** Dropdown to select the number of bytes size to advertise as the **EDNS** reassembly buffer size. This is the value that is used in UDP datagrams sent to peers. Settings are:

- **Automatic value based on active interface MTUs:** Sets optimal buffer size by using the smallest MTU of active interfaces and subtracting the IPv4/IPv6 header size
- **512: IPV4 Minimum:** Bypasses most IPv4 MTU path problems, but it can generate an excessive amount of TCP fallback
- **1220: NSD IPV5 EDNA Minimum**
- **1232: IPv6 Minimum** Bypasses most IPv6 MTU path problems, but it can generate an excessive amount of TCP fallback
- **1432: 1500 Byte MTU:** Use if fragmentation reassemble problems occur, usually seen as timeouts
- **1480: NSD IPv4 EDNS Minimum**
- **1480: NSD IPv4 EDNS Minimum**

- **Number of Queries per Thread:** Dropdown to select The number of queries that every thread will service simultaneously. If more queries arrive that need to be serviced, and no queries can be jostled, then these queries are dropped. Settings are 512 (default), 1024, 2048

- **Jostle Timeout:** Dropdown to select timeout in milliseconds for instances where the server is busy. This protects against denial of service by slow queries or high query rates. Settings are 100ms, 200ms (default), 500ms, 1000ms

- **Maximum TTL for RRsets and Messages:** Numeric entry for the Maximum Time to Live for **RRsets** and messages in the cache. The default is 86400 seconds (1 day). When the internal TTL expires, the cache item is expired. This can be configured to force the resolver to query for data more often and not trust (very large) TTL values
- **Minimum TTL for RRsets and Messages:** Numeric entry for the Minimum Time to Live for **RRsets** and messages in the cache. The default is 0 seconds. If the minimum value enables, the data is cached for longer than the domain owner intended, and thus, less queries are made to look up the data. The 0 value ensures the data in the cache is as the domain owner intended.

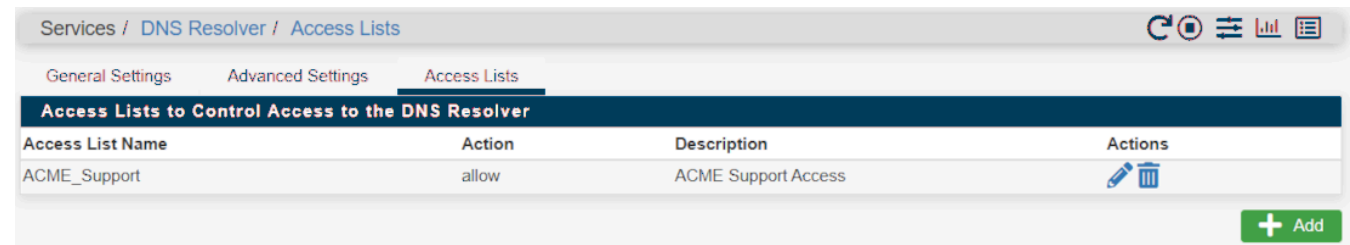
ⓘ Higher values can cause issues with the data in the cache mismatching with the actual data

- **TTL for Host Cache Entries:** Dropdown to select the Time to Live (TTL), in seconds, for entries in the infrastructure host cache. The infrastructure host cache contains round trip timing, lameness, and EDNS support information for DNS servers. Settings are 1, 2, 5, 10, and 15 (default) minutes
- **Number of Hosts to Cache:** Numeric entry for for the Number of infrastructure hosts for which information is cached. The default is 10,000
- **Unwanted Reply Threshold:** Dropdown to enable/disable a set number of unwanted replies to track in every thread. When it reaches the threshold, a defensive action is taken and a warning is printed to the log file. This defensive action is to clear the RRSet and message caches. Settings are:
 - **Disabled:** No unwanted replies are track (default)
 - **5 million**
 - **10 million:** Suggested amount if enabled
 - **20 million**
 - **40 milion**
 - **50 million**
- **Log Level:** Dropdown to select the level of detail to be logged. Each level also includes the information from previous levels. Settings are:
 - **Level 0: No Logging:**
 - **Level 1: Basic operational information:** Default
 - **Level 2: Detailed operational information**
 - **Level 3: Query level information**
 - **Level 4: Algorithm level information**
 - ****Level 5: Client identification for cache misses**
- **Disable Auto-added Access Control:** If checked, the default behavior of permitting IPv4 and IPv6 networks residing on internal interfaces of this Anybus Defender is disabled. Allowed networks must be manually configured on the Access Lists tab if the auto-added entries are disabled.
- **Disable Auto-added Host Entries:** If checked, the default behavior of adding IPv4 and IPv6 addresses of this Anybus Defender are added as records for the system domain of this firewall as configured in [System > General Setup](#) is disabled
- **Experimental Bit 0x20 Support:** If checked, **0x-20** encoded random bits are used in the DNS query to foil spoofing attempts. See the implementation [draft dns-0x20](#) for more information.
- **DNS64 Support:** If checked, DNS64, which is used with an IPv6/IPv4 translator to enable client-server communication between an IPv6-only client and an IPv4-only servers, is enabled

Below this section is a **Save** button to save the DNS Resolver Advanced settings

Access Lists

Overview



Services / DNS Resolver Access List Tab Showing Sample Entry

This section has [Top Banner Buttons](#)

For IPv4 and IPv6 networks outside of the interfaces of the Anybus Defender, access must be configured manually using the Access List table

Access Lists to Control Access to the DNS Resolver

- **Action:** Action to apply to hosts (See list below)
- **Comment:** Optional description of the access list
- **Actions:** Buttons for:
 - **(Pencil icon):** Edit the access list
 - **(garbage icon):** Delete the access list
 -

Below the table is an **Add** button to add new access lists. The resulting New Access List edit page will load:

A screenshot of the 'New Access List' edit page. The breadcrumb trail is 'General Settings / Advanced Settings / Access Lists'. The 'Access Lists' tab is active. The form has a title 'New Access List'. It contains several fields: 'Access List name' (text input), 'Action' (dropdown menu with 'Allow' selected), 'Description' (text input), and 'Networks' (a complex field with a text input, a slash, a '128' dropdown, and another text input). Below the 'Networks' field is a 'Save' button and an 'Add Network' button. There is also a 'Description' label for the second text input in the 'Networks' field.

Host Overrides Section

New Access List

- **Access List name:** Name of the Access List
- **Action:** Dropdown to select the action for this accessor:
 - **Allow:** Allow queries from hosts within the netblock defined below
 - **Deny:** Stops queries from hosts within the netblock defined below with no return error message
 - **Refuse:** Stops queries from hosts within the netblock defined below, but sends a DNS rcode **REFUSED** error message back to the client
 - **Allow Snoop:** Allow recursive and non-recursive access from hosts within the netblock defined below. Used for cache snooping and ideally should only be configured for the administrative host
 - **Deny Nonlocal:** Allow only authoritative local-data queries from hosts within the netblock defined below. Messages that are disallowed are dropped
 - **Refuse Nonlocal:** Allow only authoritative local-data queries from hosts within the netblock defined below. Sends a DNS rcode REFUSED error message back to the client for messages that are disallowed.

Below this section are these buttons:

- **Save:** Saves the Access List settings
- **Add Network:** Add additional networks to the **Networks** setting above

IGMP Proxy

Overview

Services / [IGMP Proxy](#)

General IGMP Options

Enable

☒ Enable IGMP

Verbose Logging

☐ Enable verbose logging (Default is terse logging)

 Save

Services / IGMP Proxy

IGMP Snooping (Internet Group Management Protocol Snooping) is a network optimization technique used in the Anybus Defender to manage and optimize multicast traffic. It works by monitoring (or "snooping on") IGMP messages exchanged between multicast routers and hosts in an IP network



Add the interface for upstream, the allowed subnets, and the downstream interfaces for the proxy to allow. Only one "upstream" interface (see below) can be configured

The **Services / IGMP Proxy** page is divided into these sections:

General IGMP Options

- **Enable:** Enables/Disables IGMP
- **Verbose Logging:** If checked, verbose [System Logging](#) is used. If unchecked, terse logging will be used

Below these options a **Save** button to save these settings

IGMP Proxy

IGMP Proxy				
Name	Type	Values	Description	Actions
WAN	upstream	192.168.99.0/32		 
				 Add

IGMP Proxy Section With Sample Proxy

Within this table, the information displayed is as follows:

- **Name:** Name of the IGMP Proxy
- **Type:** Dropdown to select of of these types:
 - **Upstream Interface:** The outgoing interface which is responsible for communicating to available multicast data sources
 - ❗ There can only be one upstream interface
 - **Downstream Interface:** The distribution interfaces to the destination networks, where multicast clients can join groups and receive multicast data
 - ❗ One or more downstream interfaces must be configured
 - **Threshold:** Numeric Entry to define the TTL threshold for the network interface. Packets with a lower TTL than the threshold value will be ignored. If left blank, a value of 1 is used
 - **Networks:** List of IP network and subnet CIDR for the proxy
 - **Add network:** Button allowed multiple Networks to be defined

Below these options is a **Save** button to save the IGMP Proxy

Settings

Overview

Services / NTP / Settings

SettingsACLsPPS

NTP Server Configuration

Enable

☒ Enable NTP Server

You may need to disable NTP if ICS360.Defender is running in a virtual machine and the host is responsible for the clock.

Interface

PLANTNETWORK

CONTROLSNETWORK

Localhost

Interfaces without an IP address will not be shown.
Selecting no interfaces will listen on all interfaces with a wildcard.
Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.

Time Servers

pool.ntp.org

☐ Prefer

☐ No Select

☒ Is a Pool

Add

+ Add

NTP will only sync if a majority of the servers agree on the time. For best results you should configure between 3 and 5 servers (NTP support pages recommend at least 4 or 5), or a pool. If only one server is configured, it **will** be believed, and if 2 servers are configured and they disagree, **neither** will be believed. Options:
Prefer - NTP should favor the use of this server more than all others.
No Select - NTP should not use this server for time, but stats for this server will be collected and displayed.
Is a Pool - this entry is a pool of NTP servers and not a single address. This is assumed for *.pool.ntp.org.

Max candidate pool peers

Maximum number of candidate peers in the NTP pool. This value should be set low enough to provide sufficient alternate sources while not contacting an excessively large number of peers. Many servers inside public pools are provided by volunteers, and a large candidate pool places unnecessary extra load on the volunteer time servers for little to no added benefit. (Default: 5).

Orphan Mode

12

Orphan mode allows the system clock to be used when no other clocks are available. The number here specifies the stratum reported during orphan mode and should normally be set to a number high enough to insure that any other servers available to clients are preferred over this server (default: 12).

Minimum Poll Interval

Default

Minimum poll interval for NTP messages. If set, must be less than or equal to Maximum Poll Interval.

Maximum Poll Interval

Default

Maximum poll interval for NTP messages. If set, must be greater than or equal to Minimum Poll Interval.

NTP Graphs

☐ Enable RRD graphs of NTP statistics (default: disabled).

Logging

☐ Log peer messages (default: disabled).

☐ Log system messages (default: disabled).

These options enable additional messages from NTP to be written to the System Log [Status > System Logs > NTP](#).

Statistics Logging

Display Advanced

Warning: These options will create persistent daily log files in /var/log/ntp.

Leap seconds

Display Advanced

Leap seconds may be added or subtracted at the end of June or December. Leap seconds are administered by the [IERS](#), who publish them in their Bulletin C approximately 6 - 12 months in advance. Normally this correction should only be needed if the server is a stratum 1 NTP server, but many NTP servers do not advertise an upcoming leap second when other NTP servers synchronise to them.
If the leap second is important to your network services, it is [good practice](#) to download and add the leap second file at least a day in advance of any time correction.
More information and files for downloading can be found on their [website](#), and also on the [IST](#) and [NTP](#) websites.

DNS Resolution

Auto

Force NTP peers DNS resolution IP protocol. Do not affect pools.

Enable NTP Server Authentication

☐ Enable NTPv3 authentication (RFC 1305)

Authentication allows the NTP client to confirm it is communicating with the intended server, which protects against man-in-the-middle attacks.

Save

This section has [Top Banner Buttons](#)

NTP (Network Time Protocol) is used to synchronize the clocks of computer systems over a network. Consistency in time is important for [Logging](#), security events, and other time-sensitive operations

The **Services / NTP / Settings** page is divided into these sections:

NTP Server Configuration

- **Enable:** Enables/Disables the NTP server

❗ Disable the NTP if the Anybus Defender is running in a virtual machine and the host is responsible for the clock

- **Interface:** Select from the list of interfaces in the Anybus Defender

❗ Selecting all interfaces will explicitly listen on only the interfaces/IPs specified

❗ Selecting no interfaces will listen on all interfaces with a wildcard

❗ Interfaces without an IP address will not be shown

- **Time Servers:** Text entry for the location of the time server used in synchronization. The default is **pool.ntp.org**

❗ The **Add** button below allows for additional time servers to be used. Each of these entries will have checkboxes to set these preferences:

- **Prefer:** This server is preferred
- **No Select:** Not used for time synchronization (only for display statistics)
- **Is a Pool:** Is a pool of worldwide providers
- **Max candidate pool peers:** Defines the maximum number of candidate peers in the NTP pool. If left blank, the default is 5

❗ This value should be set low enough to provide sufficient alternate sources while not contacting an excessively large number of peers. Many servers inside public pools are provided by volunteers, and a large candidate pool places unnecessary extra load on the volunteer time servers for little to no added benefit.

- **Orphan Mode:** Allows the system clock of the Anybus Defender to be used when no other sources are available. The number specifies the stratum reported during orphan mode, The default is 12

❗ This should normally be set to a number high enough to insure that any other servers available to clients are preferred over this server

- **Minimum Poll Interval:** Dropdown to select the minimum poll interval for NTP messages. Options are:
 - **Default**
 - **4: 16 seconds (00:00:16)**
 - **5: 32 seconds (00:00:32)**
 - **6: 64 seconds (00:01:04)**
 - **7: 128 seconds (00:02:08)**
 - **8: 256 seconds (00:04:16)**
 - **9: 512 seconds (00:08:32)**
 - **10: 1024 seconds (00:17:04)**

- 11: 2048 seconds (00:34:08)
- 12: 4096 seconds (01:08:16)
- 13: 8192 seconds (02:16:32)
- 14: 16,384 seconds (04:33:04)
- 15: 32,768 seconds (09:06:08)
- 16: 65,536 seconds (18:12:16)
- 17: 131,072 seconds (1d 12:24:32)
- Omit (Do not set)

❗ If this is set, it must be less than or equal to **Maximum Poll Interval** shown below

- **Maximum Poll Interval:** Dropdown to select the maximum poll interval for NTP messages. Options are:
 - Default
 - 4: 16 seconds (00:00:16)
 - 5: 32 seconds (00:00:32)
 - 6: 64 seconds (00:01:04)
 - 7: 128 seconds (00:02:08)
 - 8: 256 seconds (00:04:16)
 - 9: 512 seconds (00:08:32)
 - 10: 1024 seconds (00:17:04)
 - 11: 2048 seconds (00:34:08)
 - 12: 4096 seconds (01:08:16)
 - 13: 8192 seconds (02:16:32)
 - 14: 16,384 seconds (04:33:04)
 - 15: 32,768 seconds (09:06:08)
 - 16: 65,536 seconds (18:12:16)
 - 17: 131,072 seconds (1d 12:24:32)
 - Omit (Do not set)

❗ If this is set, it must be less than or equal to **Minimum Poll Interval** shown above

- **NTP Graphs:** If enabled, Round Robin Database (RRD) graphs of NTP statistics are available
- **Logging:** These options are available for logging and will be written to the [System Logs](#):
 - **Logging Peer Messages:** If enabled, Peer messages will be logged
 - **Logging System Messages:** If enabled, System messages will be logged
- **Statistics Logging:** Click this button to show more statistics that can also be logged
- **Leap seconds:** Click this button to show a text entry for advanced leap year settings. Leap seconds may be added or subtracted at the end of June or December

❗ Leap seconds are administered by the [IERS](#), who publish them in their Bulletin C approximately 6 - 12 months in advance. Normally this correction should only be needed if the server is a stratum 1 NTP server, but many NTP servers do not advertise an upcoming leap second when other NTP servers synchronise to them

❗ If the leap second is important to your network services, it is good practice to [download and add the leap second file](#) at least a day in advance of any time correction

- **DNS Resolution:** Dropdown to select IP protocol to force NTP peers DNS resolution. Options are:
 - Auto
 - IPv4

- **IPv6**

❗ This does not affect pools

- **Enable NTP Server Authentication:** If enabled, NTPv3 authentication ([RFC 1305](#)) will be activated

❗ This authentication allows the NTP client to confirm it is communicating with the intended server, which protects against man-in-the-middle attacks

Below these options is a **Save** button to save the NTP Settings

ACLs

Overview

Services / NTP / PPS

SettingsACLsPPS

NTP Serial PPS Configuration

Notes

Devices with a Pulse Per Second output such as radios that receive a time signal from DCF77 (DE), JJY (JP), MSF (GB) or WWVB (US) may be used as a PPS reference for NTP. A serial GPS may also be used, but the serial GPS driver would usually be the better option. A PPS signal only provides a reference to the change of a second, so at least one other source to number the seconds is required.

At least 3 additional time sources should be configured under Services > NTP > Settings to reliably supply the time of each PPS pulse.

Serial Port

None

All serial ports are listed, be sure to pick the port with the PPS source attached.

Fudge Time

Fudge time is used to specify the PPS signal offset from the actual second such as the transmission delay between the transmitter and the receiver (default: 0.0).

Stratum

This may be used to change the PPS Clock stratum (default: 0). This may be useful to, for some reason, have ntpd prefer a different clock and just monitor this source.

Minimum Poll Interval

Default

Minimum poll interval for NTP messages. If set, must be less than or equal to Maximum Poll Interval.

Maximum Poll Interval

Default

Maximum poll interval for NTP messages. If set, must be greater than or equal to Minimum Poll Interval.

Flags

☐ Enable falling edge PPS signal processing (default: unchecked, rising edge).

☐ Enable kernel PPS clock discipline (default: unchecked).

☐ Record a timestamp once for each second, useful for constructing Allan deviation plots (default: unchecked).

Clock ID

1 to 4 characters

This may be used to change the PPS Clock ID (default: PPS).

Save

Services / NTP / Settings

This section has [Top Banner Buttons](#)

Access Control List (ACL) is used to define and control access to NTP

The **Services / NTP / ACLs** page is divided into these sections:

Default Access Restrictions Configuration

- **Kiss-o'-death:** Enables/Disables KOD packets. This is enabled by default
- **Modifications:** Enables/Disables denial of run-time Configuration (nomodify) by ntpq and ntpdc. This is enabled by default
- **Queries:** If enabled, this will deny ntpq and ntpdc queries (noquery)
- **Service:** If enabled, this will disable all except ntpq and ntpdc queries (noserve)
- **Peer Association:** If enabled, this will deny packets that attempt a peer association (nopeer). This is enabled by default
- **Trap Service:** If enabled, this will deny mode 6 control message trap service (notrap)

Custom Access Restrictions Configuration

- **Networks** List of Hosts and Subnets with custom settings as explained in the **Default Access Restrictions** section above. Use the **Add** button to add multiple hosts

Below these options is a **Save** button to save the NTP Settings

Overview

[Services](#) / [NTP](#) / [ACLs](#)

[Settings](#)
[ACLs](#)
[PPS](#)

Default Access Restrictions

Kiss-o'-death	☒	Enable KOD packets.
Modifications	☒	Deny run-time Configuration (nomodify) by ntpq and ntpdc.
Queries	☐	Disable ntpq and ntpdc queries (noquery).
Service	☐	Disable all except ntpq and ntpdc queries (noserve).
Peer Association	☒	Deny packets that attempt a peer association (nopeer).
Trap Service	☒	Deny mode 6 control message trap service (notrap).

Custom Access Restrictions

Networks	KOD	nomodify	noquery	noserve	nopeer	notrap	
/ 128 Network/mask	☐	☐	☐	☐	☐	☐	Delete
Add + Add							
Save							

Services / NTP / PPS

This section has [Top Banner Buttons](#)

Pulse Per Second (PPS) is used for compatible devices (ex: radios) to receive a time signal from DCF77 (DE), JJY (JP), MSF (GB) or WWVB (US). It may be used as a PPS reference for NTP

- ❗ A serial GPS may also be used, but the serial GPS driver would usually be the better option

❗ A PPS signal only provides a reference to the change of a second, so at least one other source to number the seconds is required

At least 3 additional time sources should be configured under [NTP Settings](#) to reliably supply the time of each PPS pulse

NTP Serial PPS Configuration Configuration

- **Serial Port:** Dropdown to select the serial port that has the PPS source attached
- **Fudge Time:** Used to specify the PPS signal offset from the actual second such as the transmission delay between the transmitter and the receiver. If left blank, the default is 0
- **Stratum:** Allows the change of the PPS Clock stratum. If left blank, the default is 0

- ❗ This may be useful to, for some reason, have ntpd prefer a different clock and just monitor this source

- **Minimum Poll Interval:** Dropdown to select the minimum poll interval for NTP messages. Options are:
 - **Default**
 - **4: 16 seconds (00:00:16)**
 - **5: 32 seconds (00:00:32)**
 - **6: 64 seconds (00:01:04)**
 - **7: 128 seconds (00:02:08)**
 - **8: 256 seconds (00:04:16)**
 - **9: 512 seconds (00:08:32)**

- 10: 1024 seconds (00:17:04)
- 11: 2048 seconds (00:34:08)
- 12: 4096 seconds (01:08:16)
- 13: 8192 seconds (02:16:32)
- 14: 16,384 seconds (04:33:04)
- 15: 32,768 seconds (09:06:08)
- 16: 65,536 seconds (18:12:16)
- 17: 131,072 seconds (1d 12:24:32)
- Omit (Do not set)

❗ If this is set, it must be less than or equal to **Maximum Poll Interval** shown below

- **Maximum Poll Interval:** Dropdown to select the maximum poll interval for NTP messages. Options are:

- Default
- 4: 16 seconds (00:00:16)
- 5: 32 seconds (00:00:32)
- 6: 64 seconds (00:01:04)
- 7: 128 seconds (00:02:08)
- 8: 256 seconds (00:04:16)
- 9: 512 seconds (00:08:32)
- 10: 1024 seconds (00:17:04)
- 11: 2048 seconds (00:34:08)
- 12: 4096 seconds (01:08:16)
- 13: 8192 seconds (02:16:32)
- 14: 16,384 seconds (04:33:04)
- 15: 32,768 seconds (09:06:08)
- 16: 65,536 seconds (18:12:16)
- 17: 131,072 seconds (1d 12:24:32)
- Omit (Do not set)

❗ If this is set, it must be less than or equal to **Minimum Poll Interval** shown above

- **Flags:** Checkboxes for these options:
 - **Enable falling edge PPS signal processing**
 - **Enable kernel PPS clock discipline**
 - **Record a timestamp once for each second, useful for constructing Allan deviation plots**
- **Clock ID:** Text entry to change the PPS Clock ID. If left blank, **PPS** will be used

Below these options is a **Save** button to save the NTP Settings

SNMP

Overview

Services / SNMP

SNMP Daemon

Enable ☐ Enable the SNMP Daemon and its controls

Services / SNMP

The SNMP (Simple Network Management Protocol) is a standard application-layer protocol for exchanging management information between network devices, allowing for the monitoring and control of network equipment such as routers, switches, and servers

The **Services / SNMP** page is divided into these sections:

SNMP Daemon

- **Enable:** Enables/Disables the SNMP Daemon and its controls

SNMP Daemon Settings

SNMP Daemon Settings

Polling Port

161

Enter the port to accept polling events on (default 161).

System Location

US

System Contact

Joe Blow

Read Community String

public

The community string is like a password, restricting access to querying SNMP to hosts knowing the community string. Use a strong value here to protect from unauthorized information disclosure.

Services / SNMP / SNMP Daemon Settings

- **Polling Port:** The port to accept polling events on (default is 161)
- **System Location:** Text entry for the location. This can be two-letter country code (e.g.: US) or rack location
- **System Contact:** Text entry for contact information (name, email, phone, etc.)
- **Read Community String:** Text string for clients to use to connect and query the SNMP. The default is **public**

❗ It is recommended the **Read Community String** be changed to prevent unauthorized information disclosure

SNMP Traps Enable

Enable ☐ Enable the SNMP Trap and its controls

Services / SNMP / SNMP Traps Enable

- **Enable:** Enables/Disables the SNMP Trap and its controls

SNMP Modules

SNMP modules

☒ MibII
☒ Netgraph
☒ PF
☒ Host Resources
☒ UCD
☒ Regex

Services / SNMP / SNMP Modules

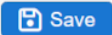
These checkboxes enable/disable these modules:

- **MibII**
- **Netgraph**
- **PF**
- **Host Resources**
- **UCD**
- **Regex**

Interface Binding

Bind Interfaces

All
WAN
LAN
VLAN_VEND



Services / SNMP / Interface Binding

- **Bind Interfaces:** All the device's interfaces are selectable (including the **All** selection) for binding the SNMP

 The `ctrl` and `shift` key can be used to do multi-selection

VPN Overview

Overview

This section contains these types of VPNs:

- IPsec
- L2TP
- [OpenVPN](#)
- [WireGuard](#)

OpenVPN

Overview

The OpenVPN section has these pages:

- [Servers](#)
- [Clients](#)
- [Client Specific Overrides](#)
- [Client Export](#)
- [Shared Key Export](#)
- [OpenVPN Wizard](#)

Servers

Overview

VPN / OpenVPN / Servers					
Servers	Clients	Client Specific Overrides	Client Export	Shared Key Export	Wizards
OpenVPN Servers					

VPN / OpenVPN / Servers

This section has [Top Banner Buttons](#)

This section provides essential information about the OpenVPN server configurations. Adding additional servers will have general server information along with cryptographic settings, tunnel settings, client settings, ping settings, and advanced configuration settings options. The **Configuration** page only has one section:

OpenVPN Servers

Servers	Clients	Client Specific Overrides	Client Export	Shared Key Export	Wizards
OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions

OpenVPN Servers of VPN / OpenVPN / Servers Page

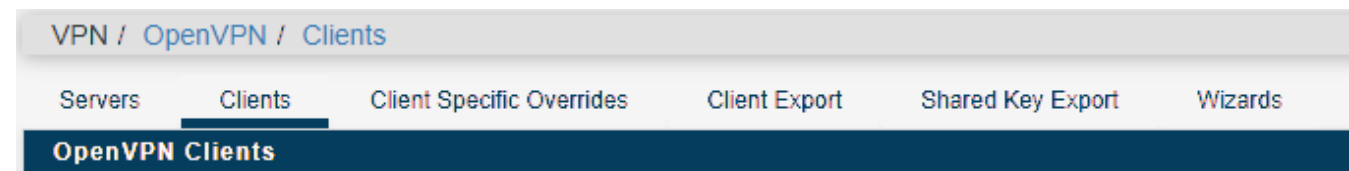
- **Interface:** Network interface of the OpenVPN server
- **Protocol / Port:** Protocol an Port used. The two main protocols used with OpenVPN are UDP and TCP
- **Tunnel Network:** Virtual network segments that are created to facilitate communication between the OpenVPN server and its clients. These tunnel networks are distinct from the physical network infrastructure and allow for the secure transmission of data over public or untrusted networks
- **Mode / Crypto:** The **Device Mode** and **Cryptographic Settings** used
- **Description:** A user-defined label used to identify the purpose or usage of a particular client configuration
- **Actions:** Two buttons   to edit or delete the selected OpenVPN server

Below the **OpenVPN Servers** table is the **Add:** button used to add entries to the table

🔔 Use the [OpenVPN Setup Wizard](#) to create a new OpenVPN server

Clients

Overview



VPN / OpenVPN / Clients

This section has [Top Banner Buttons](#)

This section has information related to the client devices that are currently connected to the OpenVPN server. Adding additional clients will have general information along with user authentication settings, cryptographic settings, tunnel settings, ping settings, and advanced configuration settings options. The **Clients** page only has one section:

OpenVPN Clients



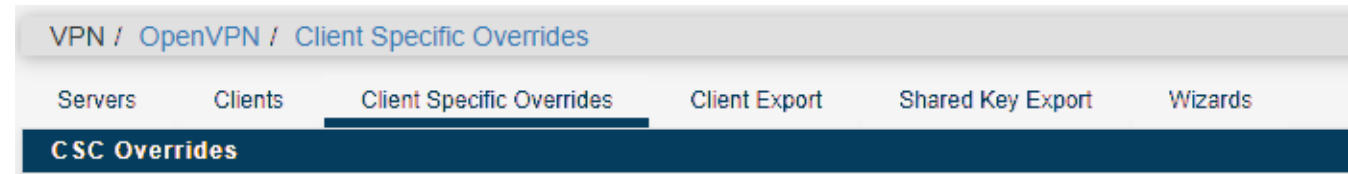
OpenVPN Clients of VPN / OpenVPN / Clients Page

- **Interface:** This refers to a network interface through which OpenVPN communicates with the outside world or with other devices on the network.
- **Protocol:** This refers to the specific protocol used by OpenVPN for creating and managing VPN connections. OpenVPN supports several protocols, each with its own characteristics and benefits. The two main protocols used with OpenVPN are UDP (User Datagram Protocol) and TCP (Transmission Control Protocol)
- **Server:** This is a descriptive name or identifier for the OpenVPN server instance that the client is connected to. This helps distinguish between multiple servers if there are several deployed.
- **Mode/Crypto:** This relates to the configuration options that determine how the VPN tunnels are established and secured. In the **Mode** setting the server is typically set up to listen for incoming connections, while clients initiate connections to the server. In the **Crypto** setting refers to the cryptographic algorithms and settings used to secure VPN connections.
- **Description:** A user-defined label used to identify the purpose or usage of a particular client configuration
- **Actions:** Two buttons   to edit or delete the selected OpenVPN client

Below the **OpenVPN Clients** table is the **Add:** button used to add OpenVPN Clients

Client Specific Overrides

Overview



VPN / OpenVPN / Client Specific Overrides

This section has [Top Banner Buttons](#)

This section allows administrators to define specific configuration settings that apply only to individual client connections. Adding additional client specific overrides will have general information, tunnel settings, and client settings options. The **Client Specific Overrides** page only has one section:

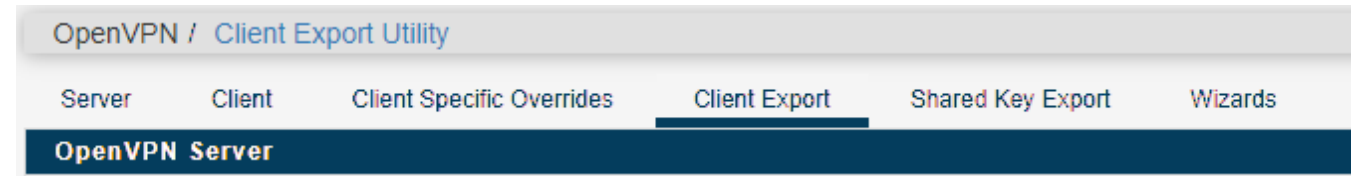
Servers	Clients	Client Specific Overrides	Client Export	Shared Key Export	Wizards
CSC Overrides					
Disabled	Common Name		Description		Actions

CSC Overrides of VPN / OpenVPN / Client Specific Overrides

- **Disabled:** This contains information about whether a particular override rule is enabled or disabled for a specific client
- **Common Name:** This refers to a field within the client's X.509 certificate. The common name serves as an identifier for the client device or entity to which the certificate is issued
- **Description:** This provides a human-readable label or description for each override rule
- **Action:** Two buttons   to edit or delete the selected Client Specific Override

Client Export

Overview

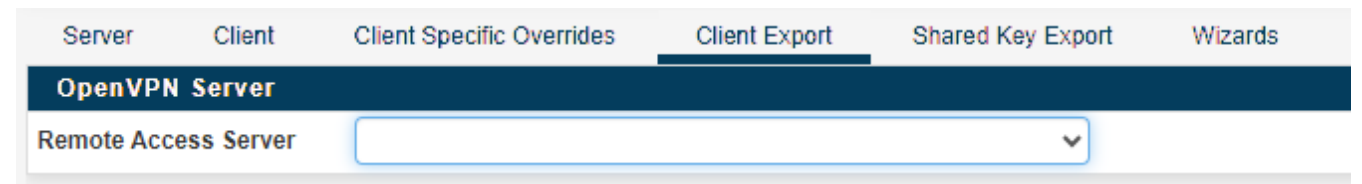


VPN / OpenVPN / Client Export

i The [Client Export Procedure](#) explains how to create OpenVPN Client software installations or configuration exports

This section explains all the ways to export user client software or configuration for the OpenVPN Client software. The **Client Export** page is divided into seven sections:

OpenVPN Server



OpenVPN Server of VPN / OpenVPN / Client Export Page

- **Remote Access Server:** A dropdown to select a specific remote access server

Client Connection Behavior

Client Connection Behavior	
Host Name Resolution	Interface IP Address
Host Name	Enter the hostname or IP address the client will use to connect to this server.
Verify Server CN	Automatic - Use verify-x509-name where possible Optionally verify the server certificate Common Name (CN) when the client connects.
Block Outside DNS	☐ Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.
Legacy Client	☐ Do not include OpenVPN 2.5 settings in the client configuration. When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.
Silent Installer	☐ Create Windows installer for unattended deploy. Create a silent Windows Installer for unattended deploy. Since this installer is not signed, you may need special software to deploy it correctly.
Use Random Local Port	☐ Use a random local source port (lport) for traffic from the client. Without this set, two clients may not run concurrently.

Client Connection Behavior of VPN / OpenVPN / Client Export Page

- **Host Name Resolution:** A dropdown to select which process of converting a human-readable hostname into its corresponding IP address
- **Host Name:** Hostname or IP address the client will use to connect to an [OpenVPN Server](#)
- **Verify Server CN:** Option for verifying the Common Name (CN) attribute in the server's SSL/TLS certificate during a secure connection establishment. This attribute is part of the X.509 certificate used for SSL/TLS encryption.
- **Enable Block Outside DNS:** When checked, blocks access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers

⚠ This requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected

- **Enable Legacy Client:** When checked for older clients (OpenVPN 2.4.x), this can prevent the exporter from placing known-incompatible settings into the client configuration

⚠ When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration

- **Enable Silent Installer:** When checked, this creates a silent Windows Installer for unattended deployment. This installation process runs automatically, typically using predefined settings or configuration options, without displaying any user interface or prompt

⚠ Since this installer is not signed, you may need special software to deploy it correctly

- **Enable Use Random Local Port:** When checked, uses a random local source port (lport) for traffic from the client. Without this set, two clients may not run concurrently

Certificate Export Options

Certificate Export Options	
PKCS#11 Certificate Storage	☐ Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.
PKCS#11 Providers	 Enter the client local path to the PKCS#11 provider(s) (DLL, module), multiple separated by a space character.
PKCS#11 ID	 Enter the object's ID on the PKCS#11 device.
Microsoft Certificate Storage	☐ Use Microsoft Certificate Storage instead of local files.
Password Protect Certificate	☐ Use a password to protect the pkcs12 file contents or key in Viscosity bundle.
Certificate Password	Certificate Password Certificate Password Password used to protect the certificate file contents. Confirm

Certificate Export Options of VPN / OpenVPN / Client Export Page

- **PKCS#11 Certificate Storage:** When checked, a KCS#11 storage device (cryptographic token, HSM, smart card) is used instead of local certificate files. These additional settings are required:
 - **PKCS#11 Providers:** The client local path to the PKCS#11 provider(s) (DLL, module). Multiple providers are allowed by using a space character separator
 - **PKCS#11 ID:** The object's ID on the PKCS#11 device
- **Microsoft Certificate Storage:** When checked, Microsoft Certificate Storage is used instead of local certificate files

- **Password Protect Certificate:** When checked, a password entry (see below) protects pkcs12 file contents or key in Viscosity bundle
 - **Certificate Password:** Password and Verify used to protect certificate file contents

Proxy Options

Proxy Options	
Use A Proxy	☐ Use proxy to communicate with the OpenVPN server.
Proxy Type	HTTP
Proxy IP Address	 Hostname or IP address of proxy server.
Proxy Port	 Port where proxy server is listening.
Proxy Authentication	None
Proxy Username	 Username for authentication to proxy server.
Proxy Password	Proxy Password Proxy Password Confirm

Proxy Options of VPN / OpenVPN / Client Export Page

- **Enable Use a Proxy:** When checked, this opens up the **Proxy Option** subsection options
 - **Proxy Type:** A dropdown to select HTTP or SOCKS proxies to handle network traffic
 - **Proxy IP Address:** IP address assigned to a proxy server
 - **Proxy Port:** Specific network port on a proxy server that is used to listen for and handle incoming connections from client devices
 - **Proxy Authentication:** Dropdown to select the proxy authentication. Options are:
 - **None:** No authentication required
 - **Basic**
 - **NTLM:** For proxy servers that supports NTLM (NT LAN Manager) authentication for client connections
 - **Proxy Username:** Username for proxy access
 - **Proxy Password:** Password and Verify used proxy access

Advanced

Advanced	
Additional configuration options	 Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon. EXAMPLE: remote-random;

Advanced Configuration Options of VPN / OpenVPN / Client Export Page

- **Additional Configuration Options:** A field to enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon

Below the **Advanced** section is the **Save as default:** button used to set the current settings as the standard

Search

Search

Search term

Q Search

↺ Clear

Enter a search string or *nix regular expression to search.

OpenVPN Server of VPN / OpenVPN / Client Export Page

- **Search Term:** a field to enter a search string or nix regular expression to search
- **Search:** and **Clear:** buttons to run queries based on entered criteria and then to remove the entered criteria

OpenVPN Clients

OpenVPN Clients		
User	Certificate Name	Export
Only OpenVPN-compatible user certificates are shown		

OpenVPN Server of VPN / OpenVPN / Client Export Page

- **User:** An individual or entity who is accessing the network through a VPN connection.
- **Certificate Name:** This refers to the common name (CN) or subject name (SN) associated with an SSL/TLS certificate. SSL/TLS certificates are used to authenticate the identity of a website or server and establish secure encrypted connections between clients (such as web browsers) and servers.
- **Export:** Set of buttons to export the user depending on OS and client software requirements. Refer to the [Client Export Procedure](#)

Shared Key Export

Overview

OpenVPN / Shared Key Export

ServerClientClient Specific OverridesClient ExportShared Key ExportWizards

OpenVPN Server

VPN / OpenVPN / Shared Key Export

These are shared key configurations for use in site-to-site tunnels with other routers

i Shared key tunnels are not normally used for remote access connections to end users

OpenVPN Server

ServerClientClient Specific OverridesClient ExportShared Key ExportWizards

OpenVPN Server

Shared Key Server

OpenVPN Server of VPN / OpenVPN / Shared Key Export Page

- Shared Key Server:** A dropdown to select the shared key server

Client Connection Behavior

Client Connection Behavior

Host Name ResolutionInterface IP Address

Host Name

Enter the hostname or IP address the client will use to connect to this server.

Client Connection Behavior of VPN / OpenVPN / Shared Key Export Page

- Host Name Resolution:** A dropdown to select the type of hostname resolution. Options are:
 - Interface IP Address
 - Automatic Mult-WAN IPs (port forward targets)
 - Automatic Mult-WAN DDNS hostnames (port forward targets)
 - Installation hostname
 - Other:** When selected a **Host Name** entry appears to enter the hostname or IP address the client will use to connect to this server
- Host Name:** A text field to enter the host name or IP address the client will use to connect to this server

Proxy Options

Proxy Options	
Use A Proxy	☐ Use proxy to communicate with the OpenVPN server.
Proxy Type	HTTP
Proxy IP Address	Hostname or IP address of proxy server.
Proxy Port	Port where proxy server is listening.
Proxy Authentication	None Choose proxy authentication method, if any.
Proxy Username	Username for authentication to proxy server.
Proxy Password	Password for authentication to proxy server.
Proxy Password (Confirm)	Password for authentication to proxy server.

Proxy Options of VPN / OpenVPN / Shared Key Export Page

- **Enable Use a Proxy:** When checked, this will open up additional proxy options for selection
- **Proxy Type:** A dropdown that allows the selection of either:
 - **HTTP** proxies primarily handle HTTP requests from clients. It can cache web content, filter requests, and provide anonymity by masking the client's IP address
 - **SOCKS** proxies handle various types of traffic, including TCP and UDP. They are commonly used for routing network traffic through a firewall or for anonymizing connections
- **Proxy IP Address:** Enter the hostname or IP address of the proxy server
- **Proxy Port:** Enter the port and where the proxy server is listening
- **Proxy Authentication:** A dropdown to choose a proxy authentication method with these options
 - **None:** No authentication required
 - **Basic**
 - **NTLM** For proxy servers that supports NTLM (NT LAN Manager) authentication for client connections
- **Proxy Username:** Username entry for authentication to the proxy server
- **Proxy Password:** Password entry for authentication to the proxy server
- **Proxy Password (Confirm):** Re-enter the proxy password for confirmation

OpenVPN Shared Key Clients

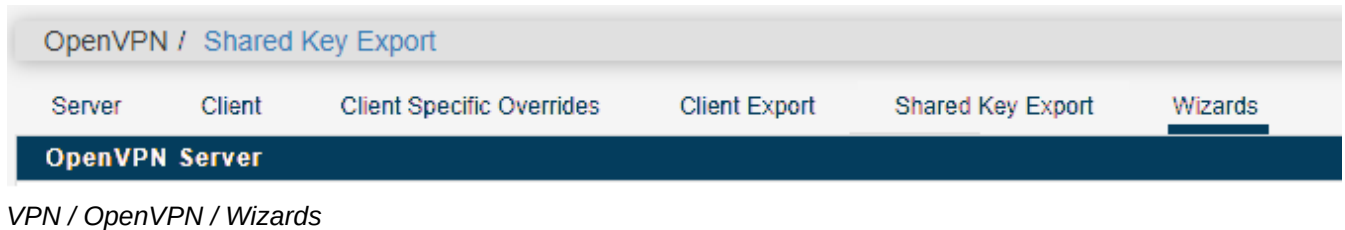
OpenVPN Shared Key Clients	
Client Type	Export

OpenVPN Shared Key Clients of VPN / OpenVPN / Shared Key Export Page

- **Client Type:** The specific type or configuration of VPN clients that will use this shared key for authentication and encryption purposes
- **Export:** An indicator to show whether the shared key can be exported from the VPN server or management interface for use on client devices

OpenVPN Wizards

Overview



OpenVPN Remote Access Server Setup

These are the types of OpenVPN Servers are:

A screenshot of the "Select an Authentication Backend Type" form. The form has a dark blue header with the text "Select an Authentication Backend Type". Below the header is a label "Type of Server" followed by a dropdown menu. The dropdown menu is open and shows the option "Local User Access". Below the dropdown menu is a note: "NOTE: If unsure, leave this set to 'Local User Access.'".

Select an Authentication Backend Type of VPN / OpenVPN / Wizards Page

- **Type of Server:** A dropdown to specify the type or protocol of the authentication server that the VPN or network system will communicate with for user authentication purposes. The choice of server type depends on the capabilities of the VPN or network infrastructure and the requirements of the organization
 - **Local User Access:** The ability of a system or service to authenticate users against a locally managed user database stored on the device or within its own infrastructure, rather than relying on an external authentication server
 - **LDAP:** The Lightweight Directory Access Protocol is used for accessing and maintaining distributed directory information services over a network. It is commonly used for user authentication and authorization in organizations where user account information is stored in a directory service such as Microsoft Active Directory or OpenLDAP
 - **RADIUS:** The Remote Authentication Dial-In User Service is a widely used protocol for providing centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service. It is often used in enterprise environments and supports various authentication methods, including username/password, digital certificates, and more

Refer to the [OpenVPN Wizard Procedure](#) for setting up an OpenVPN Server

WireGuard

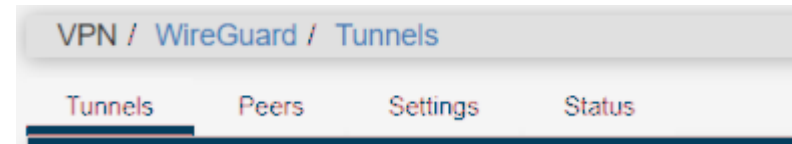
Overview

WireGuard is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography to ensure a secure connection between peers. WireGuard involves setting up [Tunnels](#) and [Peers](#) within those tunnels to facilitate these connections

i For Peer-to-Peer communication, use the [WireGuard Setup Procedure](#) to create a new WireGuard setup

Tunnels

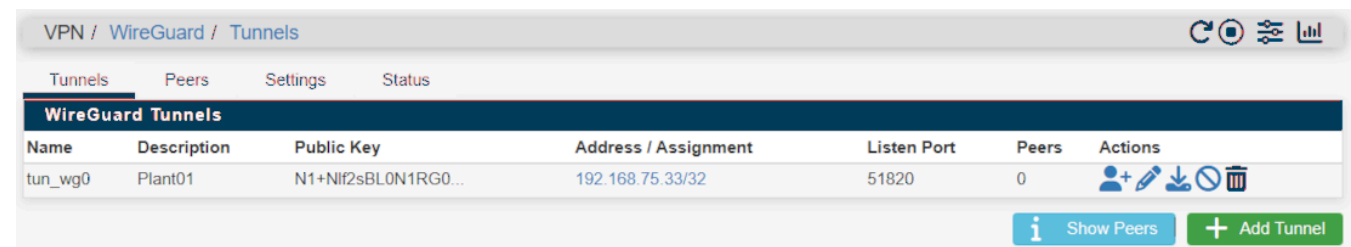
Overview



VPN / WireGuard / Tunnels

This section provides essential information about the WireGuard Tunnel configurations. The **WireGuard Tunnels** page only has one section:

WireGuard Tunnels



VPN / WireGuard / Tunnels Page

- **Name:** Name of the WireGuard tunnel
- **Description:** A user-defined label used to identify the purpose or usage of a particular tunnel configuration
- **Public Key:** A cryptographic identifier used to establish secure, encrypted connections between peers
- **Address/Assignment:** The Interface address and subnet assign to the tunnel
- **Listen Port:** The port used by the tunnel to communicate with peers
- **Peers:** Number of [Peers](#) configured for this tunnel
- **Actions:** These action buttons include the following:
 - : Adds a new [Peer](#)
 - : Edits the tunnel
 - : Downloads the tunnel configuration
 - : Disables the tunnel. While disabled, the button changes to button to enable the tunnel
 - : Deletes the tunnel

Below the **WireGuard Tunnels** table are:

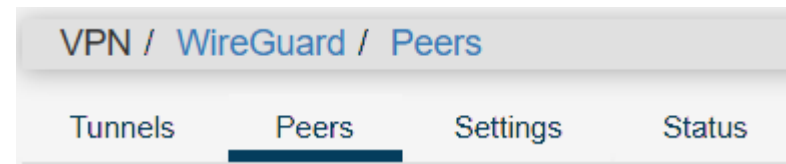
- **Show Peers:** Button to show/hide the [Peers](#) for each tunnel
- **Add Tunnel:** Button to add a new tunnel

When a tunnel is created, a **WireGuard [Interface Group](#)** and **[Firewall Rules Group](#)** are created for use in this tunnel

For Peer-to-Peer communication, use the [WireGuard Setup Procedure](#) to create a new WireGuard setup

Peers

Overview



VPN / WireGuard / Peers

This section provides essential information about the WireGuard Peer configurations. The **WireGuard Peers** page only has one section:

WireGuard Peers



VPN / WireGuard / Peers Page

- **Description:** A user-defined label used to identify the purpose or usage of a particular peer configuration
- **Public key:** A cryptographic identifier used to establish secure, encrypted connections used by the peer
- **Tunnel:** The [Tunnel](#) used by the peer
- **Allow IPs** Like host names and subnets allowed in this peer
- **Endpoint : Port:** The port of the peer's endpoint

i The Endpoint port can be set manually or set to **Dynamic** which will automatically adjust the port number as needed

- **Actions:** These action buttons include the following:
 - : Adds a new peer
 - : Disables the peer. While disabled, the button changes to button to enable the peer

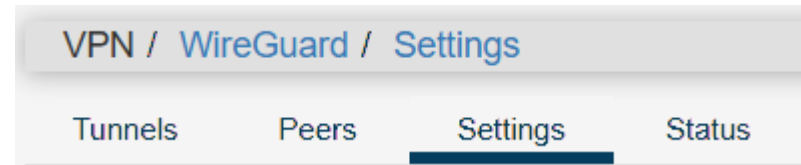
i Disabling a peer will also affect any [Tunnels](#) using this peer

- : Deletes the peer

i For Peer-to-Peer communication, use the [WireGuard Setup Procedure](#) to create a new WireGuard setup

Settings

Overview



VPN / WireGuard / Settings

This section provides essential information about the WireGuard settings. The **WireGuard Setting** page has these sections:

WireGuard Peers

General Settings	
Enable	☒ Enable WireGuard Note: WireGuard cannot be disabled when one or more tunnels is assigned to an interface.
Keep Configuration	☒ Enable Note: With 'Keep Configurations' enabled (default), all tunnel configurations and package settings will persist on install/de-install.
Endpoint Hostname Resolve Interval	300 ☐ Track System Resolve Interval Interval (in seconds) for re-resolving endpoint host/domain names. Note: The default is 300 seconds (0 to disable). Tracks the system 'Aliases Hostnames Resolve Interval' setting. Note: See System > Advanced > Firewall & NAT
Interface Group Membership	All Tunnels ▼ Configures which WireGuard tunnels are members of the WireGuard interface group. Note: Group firewall rules are evaluated before interface firewall rules. Default is 'All Tunnels.'

VPN / WireGuard / General Settings Section

- **Enable:** Enables/Disables the WireGuard service
- **Keep Configuration:** Enables/Disables persistence of all [Tunnel Configurations](#) if the WireGuard package is uninstalled then reinstalled
- **Endpoint Hostname Resolve Interval:** The interval (in seconds) for re-solving endpoint host/domain names. Default is 300
- **Track System Resolve Interval:** Enables/disables tracking of the system

Alias Hostnames Resolve Internal

 setting

See the [System / Advanced / Firewall & NAT](#) for this setting

- **Interface Group Membership:** Dropdown to select which [Tunnels](#) are members of the [WireGuard Interface Group](#). Options are:
 - All Tunnels (default)
 - Only Assigned Tunnels
 - None

Group firewall rules are evaluated before interface firewall rules

User Interface Settings

User Interface Settings

Hide Secrets

☒ Enable

Note: With 'Hide Secrets' enabled, all secrets (private and pre-shared keys) are hidden in the user interface.

 Save

VPN / WireGuard / User Interface Section

- **Hide Secrets:** Enables/Disables whether all secrets (private and pre-shared keys) are hidden in the user interface

Below the **User Interface Settings** table is the  **Save** button to save setting changes

 For Peer-to-Peer communication, use the [WireGuard Setup Procedure](#) to create a new WireGuard setup

Status

Overview

Status / WireGuard

Tunnels

Peers

Settings

Status

Status / WireGuard

This section provides status information about the current WireGuard [Tunnels](#) and package versions. The **WireGuard Status** page has these sections:

WireGuard Status

TunnelsPeersSettingsStatus

WireGuard Status

Tunnel	Description	Peers	Public Key	Address / Assignment	MTU	Listen Port	RX	TX
 tun_wg0	Plant01	0	N1+NIf2sBL0N1RG0...	192.168.75.33/32	1420	51820	0 B	0 B

 Show Peers

Status / WireGuard Status Section

- **Tunnel:** [Tunnel](#) name and it's status of **Up** or **Down**
- **Description:** Optional description of the tunnel
- **Peers:** Number of currently-connected peers
- **Public Key:** Public key used in the tunnel
- **Address/Assignment:** The tunnel address and subnet
- **MTU:** The Maximum Transmission Unit (in bytes) allowed in a single packet
- **Listen Port:** The tunnel's assigned listening port
- **RX:** Number of bytes received
- **TX:** Number of byte transmitted

Below the **WireGuard Status** table is a  **Show Peers** button to show/hide the [Peers](#) for the tunnel

Package Versions

Package Versions		
Name	Version	Comment
wireguard-kmod	0.0.20210606_1	WireGuard implementation for the FreeBSD kernel
wireguard-tools-lite	1.0.20210424	Fast, modern and secure VPN Tunnel (lite flavor)

Status / Package Versions Section

This table shows the **Name**, **Version**, and **Comment** of these two WireGuard Packages:

- **wireguard-kmod**
- **wireguard-tools-lite**

 For Peer-to-Peer communication, use the [WireGuard Setup Procedure](#) to create a new WireGuard setup

Captive Portal

Overview

Status / Captive Portal / ICSdocumentation



Status / Captive Portal

This section has [Top Banner Buttons](#)

This page has settings and data displayed relating to the Captive Portal of the Anybus Defender. The **Status / Captive Portal** page is divided into two sections:

❗ If there are no Captive Portals configured, navigate to [Services -> Captive Portal](#) on the Anybus Defender to configure or set up a captive portal

Captive Portal Zone

Captive Portal Zone

Display ZoneNone

Captive Portal Zone Section of Status / Captive Portal

This section provides users with the option to choose from their created zones from a dropdown menu. Selecting a zone will prompt a section called **Users Logged In** which displays more information regarding the selected zone

❗ If there is only one zone created, the section **Captive Portal Zone** will not display, only the section **Users Logged In(#)** will appear

Users Logged In

Users Logged In (1)				
IP address	MAC address	Username	Session start	Actions
100.101.32.100	30:9c:23:2c:26:14 <i>Micro-Star Intl</i>	Logan	03/27/2024 18:17:27	
			 Show Last Activity	 Disconnect All Users

Users Logged In Section of Status / Captive Portal / ICSdocumentation

❗ The path last part of the path displays the name of the Zone currently being viewed

Within the **Users Logged In** table, the information displayed is as follows:

- **Table Column Headers:**
 - **IP address:** Displays the IP address of the device that is logged into the Anybus Defender
 - **MAC address:** Displays the MAC address of the device that is logged into the Anybus Defender
 - **Username:** Displays the Username that was used to log in
 - **Session Start:** The timestamp indicating when the user's session began

- **Actions:** Provides a  **Delete** button to remove individual users session

Below the **Users Logged In** table are these buttons:

-  **Show Last Activity:** Click this button to display what time the user(s) was last active on the network managed by the Anybus Defender
-  **Disconnect All Users:** Click this button to disconnect all users from the network managed by the Anybus Defender

Dashboard

Overview

❗ Refer to the linked [Dashboard Overview](#) page for more information

DHCP Leases

Overview

Status / DHCP Leases



Status / DHCP Leases

This section has [Top Banner Buttons](#)

The page allows for the user to view and maintain the DHCP Leases on the Anybus Defender The **Status / DHCP Leases** page is divided into three sections:

Search

Search

Search term

All

 Search

 Clear

Enter a search string or *nix regular expression to filter entries.

Search Section of Status / DHCP Leases

- Search Term:** In this search field enter a string or *nix regular expression to filter through DHCP leases that are set up on Anybus Defender
- Search Field Modifier:** Within this dropdown are multiple ways to filter what gets displayed upon clicking the  **Search** button. These are the selectable options,
 - dropdown Options:**
 - IP Address:** Use this option to filter DHCP leases based on specific IP addresses
 - MAC Address:** Use this option to filter DHCP leases based on specific MAC addresses
 - Client ID:** Filter DHCP leases based on the Client ID provided by the device
 - Hostname:** Use this option to filter DHCP leases based on the hostname provided by the device
 - Description:** Filter DHCP leases based on any additional information provided by the device
 - Start:** Filter based on the start time of the DHCP lease
 - End:** Filter based on the end time of the DHCP lease
 - Online:** Filter for only online or offline devices
 - Lease Type:** Filters based on the type of DHCP lease (e.g., dynamic or static)
 - All:** Searches through all data fields returning DHCP leases that pertain to the string or *nix expression that has been input
- The  **Clear** button to the right of the  **Search** button is used to clear the current data that was returned by the initial search

Leases

Leases										
	IP address	MAC address	Client Id	Hostname	Description	Start	End	Online	Lease Type	Actions
✔	100.101.32.100	30:9c:23:2c:26:14 (Micro-Star Intl)			user-DYN-BW35	2024/03/27 17:57:40	2024/03/27 19:57:40	offline	active	+ + 🔌 🗑️

Leases Section of Status / DHCP Leases

❗ Active DHCP leases will display a ✅ **Checkmark** symbol to the left of the DHCP lease. Expired DHCP leases will display a ❌ **Cancel** symbol

Provides a table of all DHCP Leases on the Anybus Defender. There are ten columns in the table:

- **Table Column Headers:**
 - **IP address:** Displays the specific IP addresses assigned to the devices in the DHCP leases
 - **MAC address:** Shows the unique MAC addresses associated with the devices in the DHCP leases
 - **Client ID:** Displays the Client ID provided by the device for identification within the DHCP leases
 - **Hostname:** Shows the hostnames provided by the device within the DHCP leases for easy identification
 - **Description:** Displays additional information about the lease input during DHCP static mapping configuration
 - **Start:** Indicates the start time of each DHCP lease, showing when the IP address assignment began
 - **End:** Indicates the end time of each DHCP lease, showing when the IP address assignment will expire
 - **Online:** Indicates whether the device associated with the DHCP lease is currently online or offline. This changes states depending on if the ip address assigned to that device is receiving or sending packets
 - **Lease Type:** Displays the current status of the lease: active, static, or expired
 - **Actions:** A series of buttons to ➕ **Add** a static mapping, ➕ **Add WOL** mapping, ⏻ **Send WOL** packet, or 🗑 **Delete** the DHCP lease

❗ While a DHCP lease is Online, it cannot be deleted and the 🗑 **Delete** button will be removed as an option

Leases In Use

Leases in Use			
Interface	Pool Start	Pool End	# of leases in use
SDNNET	100.101.32.100	100.101.32.150	1

[+ Show all configured leases](#) [🗑 Clear all DHCP leases](#)

Leases In Use Section of Status / DHCP Leases

A table of active DHCP Leases provided by the Anybus Defender DHCP server. Each row in this table has these columns:

- **Interfaces:** Displays the network interface the DHCP lease is being used on
- **Pool Start:** Shows the start of the range of IP addresses for the [DHCP Server](#)
- **Pool End:** Shows the end of the range of IP addresses for the [DHCP Server](#)
- **# of leases in use:** Displays how many DHCP leases are being used on that interface range

❗ This data can be used to check for address pool exhaustion. Address pool exhaustion is when there are too many clients for the address range available

Below the **Leases In Use** table are these buttons:

- ➕ **Show all configured leases:** Click this button to display all DHCP lease types (active, static, and expired) and click it again to display only active and static leases

❗ Expired DHCP leases are only displayed on the table when the button is clicked to Show all configured leases. Otherwise, they are hidden

- 🗑 **Clear all DHCP leases:** Click this button to clear all DHCP leases on Anybus Defender

DNS Forwarder

Overview

DNS Resolver

Overview

Status / DNS Resolver



Status / DNS Resolver

This section has [Top Banner Buttons](#)

The page displays data regarding the configured DNS Resolver on the Anybus Defender The **Status / DNS Resolver** page is has one section displaying two data tables:

DNS Resolver Infrastructure Cache Speed

DNS Resolver Infrastructure Cache Speed									
Server	Zone	TTL	Ping	Var	RTT	RTO	Timeout A	Timeout AAAA	Timeout Other
198.97.190.53	.	198	0	94	376	376	0	0	0
192.203.230.10	.	198	0	94	376	376	0	0	0
199.7.83.42	.	198	0	94	376	376	0	0	0
199.9.14.201	.	198	0	94	376	376	0	0	0
192.33.4.12	.	198	0	94	376	376	0	0	0
193.0.14.129	.	198	0	94	376	376	0	0	0
202.12.27.33	.	198	0	94	376	376	0	0	0
192.58.128.30	.	198	0	94	376	376	0	0	0
198.41.0.4	.	198	0	94	376	376	0	0	0
199.7.91.13	.	198	0	94	376	376	0	0	0
192.5.5.241	.	198	0	94	376	376	0	0	0
192.36.148.17	.	198	0	94	376	376	0	0	0
192.112.36.4	.	198	0	94	376	376	0	0	0

Status / DNS Resolver / DNS Resolver Infrastructure Cache Speed Table

- This table displays information about the speeds through the configured DNS Resolver on the Anybus Defender:
- **Table Column Headers:**
 - **Zone:** Displays the DNS zone or domain the DNS Resolver is configured to resolve
 - **TTL:** Displays the Time To Live value set for how long a DNS record will be cached before it expires
 - **Ping:** Displays the network latency from the DNS Server
 - **Var:** Displays the deviation in round trip times for ping requests indicating whether the connection is stable
 - **RTT:** Displays the Round Trip Time for ping requests and provides an average value to show the responsiveness of the DNS Server
 - **RTO:** Displays the timeout value in which packets will get retransmitted to the DNS server if the packets are not reaching their destination
 - **Timeout A:** Displays timeout duration for query records on IPv4
 - **Timeout AAAA:** Displays timeout duration for query records on IPv6
 - **Timeout Other:** Displays the timeout duration for other types of DNS records

DNS Resolver Infrastructure Cache Stats

DNS Resolver Infrastructure Cache Stats								
Server	Zone	eDNS Lane Known	eDNS Version	Probe Delay	Lane DNSSEC	Lane Rec	Lane A	Lane Other
198.97.190.53	.	0	0	0	0	0	0	0
192.203.230.10	.	0	0	0	0	0	0	0
199.7.83.42	.	0	0	0	0	0	0	0
199.9.14.201	.	0	0	0	0	0	0	0
192.33.4.12	.	0	0	0	0	0	0	0
193.0.14.129	.	0	0	0	0	0	0	0
202.12.27.33	.	0	0	0	0	0	0	0
192.58.128.30	.	0	0	0	0	0	0	0
198.41.0.4	.	0	0	0	0	0	0	0
199.7.91.13	.	0	0	0	0	0	0	0
192.5.5.241	.	0	0	0	0	0	0	0
192.36.148.17	.	0	0	0	0	0	0	0
192.112.36.4	.	0	0	0	0	0	0	0

Status / DNS Resolver / DNS Resolver Infrastructure Cache Stats Table

This table displays information about the stats through the configured DNS Resolver on the Anybus Defender:

- **Table Column Headers:**
 - **Zone:** Displays the DNS zone or domain the DNS Resolver is configured to resolve
 - **eDNS Lane Known:** Displays the number of servers known by the DNS Resolver in which the servers do not respond with accurate DNS information or fail to properly respond to the DNS queries
 - **eDNS Version:** Displays what version of Extension mechanisms for DNS the server is using(if applicable)
 - **Probe Delay:** Displays the interval between successive probes checking if the DNS Server is available
 - **Lane DNSSEC:** Displays whether the DNS Resolver has detected any servers that are failing to properly validate DNS Security Extensions signatures or provide secure DNS responses
 - **Lane Rec:** Displays the number of lane servers for recursive DNS Resolution
 - **Lane A:** Displays the number of lane servers specifically resolving IPv4 address records
 - **Lane Other:** Displays the number of lane servers specifically resolving other address records. For example AAAA (IPv6) or MX (mail exchange)

Filter Reload

Overview

Status / Filter Reload



Status / Filter Reload

This section has [Top Banner Buttons](#)

This page allows the reload of all the firewall filters and rules for the Anybus Defender. The **Status / Filter Reload** page is divided into one main section and a subsection:

Filter Reload

Filter Reload



Filter Reload Section of Status / Filter Reload

This section has a  **Reload** button that reloads the firewall's current rules and filters.

ⓘ Ensure that reloading is only performed when traffic interruptions are acceptable

Reload Status

Reload status

Reload Status Subsection of Status / Filter Reload

This subsection will display a message that indicates the webpage will refresh after the filters are done reloading.

Gateways

Overview

Status / Gateways



Status / Gateways

This section has [Top Banner Buttons](#)

This page displays data regarding the gateways that are configured on the Anybus Defender. The **Status / Gateways** page has one subsection:

Gateways

Gateways		Gateway Groups					
Gateways							
Name	Gateway	Monitor	RTT	RTTsd	Loss	Status	Description
gateway2	192.168.70.236	192.168.70.236	0ms	0ms	100%	Offline, Packetloss: 100%	
WANGW (default)	192.168.70.1	192.168.70.1	0.213ms	0.03ms	0.0%	Online	

Gateways Section of Status / Gateways

This section features a table displaying information about the configured gateways currently set up on the Anybus Defender:

- **Table Column Headers:**
 - **Name:** Displays the name of the gateway. The default gateway will also have a **(default)** next to the name
 - **Gateway:** Displays the IP address of the gateway
 - **Monitor:** Displays the IP that is being monitored with an ICMP ping to check the gateway status
 - **RTT:** Displays the round trip time for the ICMP packet from the monitoring ping
 - **RTTsd:** Displays the round trip time standard deviation which is the spread of the times from the round trip times for the gateway monitoring ping
 - **Loss:** Displays the packet loss percentage from the gateway monitoring ping
 - **Status:** Displays whether the gateway is currently online or offline along with additional details such as Packetloss or Latency. The offline status may prompt the status as forced
 - **Description:** Displays the description set for the gateway

❗ Disabled gateways will not show up in this table

❗ While a gateway is in a group it cannot be disabled. To disable the gateway, remove it from all groups

Gateway Groups

Overview

Status / Gateways / Gateway Groups

Status / Gateways / Gateway Groups

This section has [Top Banner Buttons](#)

This page displays data regarding the different groups of gateways on the Anybus Defender. The **Status / Gateways** page has one subsection:

Gateway Groups

Gateways Gateway Groups			
Gateway Groups			
Group Name	Gateways		Description
Group1	Tier 1	Tier 2	Group1 of gateways
	WANGW Online		
		gateway2 Offline, Packetloss: 100%	

Gateway Groups Section of Status / Gateways / Gateway Groups

This section features a table displaying information in a table about the configured gateway groups set up on the Anybus Defender:

- **Table Column Headers:**
 - **Group Name:** Displays the name of the group
 - **Gateways:** Displays the names of gateways within the group along with the tier of the group and the status of each gateway
 - **Description:** Displays the description of the group

Hot Standby

Overview

Status / Hot Standby



Status / Hot Standby

This section has [Top Banner Buttons](#)

This page displays the current hot standby configured on the Anybus Defender. The **Status / Hot Standby** page is divided into two sections with two buttons available:

Temp Disable and Maintenance Mode Buttons

There are two buttons above the **Hot Standby Interfaces** section:

- **Hot Standby Mode Buttons:**
 -  **Temporarily Disable/Enable Hot Standby:** Selecting this button temporarily disables the hot standby connection on the Anybus Defender. Once disabled, the button changes to prompt an "Enable Hot Standby" option. Selecting this option restores the hot standby connection
 -  **Enter/Leave Persistent Hot Standby Maintenance Mode:** Selecting this button, you can configure settings for Hot Standby. Any adjustments trigger an automatic switch to the "Enter Persistent Hot Standby Maintenance Mode" state

 While Hot Standby is Temporarily Disabled; if the Anybus Defender reboots, the Temporarily Disabled state will be reset and the Hot Standby status is set back to being Enabled

Hot Standby Interfaces

Hot Standby Interfaces		
Hot Standby Interface	Virtual IP	Status
WAN@1	199.99.99.9/24	 MASTER
LAN@2	192.168.200.79/32	 MASTER

Status / Hot Standby / Hot Standby Interfaces Table View

This section displays a table with details about the Hot Standby connection set up between the current Anybus Defender and one other Anybus Defender. There are three columns in the table:

- **Table Column Headers:**
 - **Hot Standby Interface:** Displays the name of the interface set up for syncing capabilities. The number after the interface name is the VHID group for that interface. For more information about the VHID number, reference the [Firewall / Virtual IP's page](#)
 - **Virtual IP:** Displays the IP address and subnet used for the hot standby connection
 - **Status:** Displays the current status of the connection. Four states can be displayed:
 - **Master:** Displays a  Green Play symbol indicating the connection is the master
 - **Backup:** Displays a  Yellow Pause symbol indicating the connection is a backup for a master
 - **Init:** Displays a  Red Question Mark indicating that the connection is initializing
 - **Disabled:** Indicates a disconnected state with a  black 'X' icon

Hot Standby Sync Nodes

Hot Standby Sync Nodes

Hot Standby Sync nodes:

17a3398d
7aeb8795
810616f6
aa40fc05

Status / Hot Standby / Hot Standby Sync Nodes Table View

This section displays a list of the sync nodes for the Hot Standby connection. The list contains the first eight values of the host's network ID for each node.

Interfaces

Overview

Status / Interfaces

Status / Interfaces

This section has [Top Banner Buttons](#)

This page displays interfaces that are set up on the Anybus Defender. Each Interface receives a section on the page:

Interface(s)

WAN Interface (wan, lgb0)	
Status	up
MAC Address	3c:ec:ef:d4:21:7e - Super Micro Computer
IPv4 Address	192.168.70.62
Subnet mask IPv4	255.255.255.0
Gateway IPv4	192.168.70.1
IPv6 Link Local	fe80::3ecc:eff:fed4:217e%lgb0
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	626930/767385 (21.33 MiB/43.44 MiB)
In/out packets (pass)	626930/767385 (21.33 MiB/43.44 MiB)
In/out packets (block)	289153/4 (49.88 MiB/332 B)
In/out errors	0/0
Collisions	0
SDNMANAGEMENT Interface (lan, lgb1)	
Status	up
MAC Address	3c:ec:ef:d4:21:7a - Super Micro Computer
IPv4 Address	100.100.17.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::3ecc:eff:fed4:217a%lgb1
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	0/0 (0 B/0 B)
In/out packets (pass)	0/0 (0 B/0 B)
In/out packets (block)	0/4 (0 B/312 B)
In/out errors	0/0
Collisions	0
SDNNET Interface (opt1, lgb5)	
Status	up
MAC Address	3c:ec:ef:d4:21:7f - Super Micro Computer
IPv6 Link Local	fe80::3ecc:eff:fed4:217f%lgb5
IPv6 Address	2001:db8:1234:5678::1
Subnet mask IPv6	124
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	0/0 (0 B/0 B)
In/out packets (pass)	0/0 (0 B/0 B)
In/out packets (block)	5231/25522 (730 KiB/4.28 MiB)
In/out errors	0/0
Collisions	0
HOTSTANDBYINTERFACE Interface (opt2, lgb7)	
Status	disabled
DHCP	down Renew HOTSTANDBYINTERFACE
MAC Address	3c:ec:ef:d4:21:81 - Super Micro Computer
PORT7 Interface (opt3, lgb8)	
Status	no carrier
MAC Address	6c:b3:11:69:62:50 - Shenzhen Lianrui Electronics
IPv4 Address	250.1.1.235
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::6eb3:11ff:fe69:6250%lgb8
MTU	1500
Media	autoselect
In/out packets	0/0 (0 B/0 B)
In/out packets (pass)	0/0 (0 B/0 B)
In/out packets (block)	0/5 (0 B/408 B)
In/out errors	0/0
Collisions	0
Using dial-on-demand will bring the connection up again if any packet triggers it. To substantiate this point: disconnecting manually will not prevent dial-on-demand from making connections to the outside! Don't use dial-on-demand if the line is to be kept disconnected.	

Interface Section of Status / Interfaces

For each interface section data about the interface will be displayed. These data points are as follows:

- **Data Points:**
 - **Status:** Displays the current status of the interface. The different status conditions include:
 - **up:** Interface is online and is ready to transmit and receive data
 - **down:** Interface is either offline or there is no IP address
 - **disabled:** Interface has been manually disabled

- **no carrier:** Interface is missing a physical connection

❗ Check both ends of the cable being used if the connection is properly plugged into the Anybus Defender

- **DHCP:** Displays the current status of the DHCP connection and depending on the status varying options may be prompted:
 - **UP:** While in this state these options are prompted:
 -  **Release:** Selecting this button releases the DHCP lease from an interface on the Anybus Defender. When the DHCP lease is released the DHCP server will retain the IP that was assigned to the Anybus Defender and will hold it till the device renews
 - ☐ **Relinquish Checkbox:** Selecting this box and then releasing the DHCP lease deletes the DHCP reservation for the Anybus Defender allowing the DHCP lease to be assigned to other devices
 - **DOWN:** While in this state these options are prompted:
 - A  **Renew Lease:** Selecting this button will reapply the previous DHCP lease, keeping the same IP if it hasn't been reassigned. If the DHCP lease is relinquished, a new IP will be assigned from the DHCP server, which may differ if the previous IP is taken
- **MAC Address:** For Physical Interfaces, this displays the MAC address associated with the NIC on the Anybus Defender. For virtual interfaces, this displays the MAC address that the interface is currently using.
- **IPv4 Address:** Displays the IP address configured on this interface
- **Subnet Mask IPv4:** Displays the subnet configured on this interface
- **Gateway IPv4:** Displays the gateway associated with this interface, if present
- **IPv6 Link Local:** Displays the link-local IPv6 address for the interface
- **IPv6 Address:** Displays the IPv6 address assigned to the interface
- **MTU:** Displays the maximum packet size configured on this interface
- **Media:** Displays the physical type and speed of the connection that is plugged into the interface
- **In/Out Packets:** Displays the packets sent and received through the interface's port
- **In/Out Packets(pass):** Displays the amount of packets that have been allowed through the firewall
- **In/Out Packets(block):** Displays the amount of packets that have been blocked by the firewall
- **In/Out Errors:** Displays the amount of packets that have had an error either coming in or being sent out through the port
- **Collisions:** Displays the number of packets that have experienced collisions on the network connected to the interface

Monitoring

Overview

Monitoring



Status / Monitoring

This section has [Top Banner Buttons](#)

This page displays data about the Anybus Defender. There are three sections on the page:

Settings

Default

Settings

Left Axis	System	Processor			
	Category	Graph			
Right Axis	None				
	Category	Graph			
Options	1 Day	5 Minutes	Line	On	Never
	Time Period	Resolution	Graph Type	Inverse	Refresh Interval
Settings	 Display Advanced  Update Graphs				

Status / Monitoring/ Settings Section

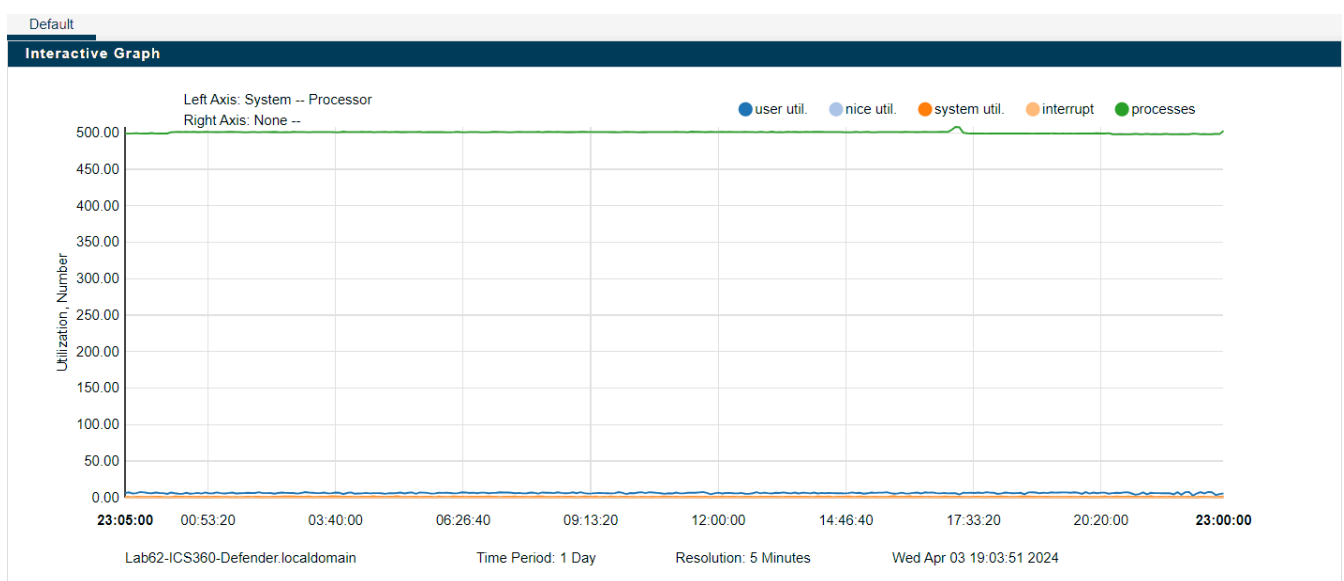
This section provides various dropdown menus. Each menu has different options allowing manipulation of how the graph displays the data. The available settings are as follows:

- **Left Axis / Right Axis:** Two dropdowns are presented:
 - **Category:** The options in this dropdown are **System, Traffic, Packets, Quality, Captive Portal, or None**
 - **Graph:** This dropdown depicts the data points that can be selected depending on the selection from the **Category** dropdown. The options from each **Category** selection are:
 - **System:** Mbuf Clusters, Memory, Processor, and States
 - **Traffic:** These data points are based on the configured interfaces of the Anybus Defender
 - **Packets:** These data points are based on the configured interfaces of the Anybus Defender
 - **Quality:** These data points are based on current connections on the Anybus Defender
 - **Captive Portal:** These data points are based on active Captive Portals of the Anybus Defender
 - **None:** Selecting this category greys out the **Graph** dropdown box removing the Axis that None is selected for from the Interactive Graph
- **Options:** There are five dropdowns to select from:
 - **Time Period:** This controls the length of time that is displayed on the X-Axis
 - **Resolution:** This setting controls how often a data point is taken
 - **Graph Type:** This changes the style of the graph in which the Interactive Graph is displayed
 - **Inverse:** Default, this option is set to **Off**. If the graph needs to be inversed, setting inverse to **On** will flip the graph
 - **Refresh Interval:** This option controls how often the graph is updated
- **Settings:** Clicking the  **Display Advanced** button displays some extra buttons to configure the Monitoring page:

- **Save View Button:** Saves any changes made to the settings of the graph
- **+ Add View Button:** Prompts the user to name the new view. Once a name is input and the **OK** button is selected in the prompt, a new tab is created. If the button is selected while nothing is input in the prompt and **OK** is selected, a new tab is not created
- **Remove View Button:** Removes the current view that is selected
- **Disable Graphing Button:** Disables graphing for all view pages
- **Reset Data Button:** Clears the RRD data and generates new RRD files
- **Update Graphs Button:** This applies any changes made within the settings to the Interactive Graph

❗ Ensure the **Update Graphs** button has been selected after configuring the settings. The graph does not automatically update upon changing settings and requires the button to be selected for the graph to update based on the configured settings

Interactive Graph



Interactive Graph Section of Status / Monitoring

This section provides an interactive graph displaying data about the Anybus Defender:

- **Graph Data:**
 - **Color Legend:** Displays which color on the graph attributes to the respective data. Clicking on a color will remove that data from the graph while double-clicking a color will show only that data, hiding the others
 - **Y-axis:** Left and Right Y-axes display data based on what has been set within the **Settings** section
 - **X-axis:** Displays the time period that data is being displayed. This is configurable within the **Settings** section
 - **Supplementary Data:** Below the X-Axis four additional information points about the graph data:
 - **Bottom Left:** Displays the name that has been set to the Anybus Defender
 - **Time Period Setting:** Displays the Time Period that has been set in the **Settings** section. This determines how much data within a certain amount of time that is depicted on the graph
 - **Resolution Setting:** Displays the Resolution that was set in the **Settings** section depicting the interval in which data is captured
 - **Bottom Right:** Displays the current date and time

Data Summary

Data Summary					
	Minimum	Average	Maximum	Last	95th Percentile
user util.	2.56 %	6.11 %	7.58 %	5.66 %	
nice util.	0.00 %	0.01 %	0.08 %	0.00 %	
system util.	0.28 %	0.94 %	1.63 %	1.30 %	
interrupt	0.00 %	0.03 %	0.22 %	0.00 %	
processes	498.00	500.65	508.21	502.84	
					

Data Summary Table Section of Status / Monitoring

The table in this section displays a table of percentage values for the data points currently being monitored by the graph. The table values are controlled by the Time Period the graph is set to. Within the table are five columns:

- **Table Column Headers:**
 - **Minimum:** Displays the lowest data point value
 - **Average:** Displays the average value based on all the current data points
 - **Maximum:** Displays the highest data point value
 - **Last:** Displays the most recent tracked data point
 - **95th Percentile:** Displays the value that is most prevalent out of 95 percent of the data points tracked

 The  **Information** button provides more insight about the Monitoring page and some additional functionalities the interactive graph provides

NTP

Overview

Status / [NTP](#)

Status / NTP

This section has [Top Banner Buttons](#)

This page displays a data table with columns covering the status of the Network Time Protocol server being used for the Anybus Defender. There is one section on this page:

Network Time Protocol Status

Network Time Protocol Status										
Status	Server	Ref ID	Stratum	Type	When	Poll (s)	Reach	Delay (ms)	Offset (ms)	Jitter (ms)
Pool Placeholder	pool.ntp.org	.POOL.	16	p	-	64	0	0.000	+0.000	0.000

Status / NTP / Data Table

- **Table Columns:**
 - **Status:** This shows the current status of the NTP server
 - **Server:** Displays the IP address of the NTP server being used
 - **Ref ID:** Displays the reference ID based on the Stratum number and gives vital context about the source the time is being acquired from
 - **Stratum:** Displays the number of layers between the NTP server and the device
 - **Type:** Displays a letter representing the type of NTP server being used
 - **When:** Displays the last time the NTP server output information to the device
 - **Poll(s):** Interval at which the NTP server is checked
 - **Reach:** Displays a value indicating if the NTP server is being reached successfully or not
 - **Delay(ms):** Displays the delay in milliseconds while communicating to the NTP server
 - **Offset(ms):** Displays the time difference in milliseconds between the device and the NTP server
 - **Jitter(ms):** Displays the time difference in milliseconds of information returning from the NTP server

OpenVPN

Overview

Status / OpenVPN

Status / OpenVPN

This section has [Top Banner Buttons](#)

The **Status / OpenVPN** page has one section per OpenVPN server with a subsection providing additional details:

Client Connections Table

For each OpenVPN server that has been configured, there is a Client Connections table. Within the table are seven columns of data about connected client(s):

Sample OpenVPN UDP4:1194 Client Connections: 2

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received	Cipher	
emartin emartin	192.168.70.160:65192	10.0.10.3	2024-04-18 14:29:34	5 KiB	56 KiB	AES-128-CBC	
lhalloran lhalloran	192.168.70.160:1194	10.0.10.2	2024-04-18 14:29:11	5 KiB	83 KiB	AES-128-CBC	

Status: Actions:

Status / OpenVPN / Client Connections Table

- **Table Column Headers:**
 - **Common Name:** Shows the username attributed to the connected client
 - **Real Address:** Displays the IP address and port the client is using to access the OpenVPN server
 - **Virtual Address:** Displays the IP address assigned by the OpenVPN server to the client to facilitate local connections
 - **Connected Since:** Displays the date and time when the client started their connection to the OpenVPN server
 - **Bytes Sent:** Displays the total value of bytes that have been sent by the client to the OpenVPN server
 - **Bytes Received:** Displays the total value of bytes that the OpenVPN server has received from the client
 - **Cipher:** Displays the configured Data Encryption method that was used for the connection between the client and the OpenVPN server
- **Status and Action Panel:**
 - **Status:** Displays the current state of the OpenVPN server and displays these icons along with the respective action button(s):
 - **Operational Indicator:** Indicates that the OpenVPN server is running and connected. Action button(s) available while this status is present:
 - **Restart-Service:** Restarts the OpenVPN server prompting any client connected to log in again
 - **Stop-Service:** This sets the OpenVPN server to the down status preventing any clients from connecting
 - **Down Indicator:** Indicates that the OpenVPN server is not running or is down. Action button(s) available while this status is present:
 - **Start-Service:** Clicking this will start the OpenVPN server setting the status to the operational state allowing clients to connect to the OpenVPN server

Routing Table

While there are clients connected to the OpenVPN server there is a  **Show Routing Table** button. Selecting this button presents a table with four columns of data about the routed connections:

Sample OpenVPN UDP4:1194 Routing Table			
Common Name	Real Address	Target Network	Last Used
emartin	192.168.70.160:65192	10.0.10.3	2024-04-18 14:29:36
lhalloran	192.168.70.160:1194	10.0.10.2	2024-04-18 14:29:14

An IP address followed by C indicates a host currently connected through the VPN.

Status / OpenVPN / Routing Table

- **Table Column Headers:**
 - **Common Name:** Displays the connected client's username
 - **Real Address:** Displays the IP address of the device the client is using to connect to the OpenVPN server
 - **Target Network:** Displays the target network the OpenVPN server is routing the client to
 - **Last Used:** Displays the time the connected client had last used the connection to the OpenVPN server

Services

Overview

Status / [Services](#)

Status / Services

This section has [Top Banner Buttons](#)

The Services page gives a brief overview of any services that have been configured on the Anybus Defender. The **Status / Services** page has one section:

Services

Presented in this section is a table populated with services on the Anybus Defender

Services			
Service	Description	Status	Actions
bsnmpd	SNMP Service	✓	↺ ⏸ ⏹
dpinger	Gateway Monitoring Daemon	✓	↺ ⏸ ⏹ 📊 📋
identifyasset	Asset Management	✗	▶
pcscd	PC/SC Smart Card Daemon	✓	↺ ⏸
remote_management	Remote Management	✓	↺ ⏸
snort	Snort IDS/IPS Daemon	✗	▶
sshd	Secure Shell Daemon	✓	↺ ⏸
syslogd	System Logger Daemon	✓	↺ ⏸ ⏹ 📊 📋
unbound	DNS Resolver	✓	↺ ⏸ ⏹ 📊 📋
wireguard	WireGuard	⚠	⏹ 📊

Status / Services / Services Table

There are four columns of data regarding the services:

- **Table Column Headers:**
 - **Service:** Displays the name of the service
 - **Description:** Provides a brief overview of the service
 - **Status:** Two icons indicate the current state of the service:
 - **Operational:** depicted by an **✓ Operational Indicator** that is a green checkmark
 - **Down:** Depicted by a **✗ Down Indicator** that is a red 'x'
 - **Actions:** For more information on the action buttons, check out the Universal Buttons section

System Logs

Overview

This section has [Top Banner Buttons](#)

This page displays logs from various Anybus Defender services. The **Status / System Logs / System** page has four subsections:

- System Subsections:
 - General:** Displays logs about the Anybus Defender giving insight into how the unit is functioning
 - Gateways:** Displays logs generated by the interfaces that are configured on the Anybus Defender
 - Routing:** Displays logs generated by any routing that is being handled by the Anybus Defender
 - DNS Resolver:** Displays logs generated by the DNS services that are on the Anybus Defender

System Subsections Logs Table

General	Gateways	Routing	DNS Resolver
Last 500 General Log Entries. (Maximum 500)			
Time	Process	PID	Message
2024-04-17 17:25:02.955957+00:00	kernel	-	le0: <AMD PCnet-PCI> port 0x2000-0x207f irq 18 at device 4.0 on pci2
2024-04-17 17:25:02.955965+00:00	kernel	-	le0: 16 receive buffers, 4 transmit buffers
2024-04-17 17:25:02.955972+00:00	kernel	-	le0: Ethernet address: 00:0c:29:81:b0:e7
2024-04-17 17:25:02.955979+00:00	kernel	-	le1: <AMD PCnet-PCI> port 0x2080-0x20ff irq 19 at device 5.0 on pci2
2024-04-17 17:25:02.955985+00:00	kernel	-	le1: 16 receive buffers, 4 transmit buffers
2024-04-17 17:25:02.955992+00:00	kernel	-	le1: Ethernet address: 00:0c:29:81:b0:f1
2024-04-17 17:25:02.955999+00:00	kernel	-	pcib3: <ACPI PCI-PCI bridge> at device 21.0 on pci0
2024-04-17 17:25:02.956006+00:00	kernel	-	pcib3: [GIANT-LOCKED]
2024-04-17 17:25:02.956013+00:00	kernel	-	pcib4: <ACPI PCI-PCI bridge> at device 21.1 on pci0
2024-04-17 17:25:02.956020+00:00	kernel	-	pcib4: [GIANT-LOCKED]
2024-04-17 17:25:02.956027+00:00	kernel	-	pcib5: <ACPI PCI-PCI bridge> at device 21.2 on pci0
2024-04-17 17:25:02.956034+00:00	kernel	-	pcib5: [GIANT-LOCKED]
2024-04-17 17:25:02.956041+00:00	kernel	-	pcib6: <ACPI PCI-PCI bridge> at device 21.3 on pci0
2024-04-17 17:25:02.956048+00:00	kernel	-	pcib6: [GIANT-LOCKED]

Status / System Logs / System / Log Table Layout

Each subsection has an identical layout for the table which provides details on the logs that are being collected. There are four columns for the tables:

- Table Column Headers:
 - Time:** Displays the time at which the log entry was taken
 - Process:** Displays the type of log entry
 - PID:** Displays the unique identifier associated with the log entry
 - Message:** Provides a brief overview of each log entries contents, see above for specific message contents

Filter/Manage Logs Sections

For each of the subsections, there are two additional buttons:

- Filter Logs Section

Advanced Log Filter

Time

Process

PID

Quantity

Message

[Regular expression reference](#)
 Precede with exclamation (!) to exclude match.

Apply Filter

Status / System Logs / System / Filter Logs Section

This section provides a way for the user to filter through the list of log entries. After completing the filter entries, click the green **Apply Filter** button to show the filtered log. These are some ways that the logs can be filtered:

- Filter Logs Options:**
 - Time:** Entering a date and/or time will display any logs with the matching data in the **Time** column
 - Process:** Entering in a specific process style will display any logs matching that within the **Process** column
 - PID:** Entering in a PID value will display any logs matching the value within the **PID** column
 - Quantity:** This allows for the control of how many logs are displayed regarding the number of filtered logs that are being displayed
 - Message:** Entering a log message will display any logs that match within the **Message** column
- Manage Logs Section**

Manage General Log

Forward/Reverse Display

Forward

Reverse

General Logging Options Setting

(newest at bottom)

(newest at top)

Show log entries in forward or reverse order.

GUI Log Entries

500

This is the number of log entries displayed in the GUI. It does not affect how many entries are contained in the log.

Log Rotation Size (Bytes)

512000

This field controls the size at which logs will be rotated. By default this is per log file.

NOTE: Log file sizes are checked once per minute to determine if rotation is necessary, so a very rapidly growing log file may exceed this value.

Log Retention Count

7

The number of log files to keep before the oldest copy is removed on rotation.

Formatted/Raw Display

Formatted

Raw

General Logging Options Setting

Show the log entries as formatted or raw output as generated by the service. The raw output will reveal more detailed information, but it is more difficult to read.

Web Server Log

Log errors from the web server process

If this is checked, errors from the nginx web server process for the GUI or Captive Portal will appear in the system log.

Action

Save

Clear log

Saves changed settings.

Clears local log file and reinitializes it as an empty log. Save any settings changes first.

Status / System Logs / System / Manage Logs Section

This section allows for the management of how the logs are displayed. These configuration fields can be:

Manage Logs Options:

- Forward/Reverse Display:** Change the order in which the logs are displayed within the table. There are three options:
 - Forward:** Displays the newest logs at the bottom, old logs at the top
 - Reverse:** Displays the newest logs at the top, old logs at the bottom
 - General Logging Options Settings:** Displays the default way in which logs are ordered
- GUI Log Entries:** Changes the total number of logs that are displayed within the log entries table
- Log Rotation Size (Bytes):** Changes the amount of bytes till a log entry is rotated out. The default value is per log file. This value is checked once per minute to determine if rotation is necessary
- Log Retention Count:** Controls the number of log files kept till the oldest copy is removed during rotation
- Formatted/Raw Display:** Changes the way the log entries are displayed. There are three options:
 - Formatted:** Displays a more structured and organized format of the log entries

- **Raw:** Displays a more detailed log entry but makes the log entries more difficult to read. This selection only displays a **Time** and **Message** column
- **General Logging Options Setting:** Displays the log entries in a default style
- **Web Server Log:** Allows for the log entry of any errors from the nginx web server process for the GUI or captive portal. This option is only available in the settings page for the **General** subsection
- **Action:** There are two buttons in this area:
 -  **Save:** Select this button to save any changes made within the settings section
 -  **Clear Log:** Select this button to clear the local log file and reinitialize it as an empty log. Please ensure all settings are saved before proceeding

 In the table, clicking on the header of the 'Time' column sorts the logs chronologically. The default order is oldest to newest. Meanwhile, the other three columns enable sorting by grouping logs according to their respective names

Firewall Logs

Overview

This page provides logs gathered from different functionalities within the Firewall dropdown on the Anybus Defender. The **Status / System Logs / Firewall** page has three subsections:

Normal View

Status / System Logs / Firewall / Normal View



Status / System Logs / Firewall

This section has [Top Banner Buttons](#)

Normal View Table

Normal View	Dynamic View	Summary View			
Last 500 Firewall Log Entries. (Maximum 500)					
Action	Time	Interface	Source	Destination	Protocol
✖	2024-04-19 12:45:02.495946+00:00	WAN	 192.168.70.234:54915	 192.168.70.255:54915	UDP
✖	2024-04-19 12:45:02.496016+00:00	WAN	 192.168.70.167:57621	 192.168.70.255:57621	UDP
✖	2024-04-19 12:45:02.496047+00:00	WAN	 192.168.70.153:57621	 192.168.70.255:57621	UDP
✖	2024-04-19 12:45:03.493472+00:00	WAN	 192.168.70.234:54915	 192.168.70.255:54915	UDP
✖	2024-04-19 12:45:04.499869+00:00	WAN	 192.168.70.234:54915	 192.168.70.255:54915	UDP
✖	2024-04-19 12:45:04.499907+00:00	WAN	 0.0.0.0:68	 255.255.255.255:67	UDP
✖	2024-04-19 12:45:04.499921+00:00	WAN	 192.168.70.34:67	 255.255.255.255:68	UDP
✖	2024-04-19 12:45:05.493190+00:00	WAN	 192.168.70.234:54915	 192.168.70.255:54915	UDP
✖	2024-04-19 12:45:06.499768+00:00	WAN	 192.168.70.234:54915	 192.168.70.255:54915	UDP
✖	2024-04-19 12:45:07.499851+00:00	WAN	 192.168.70.4	 224.0.0.1	ICMP
✖	2024-04-19 12:45:07.499895+00:00	WAN	 192.168.70.234:54915	 192.168.70.255:54915	UDP
✖	2024-04-19 12:45:08.500235+00:00	WAN	 192.168.70.234:54915	 192.168.70.255:54915	UDP
✖	2024-04-19 12:45:08.500311+00:00	WAN	 192.168.70.154:137	 192.168.70.255:137	UDP
✖	2024-04-19 12:45:09.493351+00:00	WAN	 192.168.70.234:54915	 192.168.70.255:54915	UDP
✖	2024-04-19 12:45:09.493425+00:00	WAN	 192.168.70.90:138	 192.168.70.255:138	UDP
✖	2024-04-19 12:45:10.499526+00:00	WAN	192.168.70.234:54915	192.168.70.255:54915	UDP

Status / System Logs / System / Normal View

This subsection presents logs displaying blocked communications by the Anybus Defender. The **Status / System Logs / Firewall / Normal View** has a table with six columns:

- **Table Column Headers:**
 - **Action:** Displays the type of action the firewall enacted onto the connection. The table defaults to displaying blocked connections. There are two symbols used to depict the action that was taken:
 - **Allowed:** Displays a green check mark
 - **Blocked:** Displays a red 'x'
 - **Time:** Displays the time at which the log was taken
 - **Interface:** Presents the interface in which the log was gathered
 - **Rule:** Depicts the Rule that was enacted onto the connection
 - **Source:** Displays the IP address and port of the device attempting to gain access through the Anybus Defender. In this column are two buttons:
 -  **Resolve:** The Resolve Button has the Anybus Defender reaches out to the DNS server and validates the IP address. Once validated it displays the **hostname** underneath any instance within the log table. If the

IP address is not validated it displays **Cannot Resolve**

- **Add to Block List:** This Easy Rule button enables the creation of a specific block rule for the source IP associated with the button. Refer to the firewall documentation for more information about firewall rules
- **Destination:** Displays the IP address and port of the endpoint location that the Source IP address was attempting to reach.
- **Resolve:** The Resolve Button has the Anybus Defender reaches out to the DNS server and validates the IP address. Once validated it displays the **hostname** underneath any instance within the log table. If the IP address is not validated it displays **Cannot Resolve**
- **Pass This Traffic:** This Easy Rule button enables the creation of a specific allow rule for the source IP associated with the button. Refer to the firewall documentation for more information about firewall rules
- **Protocol:** Displays the type of communication that the connection was using

❗ In the table, clicking on the header of the 'Time' column sorts the logs chronologically. The default order is oldest to newest. Meanwhile, the other three columns enable sorting by grouping logs according to their respective names

Dynamic View

This subsection displays an identical table to the one in the **Normal View** subsection. The difference is that the **Dynamic View** table has no action buttons and instead presents the option to pause the table from updating with new logs. This is depicted at the top by a Pause check box. Reference the **Normal View** subsection for more details on the column headers

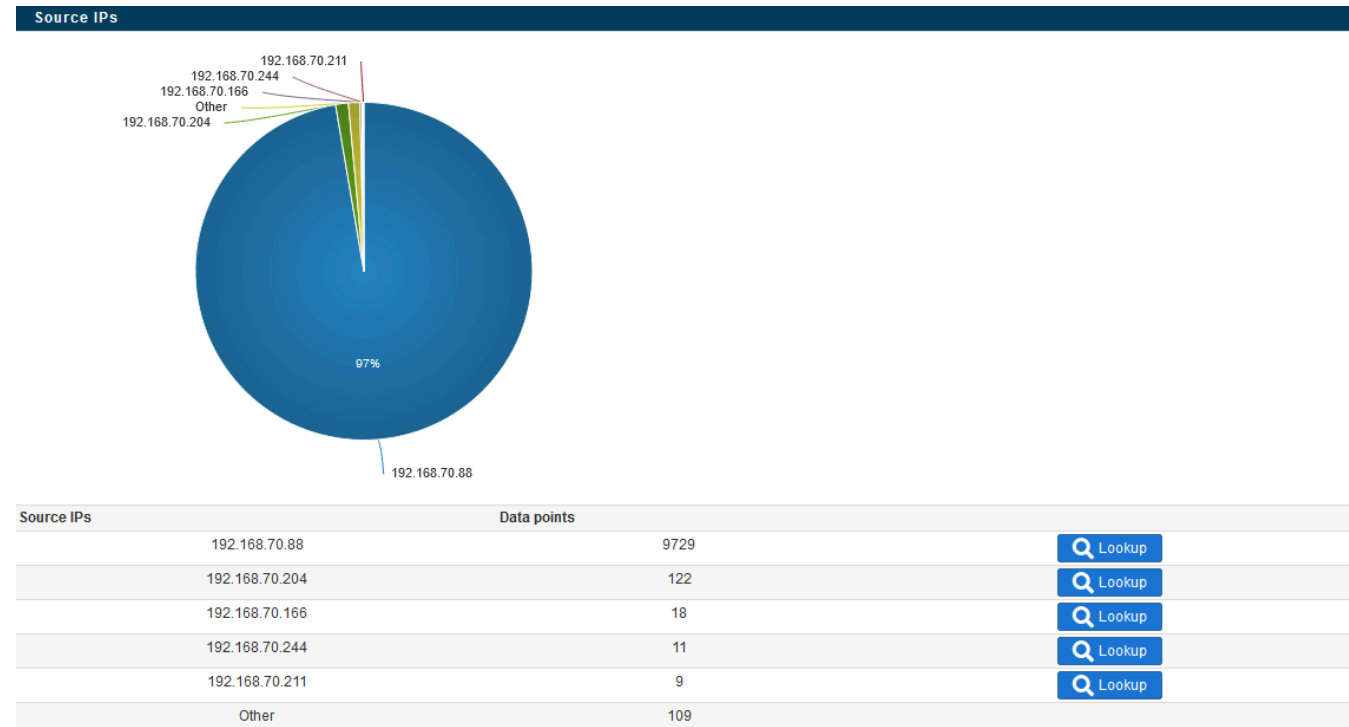
Dynamic View Table

Normal ViewDynamic ViewSummary View					
Last 500 Firewall Log Entries. (Maximum 500) Pause ☐					
Action	Time	Interface	Source	Destination	Protocol
	2024-04-19 17:11:17.446185+00:00	WAN	192.168.70.28:137	192.168.70.255:137	UDP
	2024-04-19 17:11:17.446251+00:00	WAN	192.168.70.234:54915	192.168.70.255:54915	UDP
	2024-04-19 17:11:18.447285+00:00	WAN	192.168.70.28:137	192.168.70.255:137	UDP
	2024-04-19 17:11:18.447327+00:00	WAN	192.168.70.28:137	192.168.70.255:137	UDP
	2024-04-19 17:11:18.447344+00:00	WAN	192.168.70.234:54915	192.168.70.255:54915	UDP
	2024-04-19 17:11:18.447357+00:00	WAN	192.168.35.14:40097	255.255.255.255:4680	UDP
	2024-04-19 17:11:18.447370+00:00	WAN	192.168.35.14:40097	255.255.255.255:4680	UDP
	2024-04-19 17:11:19.447608+00:00	WAN	192.168.70.234:54915	192.168.70.255:54915	UDP
	2024-04-19 17:11:20.448225+00:00	WAN	192.168.70.234:54915	192.168.70.255:54915	UDP
	2024-04-19 17:11:21.448771+00:00	WAN	192.168.70.199:138	192.168.70.255:138	UDP
	2024-04-19 17:11:21.448830+00:00	WAN	192.168.70.234:54915	192.168.70.255:54915	UDP
	2024-04-19 17:11:22.449566+00:00	WAN	192.168.70.234:54915	192.168.70.255:54915	UDP
	2024-04-19 17:11:23.445843+00:00	WAN	192.168.70.234:54915	192.168.70.255:54915	UDP

❗ In the table, clicking on the header of the 'Time' column sorts the logs chronologically. The default order is oldest to newest. Meanwhile, the other three columns enable sorting by grouping logs according to their respective names

Summary View

Pie Chart View



This subsection displays a pie chart-style summary of multiple firewall processes. Each pie chart has two columns giving a brief insight into the data being displayed:

- **Table Column Headers:**
 - **Left Column:** This column is labeled with the name of the section. Within the column are the topics from the section from which data is taken from
 - **Right Column:** This column is labeled Data Points. Within this column are the number of data points taken from each topic. The graph combines these data points into a pie graph that displays the total percentage for each data type

There are seven sections within the Summary View page:

- **Actions:** The two topics displayed in this are Pass and Block
- **Interfaces:** Displays interfaces that are active and getting log entries
- **Protocols:** Displays the communication protocols that are being used to communicate to or from the Anybus Defender
- **Source IPs:** Displays any source IP addresses that are communicating through the Anybus Defender
- **Destination IPs:** Displays any Destination IP addresses that are being communicated with through the Anybus Defender
- **Source Ports:** Displays any ports that Source IP addresses are using to communicate through the Anybus Defender
- **Destination Ports:** Displays the protocol port value the connection is using to communicate

Sections with IP addresses, each topic receives an additional capability of a 🔍 **Lookup** button. This takes the user to the Diagnostic / DNS Lookup page, populating the Hostname with the IP this button was selected from. Click the link for more information on the aforementioned page

Filter/Manage Logs Sections

For each of the subsections, there are two additional buttons:

- **Filter Logs Section**

Advanced Log Filter

Time

Process

PID

500

Quantity

Message

Apply Filter

Regular expression reference

Precede with exclamation (!) to exclude match.

Status / System Logs / Firewall / Filter Logs Section

This section provides a way for the user to filter through the list of log entries. After completing the filter entries, click the green **Apply Filter** button to show the filtered log. There are five ways that the logs can be filtered:

- **Filter Logs Options:**
 - **Time:** Entering a date and/or time will display any logs with the matching data in the **Time** column
 - **Process:** Entering in a specific process style will display any logs matching that within the **Process** column
 - **PID:** Entering in a PID value will display any logs matching the value within the **PID** column
 - **Quantity:** This allows for the control of how many logs are displayed regarding the number of filtered logs that are being displayed
 - **Message:** Entering a log message will display any logs that match within the **Message** column
- **Manage Logs Section**

Manage Firewall Log

These settings override the "General Logging Options" settings.

Forward/Reverse Display

Forward

(newest at bottom)

Reverse

(newest at top)

General Logging Options Setting

Show log entries in forward or reverse order.

GUI Log Entries

500

This is the number of log entries displayed in the GUI. It does not affect how many entries are contained in the log.

Log Rotation Size (Bytes)

512000

This field controls the size at which logs will be rotated. By default this is per log file.

Log Retention Count

7

NOTE: Log file sizes are checked once per minute to determine if rotation is necessary, so a very rapidly growing log file may exceed this value.

The number of log files to keep before the oldest copy is removed on rotation.

Formatted/Raw Display

Formatted

Raw

General Logging Options Setting

Show the log entries as formatted or raw output as generated by the service. The raw output will reveal more detailed information, but it is more difficult to read.

Log firewall default blocks

Log packets matched from the default block rules in the ruleset

Packets that are blocked by the implicit default block rule will not be logged if this option is unchecked. Per-rule logging options are still respected.

Log packets matched from the default pass rules put in the ruleset

Packets that are allowed by the implicit default pass rule will be logged if this option is checked. Per-rule logging options are still respected.

Log packets blocked by 'Block Bogon Networks' rules

Log packets blocked by 'Block Private Networks' rules

Where to show rule descriptions

Display as column

Show the applied rule description below or in the firewall log rows. Displaying rule descriptions for all lines in the log might affect performance with large rule sets.

Action

Save

Saves changed settings.

Clear log

Clears local log file and reinitializes it as an empty log. Save any settings changes first.

Status / System Logs / Firewall / Manage Logs Section

This section allows for the management of how the logs are displayed. These configuration fields can be:

- **Manage Logs Options:**

- **Forward/Reverse Display:** Change the order in which the logs are displayed within the table. There are three options:
 - **Forward:** Displays the newest logs at the bottom, old logs at the top
 - **Reverse:** Displays the newest logs at the top, old logs at the bottom
 - **General Logging Options Settings:** Displays the default way in which logs are ordered
- **GUI Log Entries:** Changes the total number of logs that are displayed within the log entries table
- **Log Rotation Size (Bytes):** Changes the amount of bytes till a log entry is rotated out. The default value is per log file. This value is checked once per minute to determine if rotation is necessary
- **Log Retention Count:** Controls the number of log files kept till the oldest copy is removed during rotation
- **Formatted/Raw Display:** Changes the way the log entries are displayed. There are three options:
 - **Formatted:** Displays a more structured and organized format of the log entries
 - **Raw:** Displays a more detailed log entry but makes the log entries more difficult to read. This selection only displays a **Time** and **Message** column
 - **General Logging Options Setting:** Displays the log entries in a default style
- **Log Firewall Default Blocks:** Prompts a few options on different logs that the user may or may not want to be displayed/ omitted from the log entries table
- **Where To Show Rule Descriptions:** A dropdown that has three selections for how the user would like the rule descriptions to be displayed:
 - **Display as Column**
 - **Dont Load Descriptions**
 - **Display As Second Row**
- **Action:** There are two buttons in this area:
 -  **Save:** Select this button to save any changes made within the settings section
 -  **Clear Log:** Select this button to clear the local log file and reinitialize it as an empty log. Please ensure all settings are saved before proceeding

DHCP Logs

Overview

Status / System Logs / DHCP

Status / System Logs / DHCP

This section has [Top Banner Buttons](#)

This page provides logs gathered from the DHCP dropdown on the Anybus Defender. The **Status / System Logs / DHCP** page has one table:

DHCP Table

System	Firewall	DHCP	Authentication	IPsec	PPP	L2TP Server	OpenVPN	NTP	Industrial	Packages	Settings
Last 17 DHCP Log Entries. (Maximum 500)											
Time	Process	PID	Message								
2024-03-14 13:27:18.941874+00:00	dhclient	7509	Cannot open or create pidfile: No such file or directory								
2024-03-14 13:27:18.944871+00:00	dhclient	8358	PREINIT								
2024-03-14 13:27:18.951563+00:00	dhclient	7509	DHCPREQUEST on le0 to 255.255.255.255 port 67								
2024-03-14 13:27:18.952190+00:00	dhclient	7509	DHCPACK from 192.168.188.254								
2024-03-14 13:27:18.954226+00:00	dhclient	9345	REBOOT								
2024-03-14 13:27:18.955518+00:00	dhclient	9775	Starting add_new_address()								
2024-03-14 13:27:18.956268+00:00	dhclient	10032	ifconfig le0 inet 192.168.188.129 netmask 255.255.255.0 broadcast 192.168.188.255								
2024-03-14 13:27:18.960918+00:00	dhclient	10272	New IP Address (le0): 192.168.188.129								
2024-03-14 13:27:18.961573+00:00	dhclient	10404	New Subnet Mask (le0): 255.255.255.0								
2024-03-14 13:27:18.962230+00:00	dhclient	10505	New Broadcast Address (le0): 192.168.188.255								
2024-03-14 13:27:18.962874+00:00	dhclient	10616	New Routers (le0): 192.168.188.2								

Status / System Logs / DHCP / Log Table Layout

In the DHCP section, logs are provided. There are four columns for the table:

- **Table Column Headers:**
 - **Time:** Displays the time at which the log entry was taken
 - **Process:** Displays the type of log entry
 - **PID:** Displays the unique identifier associated with the log entry
 - **Message:** Provides a brief overview of each log entries contents, see above for specific message contents

Filter/Manage Logs Sections

For the DHCP section, there are two additional buttons:

- **Filter Logs Section**

Advanced Log Filter

Time

Process

PID

500

Quantity

Message

Apply Filter

Regular expression reference Precede with exclamation (!) to exclude match.

Status / System Logs / DHCP / Filter Logs Section

This section provides a way for the user to filter through the list of log entries. After completing the filter entries, click the green **Apply Filter** button to show the filtered log. There are five ways that the logs can be filtered:

- **Filter Logs Options:**

- **Time:** Entering a date and/or time will display any logs with the matching data in the **Time** column
- **Process:** Entering in a specific process style will display any logs matching that within the **Process** column
- **PID:** Entering in a PID value will display any logs matching the value within the **PID** column
- **Quantity:** This allows for the control of how many logs are displayed regarding the number of filtered logs that are being displayed
- **Message:** Entering a log message will display any logs that match within the **Message** column

- **Manage Logs Section**

Manage DHCP Log

These settings override the "General Logging Options" settings.

Forward/Reverse Display

☐ Forward

☐ Reverse

☒ General Logging Options Setting

(newest at bottom)

(newest at top)

Show log entries in forward or reverse order.

GUI Log Entries

This is the number of log entries displayed in the GUI. It does not affect how many entries are contained in the log.

Log Rotation Size (Bytes)

This field controls the size at which logs will be rotated. By default this is per log file.

NOTE: Log file sizes are checked once per minute to determine if rotation is necessary, so a very rapidly growing log file may exceed this value.

Log Retention Count

The number of log files to keep before the oldest copy is removed on rotation.

Formatted/Raw Display

☐ Formatted

☐ Raw

☒ General Logging Options Setting

Show the log entries as formatted or raw output as generated by the service. The raw output will reveal more detailed information, but it is more difficult to read.

Action

Saves changed settings.

Clears local log file and reinitializes it as an empty log. Save any settings changes first.

Status / System Logs / DHCP / Manage Logs Section

This section allows for the management of how the logs are displayed. These configuration fields can be:

- **Manage Logs Options:**

- **Forward/Reverse Display:** Change the order in which the logs are displayed within the table. There are three options:
 - **Forward:** Displays the newest logs at the bottom, old logs at the top
 - **Reverse:** Displays the newest logs at the top, old logs at the bottom
 - **General Logging Options Settings:** Displays the default way in which logs are ordered
- **GUI Log Entries:** Changes the total number of logs that are displayed within the log entries table
- **Log Rotation Size (Bytes):** Changes the amount of bytes till a log entry is rotated out. The default value is per log file. This value is checked once per minute to determine if rotation is necessary
- **Log Retention Count:** Controls the number of log files kept till the oldest copy is removed during rotation
- **Formatted/Raw Display:** Changes the way the log entries are displayed. There are three options:
 - **Formatted:** Displays a more structured and organized format of the log entries
 - **Raw:** Displays a more detailed log entry but makes the log entries more difficult to read. This selection only displays a **Time** and **Message** column
 - **General Logging Options Setting:** Displays the log entries in a default style
- **Action:** There are two buttons in this area:
 - **Save:** Select this button to save any changes made within the settings section
 - **Clear Log:** Select this button to clear the local log file and reinitialize it as an empty log. Please ensure all settings are saved before proceeding

❗ In the table, clicking on the header of the 'Time' column sorts the logs chronologically. The default order is oldest to newest. Meanwhile, the other three columns enable sorting by grouping logs according to their respective names

Authentication Logs

Overview

This page provides logs gathered from different functionalities within the Authentication dropdown on the Anybus Defender. The **Status / System Logs / Authentication** page has four subsections:

General

In the General section, logs are provided. The table has four columns:

General Log Table

General	Captive Portal Auth	L2TP Logins	OS User Events	OS Account Changes
Last 74 General Log Entries. (Maximum 500)				
Time	Process	PID	Message	
2024-03-14 13:28:26.946978+00:00	login	1131	login on ttyv0 as admin	
2024-03-14 13:28:26.947023+00:00	login	1131	ROOT LOGIN (admin) ON ttyv0	
2024-03-14 13:36:58.468982+00:00	php-fpm	66311	/index.php: Successful login for user 'admin' from: 192.168.201.79 (Local Database)	
2024-03-25 14:06:52.447708+00:00	login	77799	login on ttyv0 as admin	
2024-03-25 14:06:52.447757+00:00	login	77799	ROOT LOGIN (admin) ON ttyv0	
2024-03-25 14:08:31.548369+00:00	php-fpm	28007	/index.php: Successful login for user 'admin' from: 192.168.201.1 (Local Database)	
2024-03-25 15:52:50.519063+00:00	php-fpm	56751	/system.php: Successful login for user 'admin' from: 192.168.201.1 (Local Database)	
2024-03-25 19:52:55.000452+00:00	date	14794	date set by root	
2024-03-25 20:44:30.701409+00:00	sshd	11172	Server listening on :: port 22.	
2024-03-25 20:44:30.705469+00:00	sshd	11172	Server listening on 0.0.0.0 port 22.	
2024-03-25 20:51:55.410466+00:00	shutdown	92074	power-down by root:	
2024-03-26 01:43:16.629199+00:00	sshd	43354	Server listening on :: port 22.	
2024-03-26 01:43:16.629810+00:00	sshd	43354	Server listening on 0.0.0.0 port 22.	
2024-03-26 01:43:47.712863+00:00	php-fpm	40377	/index.php: Successful login for user 'admin' from: 192.168.201.1 (Local Database)	

Status / System Logs / Authentication / General / Log Table

This section has [Top Banner Buttons](#)

- **Table Column Headers:**
 - **Time:** Displays the time at which the log entry was taken
 - **Process:** Displays the type of log entry
 - **PID:** Displays the unique identifier associated with the log entry
 - **Message:** Provides a brief overview of each log entries contents, see above for specific message contents

Captive Portal Authentication

In the General section, there is a table displaying log entries. The table has four columns:

General	Captive Portal Auth	L2TP Logins	OS User Events	OS Account Changes
Last 2 Captive Portal Auth Log Entries. (Maximum 500)				
Time	Process	PID	Message	
2024-03-26 15:09:17.456254+00:00	logportalauth	6485	Zone: documentation - Reconfiguring captive portal(documentation).	
2024-04-16 19:02:34.333942+00:00	logportalauth	65336	Zone: testing_for_docu - Reconfiguring captive portal(Testing_For_Docu).	

Status / System Logs / Authentication / Captive Portal Authentication / Log Table

- **Table Column Headers:**
 - **Time:** Displays the time at which the log entry was taken
 - **Process:** Displays the type of log entry
 - **PID:** Displays the unique identifier associated with the log entry

- **Message:** Provides a brief overview of each log entries contents, see above for specific message contents

Filter/Manage Logs Sections

With the General and Captive Portal Authentication subsections, there are two additional buttons:

- **Filter Logs Section**

Advanced Log Filter			
			500
Time	Process	PID	Quantity
			Apply Filter
Message			
Regular expression reference Precede with exclamation (!) to exclude match.			

Status / System Logs / Authentication / Filter Logs Section

This section provides a way for the user to filter through the list of log entries. After completing the filter entries, click the green **Apply Filter** button to show the filtered log. There are five ways that the logs can be filtered:

- **Time:** Entering a date and/or time will display any logs with the matching data in the **Time** column
- **Process:** Entering in a specific process style will display any logs matching that within the **Process** column
- **PID:** Entering in a PID value will display any logs matching the value within the **PID** column
- **Quantity:** This allows for the control of how many logs are displayed regarding the number of filtered logs that are being displayed
- **Message:** Entering a log message will display any logs that match within the **Message** column
- **Manage Logs Section**

Manage General Log	
These settings override the "General Logging Options" settings.	
Forward/Reverse Display	☐ Forward (newest at bottom) ☐ Reverse (newest at top) ☒ General Logging Options Setting
Show log entries in forward or reverse order.	
GUI Log Entries	500 This is the number of log entries displayed in the GUI. It does not affect how many entries are contained in the log.
Log Rotation Size (Bytes)	512000 This field controls the size at which logs will be rotated. By default this is per log file. NOTE: Log file sizes are checked once per minute to determine if rotation is necessary, so a very rapidly growing log file may exceed this value.
Log Retention Count	7 The number of log files to keep before the oldest copy is removed on rotation.
Formatted/Raw Display	☐ Formatted ☐ Raw ☒ General Logging Options Setting
Show the log entries as formatted or raw output as generated by the service. The raw output will reveal more detailed information, but it is more difficult to read.	
Web Server Log	☒ Log errors from the web server process If this is checked, errors from the nginx web server process for the GUI or Captive Portal will appear in the system log.
Action	Save Clear log
Saves changed settings. Clears local log file and reinitializes it as an empty log. Save any settings changes first.	

Status / System Logs / Authentication / Manage Logs Section

This section allows for the management of how the logs are displayed. These configuration fields can be:

- **Forward/Reverse Display:** Change the order in which the logs are displayed within the table. There are three options:
 - **Forward:** Displays the newest logs at the bottom, old logs at the top
 - **Reverse:** Displays the newest logs at the top, old logs at the bottom
 - **General Logging Options Settings:** Displays the default way in which logs are ordered
- **GUI Log Entries:** Changes the total number of logs that are displayed within the log entries table
- **Log Rotation Size (Bytes):** Changes the amount of bytes till a log entry is rotated out. The default value is per log file. This value is checked once per minute to determine if rotation is necessary
- **Log Retention Count:** Controls the number of log files kept till the oldest copy is removed during rotation

- **Formatted/Raw Display:** Changes the way the log entries are displayed. There are three options:
 - **Formatted:** Displays a more structured and organized format of the log entries
 - **Raw:** Displays a more detailed log entry but makes the log entries more difficult to read. This selection only displays a **Time** and **Message** column
 - **General Logging Options Setting:** Displays the log entries in a default style
- **Web Server Log:** Allows for the log entry of any errors from the nginx web server process for the GUI or captive portal. This option is only available in the settings page for the **General** subsection
- **Action:** There are two buttons in this area:
 -  **Save:** Select this button to save any changes made within the settings section
 -  **Clear Log:** Select this button to clear the local log file and reinitialize it as an empty log. Please ensure all settings are saved before proceeding

OS User Events

This subsection gives log entries on OS user events on the Anybus Defender. There are three sections:

Advanced Log Filter

Advanced Log Filter

500

Login Time

Duration

TTY

Quantity

User/Message

Apply Filter

Regular expression reference

Precede with exclamation (!) to exclude match.

Status / System Logs / Authentication / OS User Events / Filter Logs

This section provides a way for the user to filter through the list of log entries. Once the desired data the user wants to filter by is filled in, filtering will be enacted once the green  **Apply Filter** button is selected. There are five ways that the logs can be filtered:

- **Filter Section**
 - **Login Time:** Entering a date and/or time will display any logs with the matching data in the **Time** column
 - **Duration:** Entering a specific duration will display any logs matching that within the **Duration** column
 - **TTY:** Entering a TTY style will display any logs matching the value within the **TTY** column
 - **Quantity:** This allows for the control of how many logs are displayed regarding the number of filtered logs that are being displayed
 - **User/Message:** Entering a log user/message will display any logs that match within the **User/Message** column

User Log Entries Table

Last 21 OS User Events Log Entries. (Maximum 500)			
Login Time	Duration	TTY	User/Message
Tue Jan 16 18:04			shutdown time
Tue Jan 16 18:08			shutdown time
Tue Jan 16 18:11			shutdown time
Tue Jan 16 20:09 - 20:14	00:04	pts/0	admin
Wed Jan 17 14:47	35+05:11	ttyv0	admin
Wed Feb 21 19:58	00:00	ttyv0	admin
Wed Feb 21 19:59			shutdown time
Wed Feb 21 20:10 - 20:36	00:26	ttyv0	admin
Wed Feb 21 20:36 - still logged in		ttyv0	root
Wed Feb 21 20:40 - 22:02	01:22	pts/0	admin
Tue Mar 5 16:37 - still logged in		ttyv0	root
Tue Mar 5 18:27 - still logged in		ttyv0	root
Tue Mar 5 18:38 - 18:54	00:16	ttyv0	root
Tue Mar 5 18:54 - still logged in		ttyv0	root
Wed Mar 6 22:30 - 22:37	00:07	pts/0	admin

[Status](#) / [System Logs](#) / [Authentication](#) / [OS User Events](#) / [User Event Log Entries Table](#)

This section provides a table that displays a table populated with events done by users. There are four columns:

- **Table Column Headers:**
 - **Login Time:** Displays the day, month, date, and time at which a user was logged in for when the event was logged
 - **Duration:** Displays the duration of the event that had taken place
 - **TTY:** Displays the style in which the user was connected
 - **User/Message:** Displays the username of the user and a message about what event took place

Managed OS Events Log

Manage OS User Events Log

These settings override the "General Logging Options" settings.

Forward/Reverse Display

☐ Forward
(newest at bottom)

☐ Reverse
(newest at top)

☒ General Logging Options Setting

Show log entries in forward or reverse order.

GUI Log Entries

This is the number of log entries displayed in the GUI. It does not affect how many entries are contained in the log.

Log Rotation Size (Bytes)

This field controls the size at which logs will be rotated. By default this is per log file.

NOTE: Log file sizes are checked once per minute to determine if rotation is necessary, so a very rapidly growing log file may exceed this value.

Log Retention Count

The number of log files to keep before the oldest copy is removed on rotation.

Formatted/Raw Display

☐ Formatted

☐ Raw

☒ General Logging Options Setting

Show the log entries as formatted or raw output as generated by the service. The raw output will reveal more detailed information, but it is more difficult to read.

Action

Save

Clear log

Saves changed settings.

Clears local log file and reinitializes it as an empty log. Save any settings changes first.

[Status](#) / [System Logs](#) / [Authentication](#) / [OS User Events](#) / [Manage Logs](#)

This section allows for the management of how the logs are displayed. Six areas can be configured:

Manage Logs Section:

- **Forward/Reverse Display:** Change the order in which the logs are displayed within the table. There are three options:
 - **Forward:** Displays the newest logs at the bottom, old logs at the top
 - **Reverse:** Displays the newest logs at the top, old logs at the bottom
 - **General Logging Options Settings:** Displays the default way in which logs are ordered
- **GUI Log Entries:** Changes the total number of logs that are displayed within the log entries table
- **Log Rotation Size (Bytes):** Changes the amount of bytes till a log entry is rotated out. The default value is per log file. This value is checked once per minute to determine if rotation is necessary
- **Log Retention Count:** Controls the number of log files kept till the oldest copy is removed during rotation

- **Formatted/Raw Display:** Changes the way the log entries are displayed. There are three options:
 - **Formatted:** Displays a more structured and organized format of the log entries
 - **Raw:** Displays a more detailed log entry but makes the log entries more difficult to read. This selection only displays a **Time** and **Message** column
 - **General Logging Options Setting:** Displays the log entries in a default style
- **Action:** There are two buttons in this area:
 -  **Save:** Select this button to save any changes made within the settings section
 -  **Clear Log:** Select this button to clear the local log file and reinitialize it as an empty log. Please ensure all settings are saved before proceeding

OS Account Changes

This section displays a table with log entries based on User Account changes. This subsection has three sections:

Advanced Log Filter

Log Filter

Filter Expression

Regular expression reference Precede with exclamation (!) to exclude match.

500

Quantity

Apply Filter

Status / System Logs / Authentication / OS Account Changes / Filter Logs

This section provides a way for the user to filter through the list of log entries. Once the desired data the user wants to filter by is filled in, filtering will be enacted once the green  **Apply Filter** button is selected. There are two ways that the logs can be filtered:

- **Filter Options:**
 - **Filter Expression:** Entering an expression will display any logs that match within the **Message** column
 - **Quantity:** This allows for the control of how many logs are displayed regarding the number of filtered logs that are being displayed

OS Account Changes Log Entries

Last 160 OS Account Changes Log Entries. (Maximum 500)	
Time	Message
2023-12-26 00:29:27	[root:groupadd] messagebus(556)
2023-12-26 00:29:27	[root:useradd] messagebus(556):messagebus(556):D-BUS Daemon User:/nonexistent/usr/sbin/nologin
2023-12-26 00:29:38	[root:groupadd] dhcpd(136)
2023-12-26 00:29:38	[root:useradd] dhcpd(136):dhcpd(136):ISC DHCP daemon:/nonexistent/usr/sbin/nologin
2024-01-16 18:07:16	[unknown:groupadd] all(1998)
2024-01-16 18:07:16	[unknown:usermod] root(0):wheel(0):Charlie &:/root/bin/sh
2024-01-16 18:07:16	[unknown:useradd] admin(0):wheel(0):System Administrator:/root/etc/rc.initial
2024-01-16 18:07:16	[unknown:useradd] admin(0) home /root made
2024-01-16 18:07:16	[unknown:groupmod] all(1998)
2024-01-16 18:07:16	[unknown:groupadd] admins(1999)
2024-01-16 18:10:39	[unknown:userdel] admin(0) account removed
2024-01-16 18:10:39	[unknown:groupmod] all(1998)
2024-01-16 18:10:39	[unknown:usermod] root(0):wheel(0):Charlie &:/root/bin/sh

Status / System Logs / Authentication / OS Account Changes / Log Table

In this section, there is a table that displays log entries. The table has two columns:

- **Table Column Headers:**
 - **Time:** Displays the date and time the log entry was collected
 - **Message:** Displays a message in expression form providing details from the log

Manage OS Account Changes Log

Manage OS User Events Log

These settings override the "General Logging Options" settings.

Forward/Reverse Display

☐ Forward
(newest at bottom)
 ☐ Reverse
(newest at top)

☒ General Logging Options Setting

Show log entries in forward or reverse order.

GUI Log Entries

This is the number of log entries displayed in the GUI. It does not affect how many entries are contained in the log.

Log Rotation Size (Bytes)

This field controls the size at which logs will be rotated. By default this is per log file.

NOTE: Log file sizes are checked once per minute to determine if rotation is necessary, so a very rapidly growing log file may exceed this value.

Log Retention Count

The number of log files to keep before the oldest copy is removed on rotation.

Formatted/Raw Display

☐ Formatted
 ☐ Raw

☒ General Logging Options Setting

Show the log entries as formatted or raw output as generated by the service. The raw output will reveal more detailed information, but it is more difficult to read.

Action

Saves changed settings.

Clears local log file and reinitializes it as an empty log. Save any settings changes first.

Status / System Logs / Authentication / OS User Events / Manage Logs

This section allows for the management of how the logs are displayed. Six areas can be configured:

Manage Logs Options:

- Forward/Reverse Display:** Change the order in which the logs are displayed within the table. There are three options:
 - Forward:** Displays the newest logs at the bottom, old logs at the top
 - Reverse:** Displays the newest logs at the top, old logs at the bottom
 - General Logging Options Settings:** Displays the default way in which logs are ordered
 - GUI Log Entries:** Changes the total number of logs that are displayed within the log entries table
 - Log Rotation Size (Bytes):** Changes the amount of bytes till a log entry is rotated out. The default value is per log file. This value is checked once per minute to determine if rotation is necessary
 - Log Retention Count:** Controls the number of log files kept till the oldest copy is removed during rotation
 - Formatted/Raw Display:** Changes the way the log entries are displayed. There are three options:
 - Formatted:** Displays a more structured and organized format of the log entries
 - Raw:** Displays a more detailed log entry but makes the log entries more difficult to read. This selection only displays a **Time** and **Message** column
 - General Logging Options Setting:** Displays the log entries in a default style
 - Action:** There are two buttons in this area:
 - Save:** Select this button to save any changes made within the settings section
 - Clear Log:** Select this button to clear the local log file and reinitialize it as an empty log. Please ensure all settings are saved before proceeding

In the table, clicking on the header of the 'Time' column sorts the logs chronologically. The default order is oldest to newest. Meanwhile, the other three columns enable sorting by grouping logs according to their respective names

OpenVPN Logs

Overview

Status / System Logs / OpenVPN

Status / System Logs / OpenVPN

This section has [Top Banner Buttons](#)

This page provides logs gathered from OpenVPN on the Anybus Defender. The **Status / System Logs / OpenVPN** page has one section:

OpenVPN Log Table

Overview

This table displays the log from OpenVPN. There are four table columns:

System	Firewall	DHCP	Authentication	IPsec	PPP	L2TP Server	OpenVPN	NTP	Industrial	Packages	Settings
Last 52 OpenVPN Log Entries. (Maximum 500)											
Time	Process	PID	Message								
2024-04-18 12:28:49.427309+00:00	openvpn	92492	OpenVPN 2.5.2 amd64-portbld-freebsd12.2 [SSL (OpenSSL)] [LZO] [LZ4] [MH/RECVDA] [AEAD] built on Dec 8 2023								
2024-04-18 12:28:49.427771+00:00	openvpn	92492	library versions: OpenSSL 1.1.1k-freebsd 25 Mar 2021, LZO 2.10								
2024-04-18 12:28:49.429355+00:00	openvpn	92756	GDG: problem writing to routing socket								
2024-04-18 12:28:49.429418+00:00	openvpn	92756	NOTE: the current --script-security setting may allow this configuration to call user-defined scripts								
2024-04-18 12:28:49.498293+00:00	openvpn	92756	WARNING: experimental option --capath /var/etc/openvpn/server1/ca								
2024-04-18 12:28:49.498561+00:00	openvpn	92756	TUN/TAP device ovpn1 exists previously, keep at program end								
2024-04-18 12:28:49.498909+00:00	openvpn	92756	TUN/TAP device /dev/tun1 opened								
2024-04-18 12:28:49.499859+00:00	openvpn	92756	ioctl(TUNSIFMODE): Device busy (errno=16)								
2024-04-18 12:28:49.499912+00:00	openvpn	92756	/sbin/ifconfig ovpn1 10.0.10.1 10.0.10.2 mtu 1500 netmask 255.255.255.0 up								
2024-04-18 12:28:49.509190+00:00	openvpn	92756	/usr/local/sbin/ovpn-linkup ovpn1 1500 1621 10.0.10.1 255.255.255.0 init								
2024-04-18 12:28:49.534139+00:00	openvpn	92756	UDPv4 link local (bound): [AF_INET]199.99.99.99:1194								
2024-04-18 12:28:49.534770+00:00	openvpn	92756	UDPv4 link remote: [AF_UNSPEC]								
2024-04-18 12:28:49.534924+00:00	openvpn	92756	Initialization Sequence Completed								
2024-04-19 12:13:09.521366+00:00	openvpn	30278	OpenVPN 2.5.2 amd64-portbld-freebsd12.2 [SSL (OpenSSL)] [LZO] [LZ4] [MH/RECVDA] [AEAD] built on Dec 8 2023								
2024-04-19 12:13:09.521032+00:00	openvpn	30278	library versions: OpenSSL 1.1.1k-freebsd 25 Mar 2021, LZO 2.10								
2024-04-19 12:13:09.522132+00:00	openvpn	30359	GDG: problem writing to routing socket								
2024-04-19 12:13:09.522152+00:00	openvpn	30359	NOTE: the current --script-security setting may allow this configuration to call user-defined scripts								
2024-04-19 12:13:09.529068+00:00	openvpn	30359	WARNING: experimental option --capath /var/etc/openvpn/server1/ca								
2024-04-19 12:13:09.529947+00:00	openvpn	30359	TUN/TAP device ovpn1 exists previously, keep at program end								
2024-04-19 12:13:09.530946+00:00	openvpn	30359	TUN/TAP device /dev/tun1 opened								

Status / System Logs / OpenVPN / Log Table Layout

- **Table Column Headers:**
 - **Time:** Displays the time at which the log entry was taken
 - **Process:** Displays the type of log entry
 - **PID:** Displays the unique identifier associated with the log entry
 - **Message:** Provides a brief overview of each log entries contents, see above for specific message contents

Filter/Manage Logs Sections

Overview

For each of the subsections, there are two additional buttons:

- **Filter Logs Section**

Advanced Log Filter			
			500
Time	Process	PID	Quantity
 Message Regular expression reference Precede with exclamation (!) to exclude match.			Apply Filter

Status / System Logs / OpenVPN / Filter Logs Section

This section provides a way for the user to filter through the list of log entries. After completing the filter entries, click the green **Apply Filter** button to show the filtered log. There are five ways that the logs can be filtered:

- **Filter Logs Options:**
 - **Time:** Entering a date and/or time will display any logs with the matching data in the **Time** column
 - **Process:** Entering in a specific process style will display any logs matching that within the **Process** column
 - **PID:** Entering in a PID value will display any logs matching the value within the **PID** column
 - **Quantity:** This allows for the control of how many logs are displayed regarding the number of filtered logs that are being displayed
 - **Message:** Entering a log message will display any logs that match within the **Message** column
- **Manage Logs Section**

Manage OpenVPN Log	
These settings override the "General Logging Options" settings.	
Forward/Reverse Display	☐ Forward (newest at bottom) ☐ Reverse (newest at top) ☒ General Logging Options Setting
Show log entries in forward or reverse order.	
GUI Log Entries	500 This is the number of log entries displayed in the GUI. It does not affect how many entries are contained in the log.
Log Rotation Size (Bytes)	512000 This field controls the size at which logs will be rotated. By default this is per log file. NOTE: Log file sizes are checked once per minute to determine if rotation is necessary, so a very rapidly growing log file may exceed this value.
Log Retention Count	7 The number of log files to keep before the oldest copy is removed on rotation.
Formatted/Raw Display	☐ Formatted ☐ Raw ☒ General Logging Options Setting
Show the log entries as formatted or raw output as generated by the service. The raw output will reveal more detailed information, but it is more difficult to read.	
Action	Save Clear log
Saves changed settings. Clears local log file and reinitializes it as an empty log. Save any settings changes first.	

Status / System Logs / OpenVPN / Manage Logs Section

This section allows for the management of how the logs are displayed. These configuration fields can be:

- **Manage Logs Options:**
 - **Forward/Reverse Display:** Change the order in which the logs are displayed within the table. There are three options:
 - **Forward:** Displays the newest logs at the bottom, old logs at the top
 - **Reverse:** Displays the newest logs at the top, old logs at the bottom
 - **General Logging Options Settings:** Displays the default way in which logs are ordered
 - **GUI Log Entries:** Changes the total number of logs that are displayed within the log entries table
 - **Log Rotation Size (Bytes):** Changes the amount of bytes till a log entry is rotated out. The default value is per log file. This value is checked once per minute to determine if rotation is necessary
 - **Log Retention Count:** Controls the number of log files kept till the oldest copy is removed during rotation
 - **Formatted/Raw Display:** Changes the way the log entries are displayed. There are three options:
 - **Formatted:** Displays a more structured and organized format of the log entries
 - **Raw:** Displays a more detailed log entry but makes the log entries more difficult to read. This selection only displays a **Time** and **Message** column

- **General Logging Options Setting:** Displays the log entries in a default style
- **Action:** There are two buttons in this area:
 -  **Save:** Select this button to save any changes made within the settings section
 -  **Clear Log:** Select this button to clear the local log file and reinitialize it as an empty log. Please ensure all settings are saved before proceeding

 In the table, clicking on the header of the 'Time' column sorts the logs chronologically. The default order is oldest to newest. Meanwhile, the other three columns enable sorting by grouping logs according to their respective names

NTP Logs

Overview

Status / System Logs / NTP

Status / System Logs / NTP

This section has [Top Banner Buttons](#)

This page provides logs gathered from NTP on the Anybus Defender. The **Status / System Logs / NTP** page has one section:

NTP Log Table

Overview

This table displays the logs from NTP. There are four table columns:

Last 500 NTP Log Entries. (Maximum 500)			
Time	Process	PID	Message
2024-04-19 20:03:38.867724+00:00	ntpd	72845	error resolving pool pool.ntp.org: Name does not resolve (8)
2024-04-19 20:04:45.897205+00:00	ntpd	72845	error resolving pool pool.ntp.org: Name does not resolve (8)
2024-04-19 20:05:51.896164+00:00	ntpd	72845	error resolving pool pool.ntp.org: Name does not resolve (8)
2024-04-19 20:06:58.906374+00:00	ntpd	72845	error resolving pool pool.ntp.org: Name does not resolve (8)
2024-04-19 20:08:03.886751+00:00	ntpd	72845	error resolving pool pool.ntp.org: Name does not resolve (8)
2024-04-19 20:09:07.886680+00:00	ntpd	72845	error resolving pool pool.ntp.org: Name does not resolve (8)
2024-04-19 20:10:13.889513+00:00	ntpd	72845	error resolving pool pool.ntp.org: Name does not resolve (8)
2024-04-19 20:11:18.877904+00:00	ntpd	72845	error resolving pool pool.ntp.org: Name does not resolve (8)
2024-04-19 20:12:22.917992+00:00	ntpd	72845	error resolving pool pool.ntp.org: Name does not resolve (8)
2024-04-19 20:13:28.882690+00:00	ntpd	72845	error resolving pool pool.ntp.org: Name does not resolve (8)

Status / System Logs / NTP / Log Table Layout

- **Table Column Headers:**
 - **Time:** Displays the time at which the log entry was taken
 - **Process:** Displays the type of log entry
 - **PID:** Displays the unique identifier associated with the log entry
 - **Message:** Provides a brief overview of each log entries contents, see above for specific message contents

Filter/Manage Logs Sections

Overview

For each of the subsections, there are two additional buttons:

- **Filter Logs Section**

Advanced Log Filter

Time

Process

PID

500

Quantity

Message

Regular expression reference

Precede with exclamation (!) to exclude match.

Apply Filter

Status / System Logs / NTP / Filter Logs Section

This section provides a way for the user to filter through the list of log entries. After completing the filter entries, click the green **Apply Filter** button to show the filtered log. There are five ways that the logs can be filtered:

- **Filter Logs Options:**

- **Time:** Entering a date and/or time will display any logs with the matching data in the **Time** column
- **Process:** Entering in a specific process style will display any logs matching that within the **Process** column
- **PID:** Entering in a PID value will display any logs matching the value within the **PID** column
- **Quantity:** This allows for the control of how many logs are displayed regarding the number of filtered logs that are being displayed
- **Message:** Entering a log message will display any logs that match within the **Message** column

- **Manage Logs Section**

Manage NTP Log

These settings override the "General Logging Options" settings.

Forward/Reverse Display

☐ Forward
(newest at bottom)
 ☐ Reverse
(newest at top)

☒ General Logging Options Setting

Show log entries in forward or reverse order.

GUI Log Entries

500

This is the number of log entries displayed in the GUI. It does not affect how many entries are contained in the log.

Log Rotation Size (Bytes)

512000

This field controls the size at which logs will be rotated. By default this is per log file.

NOTE: Log file sizes are checked once per minute to determine if rotation is necessary, so a very rapidly growing log file may exceed this value.

Log Retention Count

7

The number of log files to keep before the oldest copy is removed on rotation.

Formatted/Raw Display

☐ Formatted
 ☐ Raw

☒ General Logging Options Setting

Show the log entries as formatted or raw output as generated by the service. The raw output will reveal more detailed information, but it is more difficult to read.

Action

Save

Clear log

Saves changed settings.

Clears local log file and reinitializes it as an empty log. Save any settings changes first.

Status / System Logs / NTP / Manage Logs Section

This section allows for the management of how the logs are displayed. These configuration fields can be:

- **Manage Logs Options:**

- **Forward/Reverse Display:** Change the order in which the logs are displayed within the table. There are three options:
 - **Forward:** Displays the newest logs at the bottom, old logs at the top
 - **Reverse:** Displays the newest logs at the top, old logs at the bottom
 - **General Logging Options Settings:** Displays the default way in which logs are ordered
- **GUI Log Entries:** Changes the total number of logs that are displayed within the log entries table
- **Log Rotation Size (Bytes):** Changes the amount of bytes till a log entry is rotated out. The default value is per log file. This value is checked once per minute to determine if rotation is necessary
- **Log Retention Count:** Controls the number of log files kept till the oldest copy is removed during rotation
- **Formatted/Raw Display:** Changes the way the log entries are displayed. There are three options:
 - **Formatted:** Displays a more structured and organized format of the log entries
 - **Raw:** Displays a more detailed log entry but makes the log entries more difficult to read. This selection only displays a **Time** and **Message** column
 - **General Logging Options Setting:** Displays the log entries in a default style
- **Action:** There are two buttons in this area:
 - **Save:** Select this button to save any changes made within the settings section
 - **Clear Log:** Select this button to clear the local log file and reinitialize it as an empty log. Please ensure all settings are saved before proceeding

❗ In the table, clicking on the header of the 'Time' column sorts the logs chronologically. The default order is oldest to newest. Meanwhile, the other three columns enable sorting by grouping logs according to their respective names

Industrial Logs

Overview

This page provides logs from Industrial on the Anybus Defender. The **Status / System Logs / Industrial** page has two sections:

Normal View

Status / System Logs / Industrial Profile / Normal View

Status / System Logs / Industrial

Normal ViewRule Match View

Last 13 Industrial Profile Log Entries. (Maximum 500)

Time	Process	PID	Message
2024-08-20 09:59:55.825944-04:00			Anybus-Defender.localdomain icsdefender 47043 - - Reloading config from file /var/etc/icsdefender.conf.
2024-08-20 10:48:09.591908-04:00			Anybus-Defender.localdomain icsdefender 47043 - - Reloading config from file /var/etc/icsdefender.conf.
2024-08-20 10:49:11.561849-04:00			Anybus-Defender.localdomain icsdefender 47043 - - Reloading config from file /var/etc/icsdefender.conf.
2024-08-21 08:05:39.971678-04:00			Anybus-Defender.localdomain icsdefender 29352 - - Reloading config from file /var/etc/icsdefender.conf.
2024-08-21 08:43:00.241513-04:00			Anybus-Defender.localdomain icsdefender 29352 - - Reloading config from file /var/etc/icsdefender.conf.
2024-08-21 08:43:01.279654-04:00			Anybus-Defender.localdomain icsdefender 29352 - - Reloading config from file /var/etc/icsdefender.conf.
2024-08-21 09:50:22.911321-04:00			Anybus-Defender.localdomain icsdefender 29352 - - Reloading config from file /var/etc/icsdefender.conf.
2024-08-21 09:51:55.663736-04:00			Anybus-Defender.localdomain icsdefender 46513 - - Reloading config from file /var/etc/icsdefender.conf.
2024-10-07 11:14:26.501259-04:00			Anybus-Defender.localdomain icsdefender 45222 - - Reloading config from file /var/etc/icsdefender.conf.
2025-01-20 09:30:50.652607-05:00			Anybus-Defender.localdomain icsdefender 48957 - - Reloading config from file /var/etc/icsdefender.conf.
2025-01-20 09:34:41.238534-05:00			Anybus-Defender.localdomain icsdefender 48957 - - Reloading config from file /var/etc/icsdefender.conf.
2025-01-22 08:51:37.297162-05:00			Anybus-Defender.localdomain icsdefender 44864 - - Reloading config from file /var/etc/icsdefender.conf.
2025-02-15 06:39:19.754192+11:00			Anybus-Defender.localdomain icsdefender 40002 - - Reloading config from file /var/etc/icsdefender.conf.

Status / System Logs / Industrial / Log Table Layout

This section has [Top Banner Buttons](#)

A table displays the log entries from Industrial. There are four table columns:

- **Table Column Headers:**
 - **Time:** Displays the time at which the log entry was taken
 - **Process:** Displays the type of log entry
 - **PID:** Displays the unique identifier associated with the log entry
 - **Message:** Provides a brief overview of each log entries contents, see above for specific message contents

Rule Match View

Status / System Logs / Industrial Profile / Rule Match View

Status / System Logs / Industrial / Rule Match View

Normal ViewRule Match View

Last 0 Industrial Profile Log Entries. (Maximum 500)

Packet#	Action	Protocol	Source: Src. Port	Dest.: Dest. Port	Rule
tcp		ANYBUS-DEFENDER.LOCALDOMAIN	icsdefender	-	

Status / System Logs / Industrial / Log Table Layout

This section presents a table with data collected from any configured industrial profiles on the Anybus Defender regarding any rules that have been triggered or matched. The table has six columns:

- **Table Column Headers:**
 - **Packet#:** Displays the number of packets the rule affected
 - **Action:** Displays the current action status regarding the industrial profiles rule that was flagged. The states that can populate this column are Pass, Block, Warn
 - **Protocol:** The style of the packet that triggered the rule log
 - **Source: Src. Port:** Displays the source port for the IP address attempting to reach through the Anybus Defender
 - **Dest.: Dest. Port:** Displays the destination port for the IP address trying to be reached
 - **Rule:** Displays the rule that was triggered

Filter/Manage Logs Sections

For each of the subsections, there are two additional buttons:

- **Filter Logs Section**

Advanced Log Filter

Time

Process

PID

500

Quantity

Message

Apply Filter

Regular expression reference

Precede with exclamation (!) to exclude match.

Status / System Logs / Industrial / Filter Logs Section

This section provides a way for the user to filter through the list of log entries. After completing the filter entries, click the green **Apply Filter** button to show the filtered log. There are five ways that the logs can be filtered:

- **Filter Logs Options:**
 - **Time:** Entering a date and/or time will display any logs with the matching data in the **Time** column
 - **Process:** Entering in a specific process style will display any logs matching that within the **Process** column
 - **PID:** Entering in a PID value will display any logs matching the value within the **PID** column
 - **Quantity:** This allows for the control of how many logs are displayed regarding the number of filtered logs that are being displayed
 - **Message:** Entering a log message will display any logs that match within the **Message** column
- **Manage Logs Section**

Manage Industrial Profile Log

These settings override the "General Logging Options" settings.

Forward/Reverse Display

Forward

(newest at bottom)

Reverse

(newest at top)

General Logging Options Setting

Show log entries in forward or reverse order.

GUI Log Entries

500

This is the number of log entries displayed in the GUI. It does not affect how many entries are contained in the log.

Log Rotation Size (Bytes)

512000

This field controls the size at which logs will be rotated. By default this is per log file.

NOTE: Log file sizes are checked once per minute to determine if rotation is necessary, so a very rapidly growing log file may exceed this value.

Log Retention Count

7

The number of log files to keep before the oldest copy is removed on rotation.

Formatted/Raw Display

Formatted

Raw

General Logging Options Setting

Show the log entries as formatted or raw output as generated by the service. The raw output will reveal more detailed information, but it is more difficult to read.

Action

Save

Clear log

Saves changed settings.

Clears local log file and reinitializes it as an empty log. Save any settings changes first.

Status / System Logs / Industrial / Manage Logs Section

This section allows for the management of how the logs are displayed. These configuration fields can be:

- **Manage Logs Options:**

- **Forward/Reverse Display:** Change the order in which the logs are displayed within the table. There are three options:
 - **Forward:** Displays the newest logs at the bottom, old logs at the top
 - **Reverse:** Displays the newest logs at the top, old logs at the bottom
 - **General Logging Options Settings:** Displays the default way in which logs are ordered
- **GUI Log Entries:** Changes the total number of logs that are displayed within the log entries table
- **Log Rotation Size (Bytes):** Changes the amount of bytes till a log entry is rotated out. The default value is per log file. This value is checked once per minute to determine if rotation is necessary
- **Log Retention Count:** Controls the number of log files kept till the oldest copy is removed during rotation
- **Formatted/Raw Display:** Changes the way the log entries are displayed. There are three options:
 - **Formatted:** Displays a more structured and organized format of the log entries
 - **Raw:** Displays a more detailed log entry but makes the log entries more difficult to read. This selection only displays a **Time** and **Message** column
 - **General Logging Options Setting:** Displays the log entries in a default style
- **Action:** There are two buttons in this area:
 -  **Save:** Select this button to save any changes made within the settings section
 -  **Clear Log:** Select this button to clear the local log file and reinitialize it as an empty log. Please ensure all settings are saved before proceeding

❗ In the table, clicking on the header of the 'Time' column sorts the logs chronologically. The default order is oldest to newest. Meanwhile, the other three columns enable sorting by grouping logs according to their respective names

System Logs Settings

Overview

This page provides adjustable settings for logging on the Anybus Defender. The **Status / System Logs / Settings** page has three sections:

General Logging Options

General Logging Options

Log Message Format

syslog (RFC 5424, default, with RFC 3339 microsecond-precision timestamps) ▼

The format of syslog messages written to disk locally and sent to remote syslog servers (if enabled). Changing this value will only affect new log messages.

Forward/Reverse Display

☐ Show log entries in reverse order (newest entries on top)

GUI Log Entries

500

This is only the number of log entries displayed in the GUI. It does not affect how many entries are contained in the actual log files.

Log firewall default blocks

☒ Log packets matched from the default block rules in the ruleset
Log packets that are blocked by the implicit default block rule. - Per-rule logging options are still respected.

☒ Log packets matched from the default pass rules put in the ruleset
Log packets that are allowed by the implicit default pass rule. - Per-rule logging options are still respected.

☒ Log packets blocked by 'Block Bogon Networks' rules

☒ Log packets blocked by 'Block Private Networks' rules

Web Server Log

☒ Log errors from the web server process
If this is checked, errors from the web server process for the GUI or Captive Portal will appear in the main system log.

Raw Logs

☐ Show raw filter logs
If this is checked, filter logs are shown as generated by the packet filter, without any formatting. This will reveal more detailed information, but it is more difficult to read.

Where to show rule descriptions

Display as column ▼

Show the applied rule description below or in the firewall log rows. Displaying rule descriptions for all lines in the log might affect performance with large rule sets.

Local Logging

☐ Disable writing log files to the local disk

Reset Log Files

 Reset Log Files

Clears all local log files and reinitializes them as empty logs. This also restarts the DHCP daemon. Use the Save button first if any setting changes have been made.

Status / System Logs / Settings / General Logging Options Section

This section provides a list of settings allowing the configuration of the format for the "General Logging Options Setting" option within the Manage Logs sections and overall logging settings for the log tables. Nine options can be configured:

- **Available Options:**
 - **Log Message Format:** Presented is a dropdown with two log formatting options:
 - **syslog:** Syslog is the universal logging format with more accurate timing. This format also includes a severity value that is logged in addition to the priority value and any information within the log
 - **BSD:** Older format style that displays the priority number but with the difference of not providing any additional severity operator capabilities along with the rest of the logs information
 - **Forward/Reverse Display:** Set the "General Logging Options Setting" option to either use forward or reverse formatting of the data within the log entry tables
 - **GUI Log Entries:** Sets the default amount of entries value that is displayed for all log entry tables
 - **Log Firewall Default Block:** Presented are four check-boxes allowing for the option of either logging or not logging information based on the necessity for what is populating the log entry tables. These options are as follows:

- Log packets matched from the default block rules in the ruleset
- Log packets matched from the default pass rules put in the ruleset
- Log packets blocked by 'Block Bogon Networks' rules
- Log packets blocked by 'Block Private Networks' rules
- **Web Server Logs:** Presents the option to either enable or disable with a check-box whether to log any errors from the web server process within the [System Log table](#)
- **Raw Logs:** Selecting this check-box switches logs to be in a raw format making them more difficult to read but the log entry will display more information. Leaving this box unselected will default the data in the log tables to be displayed in a more organized and structured format. The downside to the formatted display of data is that there is slightly less data that will be displayed versus the Raw format
- **Where To Show Rule Descriptions:** Set the default of how rule descriptions are displayed. The dropdown presents three options:
 - Dont Load Descriptions
 - Displays As Column
 - Display As Second Row
- **Local Logging:** Selecting this option disables the writing of log files to the local disk of the Anybus Defender
-  **Reset Log Files:** Selecting this button clears all local log files and reinitializes them as empty logs

 When using the  **Reset Log Files** button, it will restart the DHCP daemon. Ensure any setting changes are saved before resetting log files

Log Rotation Options

Log Rotation Options	
Log Rotation Size (Bytes)	512000 This field controls the size at which logs will be rotated. By default this is 500 KiB per log file, and there are nearly 20 such log files. NOTE: Increasing this value allows every log file to grow to the specified size, so disk usage may increase significantly. Log file sizes are checked once per minute to determine if rotation is necessary, so a very rapidly growing log file may exceed this value. Disk space currently used by log files is: 886K Remaining disk space for log files: 16G
Log Compression	bzip2 ▼ The type of compression to use when rotating log files. Compressing rotated log files saves disk space, and the compressed logs remain available for display and searching in the GUI. WARNING: Changing this value will remove previously rotated compressed log files!
Log Retention Count	7 The number of log files to keep before the oldest copy is removed on rotation.

Status / System Logs / Settings / Log Rotation Options Section

This section presents options for controlling the log entries rotation default values. There are three options:

- **Available Options:**
 - **Log Rotation Size (Bytes):** Adjust the value of Bytes at which logs will be rotated. The default value is 500KiB (512000 Bytes)
 - **Log Compression:** Presents a dropdown selection of five ways to compress when rotating log files:
 - **bzip2:** Provides efficient compression ratios at the cost of having slower compression speeds
 - **gzip:** Provides a good balance between efficient compression ratios while maintaining faster compression speeds
 - **xz:** Provides better compression ratio than **bzip2** and **gzip**. The downside is that the compression/decompression speeds tend to be slower while also using more memory
 - **zstd:** Provides a balance between compression ratios and compression speeds. The downside is that it uses more memory to accomplish compression speeds/ratios and it may not be supported by as many systems as the other compression types

- **none:** Selecting this option sets no compression type to be used on log files
- **Log Retention Count:** Adjust the value for the number of log files that will be retained till the oldest log is removed during rotation. The default value for this is 7 log files

Remote Logging Options

Remote Logging Options

Enable Remote Logging ☐ Send log messages to remote syslog server

Status / System Logs / Remote Logging Options Section

This section has one check-box option:

- **Available Option:**
 - **Enable Remote Logging:** Selecting this tells the Anybus Defender to send log messages to a remote syslog server. This allows the viewing of log files without having to view them from the **System Logs** page

Save Button

Once the desired changes are made to the **Settings** page, select the  **Save** button located at the bottom of the page

Traffic Graph

Overview

Status / [System Logs](#) / [Settings](#)

Status / Traffic Graph

This page provides a graph displaying traffic on the interfaces being used on the Anybus Defender and settings to configure the traffic graph. There are two sections:

Graph Settings

Graph Settings

Traffic Graph

SDNDATA

Bandwidth Out

All

Description

rate (standard)

Interface

Sort by

Filter

Display

Mode

Controls

Clear graphs when not visible.

On

Background updates

Invert in/out

Graph Smoothing

Save

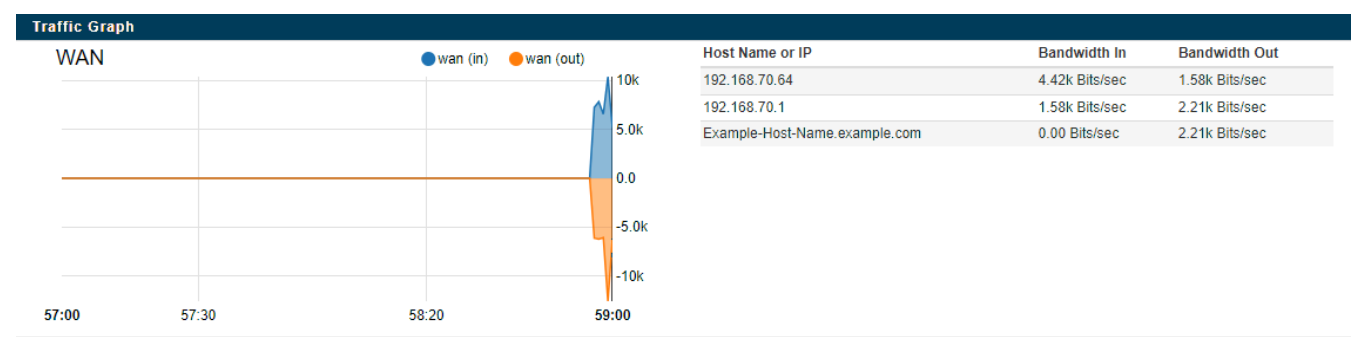
Status / Traffic Graph / Graph Settings Section

This section provides various dropdowns to configure the Traffic Graph. There are two subsections within the settings section:

- **Traffic Graph:** Five dropdowns are presented:
 - **Interface:** Select from the configured interfaces on the Anybus Defender
 - **Sort By:** Provides two options to either sort the graph by **Bandwidth In** or **Bandwidth Out** which
 - **Filter:** Three options are presented:
 - **Local:** Sets the graph to only display Local traffic
 - **Remote:** Sets the graph to only display Remote traffic
 - **All:** Sets the graph to display both Local and Remote traffic
 - **Displays:** Provides four formatting options for the first column of the data table:
 - **IP Address:** Displays the IP address for the connection
 - **Host Name:** Displays the Hostname for the connection. If there is no hostname assigned the IP will display instead
 - **Description:** Displays the description set for the connection
 - **FQDN:** The Fully Qualified Domain Name displays the hostname along with the domain name
 - **Example:** ExampleHostName.example.com
- i** Configuring the information displayed by these options can be adjusted/set in the Host Override section for DNS Resolver/Forwarder
- **Mode:** Provides two options :
 - **Rate:** Focused on getting traffic flow data within a specific time period
 - **Iftop:** Focused on getting traffic rates on active connections within real-time
 - **Controls:** Two dropdowns and a slider are presented:
 - **Background Updates:** Configure the graph to either be unpopulated while not being displayed or have the graph stay populated at all times with the cost of higher CPU usage

- **Invert In/Out:** Turning **On** will have a negative side that indicates the traffic going out and a positive side that indicates the traffic coming in. Turning this **Off** puts both in and out traffic on one side of the X-Axis
- **Graph Smoothing:** Adjusting the slider displays the graph data as less jagged between data points and instead the data points will have smoother transitions

Traffic Graph



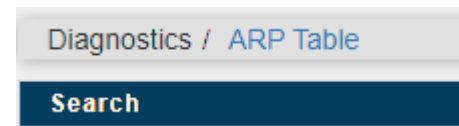
Status / Traffic Graph / Traffic Graph

This section includes two visual references. The first is a graph that shows the traffic on the selected interface, and the second is a table that provides a detailed breakdown of this traffic.

- **Traffic Graph**
 - Displays in blue for traffic that is being taken in by the Anybus Defender
 - Displays in orange for traffic that is being sent out from the Anybus Defender
 - Hovering over a data point on the graph displays four pieces of information
 - The time that the data was captured
 - The date on which the traffic was captured
 - Bits of data that were sent out
 - Bits of data that were taken in
- **Traffic Table**
 - The table displays three columns of data depending on which **Display** setting is selected
 - **HostIP/Name:** Displays the host's IP address. For every other **Display** option other than **IP Address**** this column will also display the hostname if the host has one set in the **Host Overrides** section for the DNS resolver or forwarder
 - **Bandwidth In:** Display in bits/sec the amount of data being sent from the host
 - **Bandwidth Out:** Displays in bits/sec the amount of data being sent out from the Anybus Defender

ARP Table

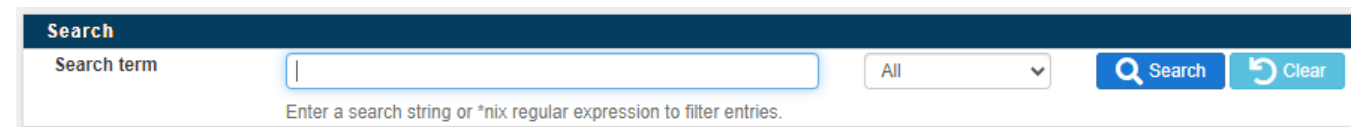
Overview



Diagnostics / ARP Table

This section allows for searching and viewing of mapped IP and MAC addresses. The **Diagnostic / ARP Table** page is divided into two sections:

Search



Search of Diagnostics / ARP Table Page

- **Search Term** Enter a search string or *nix regular expression into the search bar to filter entries
- **Table Filter** A dropdown menu to filter the search by table column
- **Search** button is used to initiate a search based on entered text
- **Clear** button is used to clear all entered text from the search bar

ARP Table

ARP Table						
Interface	IP address	MAC address	Hostname	Status	Link Type	Actions
LAN	192.168.200.1	08:00:27:50:e2:63 (Oracle VirtualBox virtual NIC)		Permanent	ethernet	
LAN	192.168.200.50	0a:00:27:00:00:10		Expires in 568 seconds	ethernet	
WAN	199.99.99.99	08:00:27:e3:06:3d (Oracle VirtualBox virtual NIC)		Permanent	ethernet	

Clear ARP Table

ARP Table of Diagnostics / ARP Table Page

This is a table of IP addresses and their corresponding MAC addresses, which can be used to identify network devices:

- **Interface:** Only the [Interfaces](#) configured in the Anybus Defender
- **IP address:** The internet protocol address is a set of rules governing the format of data sent via the network
- **MAC address:** The media access control address is a 12-digit hexadecimal number assigned to each device connected to the network
- **Hostname:** The name of the connected device
- **Status:** The expiration status
- **Link Type:** The method of connection used by the connected device
- **Actions:** button is used to remove the entry from the table
- **Clear ARP Table** button is used to remove all entries from the table

❗ Local IPv6 peers use NDP instead of ARP. Permanent ARP entries are shown for local interfaces or static ARP entries. Normal dynamic ARP entries show a countdown timer until they will expire and then be re-checked. Incomplete ARP entries indicate that the target host has not yet replied to an ARP request.

Authentication

Overview

Diagnostics / Authentication

Authentication Test

Diagnostics / Authentication

This section has [Top Banner Buttons](#)

This section allows for username and password authentication. The **Diagnostics / Authentication** page only has one section:

Authentication Test

Authentication Test	
Authentication Server	Local Database Select the authentication server to test against.
Username	Username
Password	Password
Test	

Authentication Test of Diagnostics / Authentication Page

- **Authentication Server:** Dropdown to select the server for the authentication test
- **Username:** A unique identifier chosen by the user as a digital identity to access the network
- **Password:** A confidential combination of characters used to authenticate the user's network identity

Below the **Authentication Test** table is the **Test** button to initiate an evaluation process of the user credentials

DNS Lookup

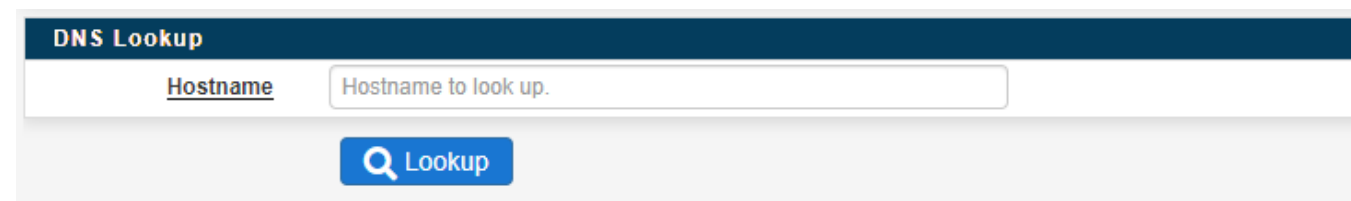
Overview



Diagnostics / DNS Lookup

This section allows hostname searches for identifying specific devices, servers, or resources on the network by their names rather than their IP addresses. The **Diagnostics / DNS Lookup** only has one section:

DNS Lookup



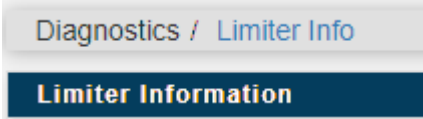
DNS Lookup of Diagnostics / DNS Lookup Page

- **Hostname:** A label assigned to a device connected to a computer network

Below the **DNS Lookup** section is the **Lookup** button to initiate a search based on the entered text in the previous field

Limiter Info

Overview

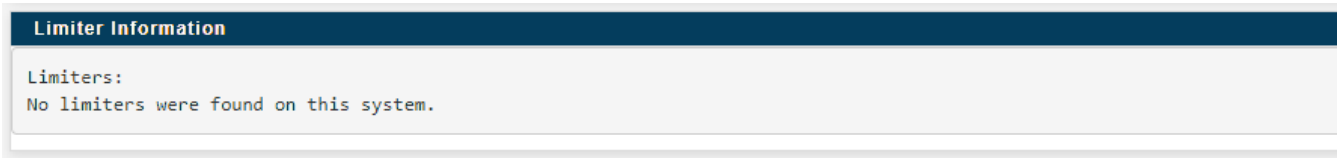


Diagnostics / Limiter Info

This section has [Top Banner Buttons](#)

This section shows any limiters that are in effect on the network. The **Diagnostics / Limiter Info** page only has one section:

Limiter Information



Limiter Information of Diagnostics / Limiter Info Page

NDP Table

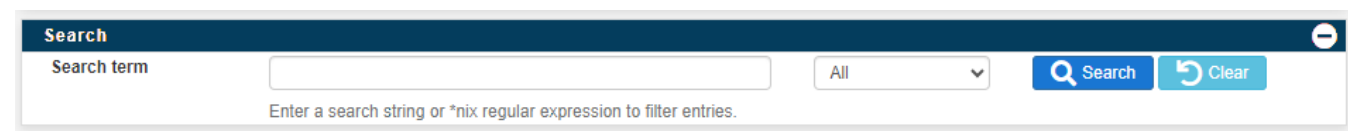
Overview



Diagnostics / NDP Table

This section has options for searching and monitoring the NDP table. The NDP table plays a crucial role in facilitating communication and connectivity in IPv6 networks by managing address resolution, neighbor discovery, router discovery, and neighbor reachability detection processes. The **NDP Table** is divided into two sections:

Search



Search of Diagnostics / NDP Table Page

- **Search Term:** Enter a search string or *nix regular expression into the search bar to filter entries
- **Table Filter:** A dropdown menu to filter the search by table column
- **Search:** button is used to initiate a search based on entered text
- **Clear:** button is used to clear all entered text from the search bar

NDP Table

NDP Table					
IPv6 address	MAC address	Hostname	Interface	Expiration	Actions
fe80::a00:27ff:fe50:e263%em1	08:00:27:50:e2:63 (Oracle VirtualBox virtual NIC)		LAN	permanent	
fe80::a00:27ff:fee3:63d%em0	08:00:27:e3:06:3d (Oracle VirtualBox virtual NIC)		WAN	permanent	

 Clear NDP Table

NDP Table of Diagnostics / NDP Table Page

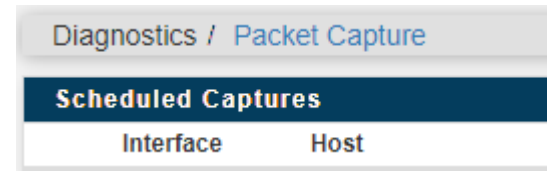
This table in IPv4 networks is a data structure used by IPv6-enabled devices to store information about neighboring devices on the same local network segment

- **IPv6 address:** A 128-bit long, colon-separated, hexadecimal label assigned to devices participating in a computer network
- **MAC address:** A unique identifier assigned to a network interface controller (NIC) for communications at the data link layer of a network segment
- **Hostname:** A label assigned to a device connected to a computer network
- **Interface:** A physical or virtual connection through which a device connects to a network
- **Expiration:** Indicates the validity duration of the IPv6 address
- **Actions:** A button  used to remove the entry from the table

Below the **NDP Table** is the **Clear NDP Table** button to remove all entries from the table

Packet Capture

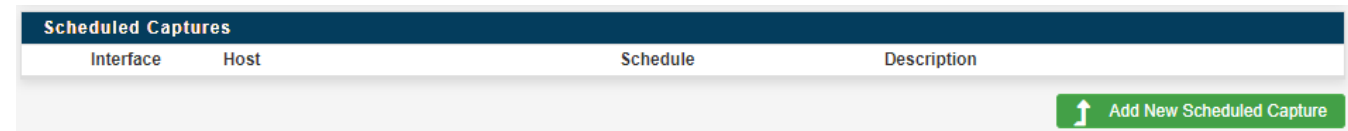
Overview



Diagnostics / Packet Capture

This section has options for scheduled and instant captures. Captures play a crucial role in network management, performance analysis, security monitoring, compliance, troubleshooting, and resource management. The **Packet Capture** page is divided into two sections:

Scheduled Captures

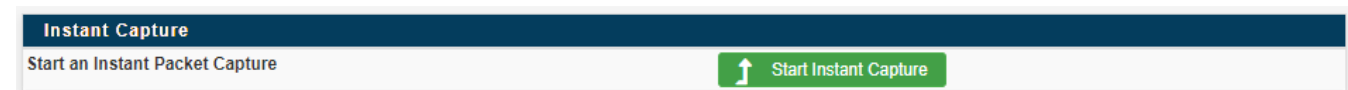


Scheduled Captures of Diagnostics / Schedule Captures Page

- **Interface:** Only the [Interfaces](#) configured in the Anybus Defender
- **Host:** Any device or computer system that is connected to the network that sends or receives data
- **Schedule:** A predetermined plan or strategy for when network packets will be captured
- **Description:** A summary of the information that provides context and details about the captured data

Below the **Scheduled Captures** table is the **Add New Schedule Capture** button to add another capture event to the list

Instant Capture

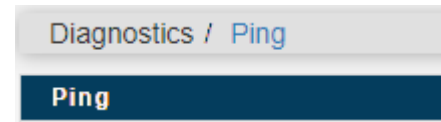


Instant Capture of Diagnostics / Instant Capture

- **Start Instant Capture** button is used to initiate the instant capture process

Ping

Overview



Diagnostics / Ping

This section has options for sending a ping command across the network. The ping command is useful for network troubleshooting, diagnostics, and performance analysis. It provides users with the knowledge and tools they need to effectively test network connectivity, verify network configuration settings, and identify and resolve network issues. The **Ping** page only has one section:

Ping

Ping	
Hostname	Hostname to ping
IP Protocol	IPv4
Source address	Automatically selected (default) Select source address for the ping.
Maximum number of pings	3 Select the maximum number of pings.
Seconds between pings	1 Select the number of seconds to wait between pings.

 Ping

Ping of Diagnostics / Ping Page

- **Hostname:** A label assigned to a device connected to a computer network
- **IP Protocol:** A dropdown for selecting the protocol format
- **Source address:** An address that identifies the sender or originator of a data packet within a network communication
- **Maximum number of pings:** Refers to the greatest number of ICMP Echo Request packets that can be sent by the ping utility in a single ping command
- **Seconds between pings:** Refers to the interval or time duration between consecutive ICMP Echo Request packets sent by the ping utility when testing network connectivity.

Below the **Ping** table is the **Ping** button to send a signal to the selected device on the network

Routes

Overview

Diagnostics / Routes

Routing Table Display Options

Diagnostics / Routes

This section has [Top Banner Buttons](#)

This section has options for monitoring routing tables. The routing tables play a crucial role in packet forwarding, path determination, dynamic routing, network segmentation, load balancing, redundancy, and policy-based routing in computer networks. The **Routes** page is divided into three sections:

Routing Table Display Options

Routing Table Display Options

Resolve names

☐ Enable

Enabling name resolution may cause the query to take longer. It can be stopped at any time by clicking the Stop button in the browser.

Rows to display

100

Filter

Use a regular expression to filter the tables.

Update

Routing Table Display Options of Diagnostics / Routes Page

- Resolve names:** An option in network diagnostic tools, such as the ping utility, that controls whether hostnames are resolved to IP addresses during the testing process
- Rows to display:** A setting that allows users to specify the number of rows or entries to be shown on the IPv4 Routes and IPv6 Routes tables
- Filter:** A regular expression text field that allows users to selectively display a subset of data based on specific criteria or conditions

Below the **Routing Table Display Options** table is the **Update** button that updates the IPv4 and IPv6 tables below with the current settings

IPv4 Routes

IPv4 Routes						
Destination	Gateway	Flags	Use	Mtu	Netif	Expire
127.0.0.1	link#3	UH	3248	16384	lo0	
192.168.200.0/24	link#2	U	2733263	1500	em1	
192.168.200.1	link#2	UHS	0	16384	lo0	
199.99.99.98/31	link#1	U	0	1500	em0	
199.99.99.99	link#1	UHS	0	16384	lo0	

IPv4 Routes of Diagnostics / Routes Page

- Destination:** The intended endpoint or target device to which data is being sent or transmitted

- **Gateway:** A gateway is a network node that serves as an entry point to another network or the internet
- **Flags:** Refer to special bits or fields within network protocol headers that convey specific information about the state or characteristics of a packet
- **Use:** Refers to the utilization or employment of various network resources, protocols, or services to facilitate communication, data exchange, and connectivity between devices or systems
- **Mtu:** Refers to the maximum size of a single data unit (or packet) that can be transmitted over a network medium in a single transmission (typically measured in bytes)
- **Netif:** Stands for "Network Interface" referring to either the physical hardware component (e.g., an Ethernet card) or the software representation of a network interface within the operating system
- **Expire:** Refers to the termination or removal of that route from the network

IPv6 Routes

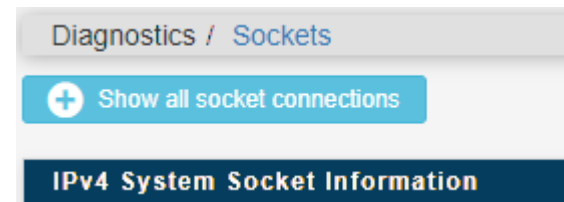
IPv6 Routes						
Destination	Gateway	Flags	Use	Mtu	Netif	Expire
::1	link#3	UH	0	16384	lo0	
fe80::%em0/64	link#1	U	0	1500	em0	
fe80::a00:27ff:fee3:63d%em0	link#1	UHS	0	16384	lo0	
fe80::%em1/64	link#2	U	0	1500	em1	
fe80::a00:27ff:fe50:e263%em1	link#2	UHS	0	16384	lo0	
fe80::%lo0/64	link#3	U	0	16384	lo0	
fe80::1%lo0	link#3	UHS	0	16384	lo0	

IPv6 of Diagnostics / Routes

- **Destination:** The intended endpoint or target device to which data is being sent or transmitted
- **Gateway:** A gateway is a network node that serves as an entry point to another network or the internet
- **Flags:** Refer to special bits or fields within network protocol headers that convey specific information about the state or characteristics of a packet
- **Use:** Refers to the utilization or employment of various network resources, protocols, or services to facilitate communication, data exchange, and connectivity between devices or systems
- **Mtu:** Refers to the maximum size of a single data unit (or packet) that can be transmitted over a network medium in a single transmission (typically measured in bytes)
- **Netif:** Stands for "Network Interface" referring to either the physical hardware component (e.g., an Ethernet card) or the software representation of a network interface within the operating system
- **Expire:** Refers to the termination or removal of that route from the network

Sockets

Overview



Diagnostics / Sockets

This section has options for displaying IPv4 and IPv6 System Socket tables. Sockets play a vital role in enabling communication between processes and applications in computer networks, allowing them to interact, exchange data, and provide services over local and wide-area networks. The **Sockets** page is divided into two sections:

IPv4 System Socket Information

IPv4 System Socket Information						
USER	COMMAND	PID	FD	PROTO	LOCAL	FOREIGN
root	php-cgi	21793	4	udp4	*:*	*:*
root	syslogd	83369	8	udp4	*:514	*:*
root	ntpd	41154	21	udp4	*:123	*:*
root	ntpd	41154	23	udp4	199.99.99.99:123	*:*
root	ntpd	41154	25	udp4	192.168.200.1:123	*:*
root	ntpd	41154	28	udp4	127.0.0.1:123	*:*
root	nginx	40113	5	tcp4	*:443	*:*
root	nginx	40113	7	tcp4	*:80	*:*
root	nginx	39990	5	tcp4	*:443	*:*
root	nginx	39990	7	tcp4	*:80	*:*
root	nginx	39959	5	tcp4	*:443	*:*
root	nginx	39959	7	tcp4	*:80	*:*
unbound	unbound	35673	3	udp4	*:53	*:*
unbound	unbound	35673	4	tcp4	*:53	*:*
unbound	unbound	35673	5	tcp4	127.0.0.1:953	*:*
root	php-fpm	344	4	udp4	*:*	*:*
root	php-fpm	343	4	udp4	*:*	*:*
root	php-fpm	342	4	udp4	*:*	*:*
root	php-fpm	341	4	udp4	*:*	*:*

IPv4 System Socket Information of Diagnostics / Sockets Page

- **User:** Refers to how IP addresses are classified and managed within the network infrastructure
- **Command:** Refers to a specific action or instruction that is issued to configure, manage, or troubleshoot network settings related to IPv4 addressing, routing, or connectivity
- **PID** Refers to Process ID which is a unique numerical identifier assigned to each running process in an operating system
- **FD** Refers to File Descriptor which is an abstract indicator or handle used by a process to access a file or a data stream
- **PROTO** Refers to Protocol Field which is the IPv4 header indicating which higher-level protocol is encapsulated within the IPv4 packet
- **LOCAL** Refers to an IPv4 address that is assigned to a device within a local network or subnet
- **FOREIGN** Refers to an IPv4 address or network that is external to the local network or domain

IPv6 System Socket Information

IPv6 System Socket Information						
USER	COMMAND	PID	FD	PROTO	LOCAL	FOREIGN
root	php-cgi	21793	5	udp6	::*	::*
root	syslogd	83369	7	udp6	:::514	::*
root	ntpd	41154	20	udp6	:::123	::*
root	ntpd	41154	22	udp6	fe80::a00:27ff:fee3:63d%em0:123	::*
root	ntpd	41154	24	udp6	fe80::a00:27ff:fe50:e263%em1:123	::*
root	ntpd	41154	26	udp6	:::1:123	::*
root	ntpd	41154	27	udp6	fe80::1%lo0:123	::*
root	nginx	40113	6	tcp6	:::443	::*
root	nginx	40113	8	tcp6	:::80	::*
root	nginx	39990	6	tcp6	:::443	::*
root	nginx	39990	8	tcp6	:::80	::*
root	nginx	39959	6	tcp6	:::443	::*
root	nginx	39959	8	tcp6	:::80	::*
root	php-fpm	344	5	udp6	::*	::*
root	php-fpm	343	5	udp6	::*	::*
root	php-fpm	342	5	udp6	::*	::*
root	php-fpm	341	5	udp6	::*	::*

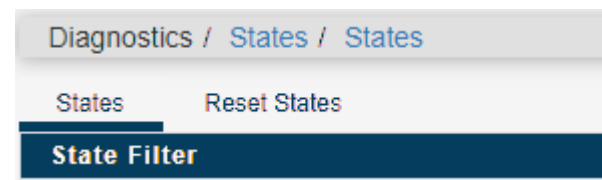
IPv6 System Socket Information of Diagnostics / Sockets Page

- **User:** Refers to how IP addresses are classified and managed within the network infrastructure
- **Command:** Refers to a specific action or instruction that is issued to configure, manage, or troubleshoot network settings related to IPv6 addressing, routing, or connectivity
- **PID:** Refers to Process ID which is a unique numerical identifier assigned to each running process in an operating system
- **FD:** Refers to File Descriptor which is an abstract indicator or handle used by a process to access a file or a data stream
- **PROTO:** Refers to Protocol Field which is the IPv6 header indicating which higher-level protocol is encapsulated within the IPv6 packet
- **LOCAL:** Refers to an IPv6 address that is assigned to a device within a local network or subnet
- **FOREIGN:** Refers to an IPv6 address or network that is external to the local network or domain

🔍 **Socket Information** This page shows all listening sockets by default and shows both listening and outbound connection sockets when **Show all socket connections** is clicked

States

Overview



Search Section of States / States

This page has settings related to the diagnostic states for the Anybus Defender. The **Diagnostics / States / States** page is divided into two sections:

State Filter

A screenshot of the 'State Filter' form. It has a header bar with 'States' and 'Reset States' tabs, with 'States' being the active tab. Below the header is a dark blue bar with 'State Filter' and a minus icon. The form contains two main sections: 'Interface' with a dropdown menu currently showing 'all', and 'Filter expression' with a text input field containing the placeholder text 'Simple filter such as 192.168, v6, icmp or ESTABLISHED'. At the bottom of the form is a blue button with a funnel icon and the text 'Filter'.

State Filter of Diagnostics / States / States Page

- **Interface:** Refers to a network interface through which traffic passes and is subject to filtering based on its state
- **Filter Expression:** Refers to a set of criteria or conditions used to define which network traffic should be allowed or denied based on its characteristics

Below the **State Filter** table is the **Filter** button to display data based on criteria entered in the filter expression text field

States

States					
Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
all	tcp	192.168.200.50:50843 -> 192.168.200.1:443	ESTABLISHED:ESTABLISHED	997 / 1.165 K	104 KiB / 439 KiB
all	udp	127.0.0.1:56933 -> 127.0.0.1:53	MULTIPLE:SINGLE	1 / 1	58 B / 58 B
all	udp	127.0.0.1:1764 -> 127.0.0.1:53	SINGLE:MULTIPLE	1 / 1	58 B / 58 B
all	udp	127.0.0.1:16259 -> 127.0.0.1:53	MULTIPLE:SINGLE	1 / 1	58 B / 58 B
all	udp	127.0.0.1:5516 -> 127.0.0.1:53	SINGLE:MULTIPLE	1 / 1	58 B / 58 B
all	udp	127.0.0.1:52205 -> 127.0.0.1:53	MULTIPLE:SINGLE	1 / 1	70 B / 70 B
all	udp	127.0.0.1:29883 -> 127.0.0.1:53	SINGLE:MULTIPLE	1 / 1	70 B / 70 B
all	udp	127.0.0.1:56217 -> 127.0.0.1:53	MULTIPLE:SINGLE	1 / 1	70 B / 70 B
all	udp	127.0.0.1:24110 -> 127.0.0.1:53	SINGLE:MULTIPLE	1 / 1	70 B / 70 B
all	udp	192.168.200.50:57621 -> 192.168.200.255:57621	NO_TRAFFIC:SINGLE	2 / 0	144 B / 0 B
all	udp	127.0.0.1:56933 -> 127.0.0.1:53	SINGLE:MULTIPLE	1 / 1	58 B / 58 B
all	udp	127.0.0.1:1764 -> 127.0.0.1:53	MULTIPLE:SINGLE	1 / 1	58 B / 58 B
all	udp	127.0.0.1:16259 -> 127.0.0.1:53	SINGLE:MULTIPLE	1 / 1	58 B / 58 B
all	udp	127.0.0.1:5516 -> 127.0.0.1:53	MULTIPLE:SINGLE	1 / 1	58 B / 58 B
all	udp	127.0.0.1:52205 -> 127.0.0.1:53	SINGLE:MULTIPLE	1 / 1	70 B / 70 B
all	udp	127.0.0.1:29883 -> 127.0.0.1:53	MULTIPLE:SINGLE	1 / 1	70 B / 70 B
all	udp	127.0.0.1:56217 -> 127.0.0.1:53	SINGLE:MULTIPLE	1 / 1	70 B / 70 B
all	udp	127.0.0.1:24110 -> 127.0.0.1:53	MULTIPLE:SINGLE	1 / 1	70 B / 70 B

State Table of Diagnostics / States / States Page

- **Interface:** Refers to a network interface through which traffic passes and is subject to stateful inspection or processing
- **Protocol:** Refers to a set of rules or conventions governing the communication and interaction between different states within a system
- **Source (Original Source)-> Destination (Original Destination):** Refers to the journey of a network packet from its source to its destination, preserving information about both the original source and destination throughout its transmission
- **State:** Refers to the various stages or conditions that network connections or sessions can exist in
- **Packets:** A fundamental unit of data that is transmitted over a network. It contains both the data being transmitted and control information used for routing and managing the transmission process.
- **Bytes:** A byte refers to a unit of data transmission and storage. It consists of a sequence of 8 bits, each of which can represent a binary value of either 0 or 1.
- **Remove:** button  is used to remove entries from the table

Reset States

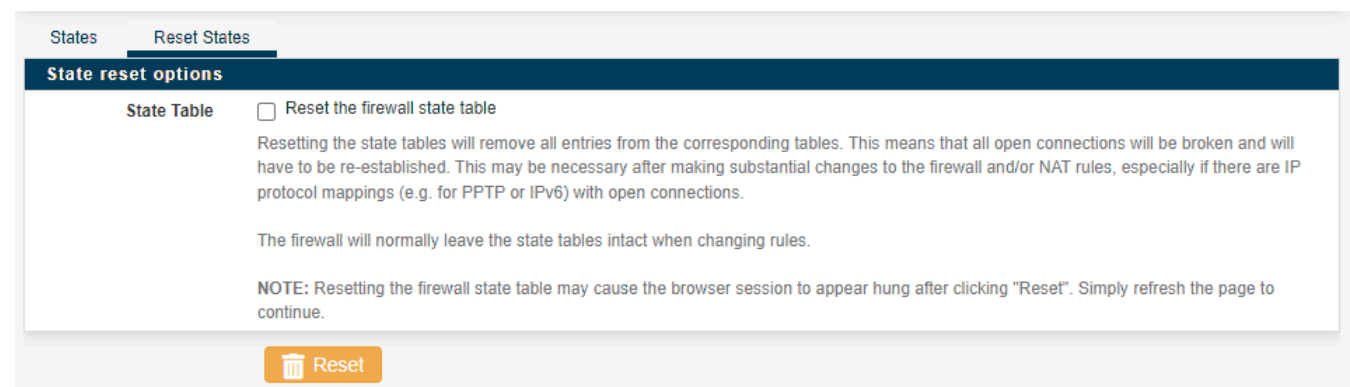
Overview



Search Section of States / State / Reset States Page

This page has settings related to the diagnostic reset states for the Anybus Defender. The **Diagnostics / States / Reset States** page only has one section:

State Reset Options



State Reset Options of Diagnostics / States / State Reset Page

- **State Table:** A data structure maintained by networking devices such as routers, firewalls, or network address translation (NAT) devices to keep track of the state of network connections

Below the **State reset options** section is the **Reset** button to remove all entries from the corresponding tables. Open connections will be broken momentarily as the state table is rebuilt

State Summary

Overview

Status / Dashboard

System Information

Diagnostics / State Summary

This section has preset summary tables based on set criteria. The **Diagnostics / State Summary** page is divided into four sections:

By Source IP

By Source IP					
			Protocol counts		
IP	# States	Protocol	# States	Source Ports	Dest. Ports
192.168.200.50	2	tcp	1		1
		udp	1		1

By Source IP of Diagnostics / State Summary Page

- **IP:** An Internet Protocol address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.
- **# States:** The total count of active states or connections being tracked by the networking device for this IP address
- **Protocol:** Protocol refers to the communication rules and conventions for data exchange between devices or systems on a network. Each protocol specifies how data is formatted, transmitted, and received, as well as how devices identify and communicate with each other.
- **# States:** The total count of active states or connections being tracked by the network device per the protocol type
- **Source Ports:** The source ports refer to the port numbers used by the sending or transmitting device in a network communication session. Ports are endpoints for communication in networking protocols, allowing multiple applications or services to use the same network interface on a device simultaneously.
- **Dest. Ports:** The destination ports refer to the port numbers used by the receiving or destination devices in network communication.

By Destination IP

By Destination IP					
			Protocol counts		
IP	# States	Protocol	# States	Source Ports	Dest. Ports
192.168.200.1	1	tcp	1		1
192.168.200.255	1	udp	1		1

By Destination IP of Diagnostics / State Summary Page

- **IP:** An Internet Protocol address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

- **# States:** The total count of active states or connections being tracked by the networking device per the destination IP address
- **Protocol:** Protocol refers to the communication rules and conventions for data exchange between devices or systems on a network. Each protocol specifies how data is formatted, transmitted, and received, as well as how devices identify and communicate with each other.
- **# States:** The total count of active states or connections being tracked by the network device per the protocol type
- **Source Ports:** The source ports refer to the port numbers used by the sending or transmitting device in a network communication session.
- **Dest. Ports:** The destination ports refer to the port numbers used by the receiving or destination devices in network communication.

Total per IP

Total per IP					
IP	# States	Protocol	Protocol counts		
			# States	Source Ports	Dest. Ports
192.168.200.1	1	tcp	1		1
192.168.200.50	2	tcp	1		1
		udp	1		1
192.168.200.255	1	udp	1		1

Total per IP of Diagnostics / State Summary Page

- **IP:** An Internet Protocol address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.
- **# States:** The total count of active states or connections being tracked by the networking device per the IP address
- **Protocol:** Protocol refers to the communication rules and conventions for data exchange between devices or systems on a network. Each protocol specifies how data is formatted, transmitted, and received, as well as how devices identify and communicate with each other.
- **# States:** The total count of active states or connections being tracked by the network device per the protocol type
- **Source Ports:** The source ports refer to the port numbers used by the sending or transmitting device in a network communication session.
- **Dest. Ports:** The destination ports refer to the port numbers used by the receiving or destination devices in network communication.

By IP Pair

By IP Pair					
IP	# States	Protocol	Protocol counts		
			# States	Source Ports	Dest. Ports
192.168.200.50 -> 192.168.200.1	1	tcp	1		1
192.168.200.50 -> 192.168.200.255	1	udp	1		1

By IP Pair of Diagnostics / State Summary Page

- **IP:** An Internet Protocol address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.
- **# States:** The total count of active states or connections being tracked by the networking device per the pair of IP address

- **Protocol:** Protocol refers to the communication rules and conventions for data exchange between devices or systems on a network. Each protocol specifies how data is formatted, transmitted, and received, as well as how devices identify and communicate with each other.
- **# States:** The total count of active states or connections being tracked by the network device per the protocol type
- **Source Ports:** The source ports refer to the port numbers used by the sending or transmitting device in a network communication session.
- **Dest. Ports:** The destination ports refer to the port numbers used by the receiving or destination devices in network communication.

Support Package Download

Overview

Diagnostics / Download Support Package

Support package has started gathering and downloading support items. The process usually completes in 20-30 seconds.

Encryption

Diagnostics / Download Support Package

This page allows for a support package to be compiled and downloaded as a zip file. This can then be sent to HMS's support at info@hms-networks.com

⚠ This support package download will include sensitive data and should only be shared with the HMS support team. Adding a password via encryption can also be done to add more security (see below)

Some of the important information that will be included in the download are:

- [System Configuration](#)
- Installed [Packages](#) with health and version information
- [Services](#) used and their configuration
- [System Logs](#)
- [Licensing](#) issues
- [User](#) data
- [VPN Configuration](#)
- Service outages and connectivity problems

Encryption

Encryption

Encryption

☒ Encrypt this configuration file.

Passwords or Private Keys were detected in configuration; it is highly recommended this file be encrypted.

Password

Confirm

Encryption Section

- **Encryption:** Option to password protect the support package download

Download

Download

Download

 Download

Download support package.

Download Section

-  **Download:** Button to download the support package

 Allow 20-30 seconds for the support package to gather all required information

System Activity

Overview

Diagnostics / System Activity

CPU Activity

Diagnostics / System Activity

This section allows observing and analyzing the usage of the Central Processing Unit (CPU) in a computer system. This monitoring typically involves tracking various metrics related to CPU performance. The **Diagnostics / System Activity** page only has one section.

CPU Activity

CPU Activity										
last pid: 45699; load averages: 0.44, 0.42, 0.23 up 0+00:07:31 10:35:37										
126 threads: 3 running, 106 sleeping, 17 waiting										
CPU: 8.9% user, 0.1% nice, 6.9% system, 0.5% interrupt, 83.7% idle										
Mem: 53M Active, 19M Inact, 101M Wired, 52M Buf, 263M Free										
PID	USERNAME	PRI	NICE	SIZE	RES	STATE	C	TIME	WCPU	COMMAND
11	root	155	ki31	0B	32K	CPU1	1	6:20	96.00%	[idle{idle: cpu1}]
11	root	155	ki31	0B	32K	RUN	0	6:17	92.97%	[idle{idle: cpu0}]
0	root	-16	-	0B	448K	swpin	0	0:18	0.00%	[kernel{swapper}]
0	root	-76	-	0B	448K	-	1	0:17	0.00%	[kernel{if_io_tqg_1}]
12	root	-60	-	0B	272K	WAIT	1	0:03	0.00%	[intr{swi4: clock (0)}]
5	root	-16	-	0B	32K	-	0	0:02	0.00%	[cam{scanner}]
0	root	-76	-	0B	448K	-	0	0:02	0.00%	[kernel{if_io_tqg_0}]
342	root	52	0	190M	39M	accept	1	0:02	0.00%	php-fpm: pool nginx (php-fpm)
0	root	-76	-	0B	448K	-	1	0:01	0.00%	[kernel{if_config_tqg_0}]
19	root	-16	-	0B	16K	-	1	0:01	0.00%	[rand_harvestq]
344	root	52	0	190M	39M	accept	1	0:01	0.00%	php-fpm: pool nginx (php-fpm)
343	root	21	0	190M	38M	piperd	1	0:01	0.00%	php-fpm: pool nginx (php-fpm)
33818	unbound	20	0	39M	17M	kqread	1	0:01	0.00%	/usr/local/sbin/unbound -c /var/unbound/unbound.conf{unbound}
39694	root	20	0	18M	6284K	select	0	0:01	0.00%	/usr/local/sbin/ntpd -g -c /var/etc/ntpd.conf -p /var/run/ntpd.pid{ntpd}
33818	unbound	20	0	39M	17M	kqread	0	0:00	0.00%	/usr/local/sbin/unbound -c /var/unbound/unbound.conf{unbound}
38259	root	20	0	29M	9084K	kqread	0	0:00	0.00%	nginx: worker process (nginx)
12	root	-72	-	0B	272K	WAIT	1	0:00	0.00%	[intr{swi1: netisr 1}]
5	root	-16	-	0B	32K	-	0	0:00	0.00%	[cam{doneq0}]
18	root	-16	-	0B	16K	pftm	1	0:00	0.00%	[pf purge]
12	root	-88	-	0B	272K	WAIT	1	0:00	0.00%	[intr{irq20: mpt0}]
20	root	-16	-	0B	48K	psleep	0	0:00	0.00%	[pagedaemon{dom0}]
96608	root	52	0	11M	2156K	nanslp	1	0:00	0.00%	daemon: /usr/local/pkg/rc.identifyassets[43737] (daemon)
7934	root	20	0	15M	3072K	select	1	0:00	0.00%	/usr/local/sbin/pcscd{pcscd}
22	root	-16	-	0B	48K	qsleep	1	0:00	0.00%	[bufdaemon{bufdaemon}]
24	root	16	-	0B	16K	syncer	0	0:00	0.00%	[syncer]
12	root	-84	-	0B	272K	WAIT	0	0:00	0.00%	[intr{irq1: atkbd0}]
341	root	20	0	189M	30M	kqread	1	0:00	0.00%	php-fpm: master process (/usr/local/lib/php-fpm.conf) (php-fpm)
58867	root	52	20	11M	2584K	wait	0	0:00	0.00%	/bin/sh /var/db/rrd/updaterrd.sh

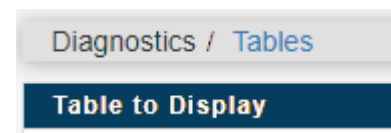
CPU Activity of Diagnostics / System Activity Page

- **PID:** Stands for Process Identifier which is a unique numerical identifier assigned to each process running on the network
- **USERNAME:** Refers to the identifier associated with a user account that is interacting with the network or the system
- **PRI:** This value indicates the priority assigned to a process by the operating system kernel. It reflects how important the process is in terms of resource allocation and execution
- **NICE:** This value indicates how much CPU time is currently allocated to processes with different priorities
- **SIZE:** This value refers to the memory size or memory footprint of a process. This could indicate how much memory (RAM) a particular process is consuming while running on the CPU
- **RES:** Stands for Resident Set Size representing the portion of a process's memory (RAM) that is currently resident in physical memory

- **STATE:** Refers to the different activity conditions that a process can be in during its execution. These states represent various stages of the process lifecycle as it interacts with the operating system and the CPU
- **C:** Refers to CPU utilization
- **TIME:** Refers to the duration or amount of time the CPU spends executing tasks or processing instructions
- **WCPU:** Refers to weighted CPU, which is a metric used to assess CPU usage, especially in multi-core or multi-threaded systems, where each core or thread may not contribute equally to the overall workload
- **COMMAND:** Refers to the specific instructions or tasks that the CPU is executing at any given time

Tables

Overview



Diagnostics / Tables

This section has [Top Banner Buttons](#)

This section allows the viewing of user-defined alias name tables or system name tables. The **Diagnostics / Tables** page is divided into two sections:

Table of Display

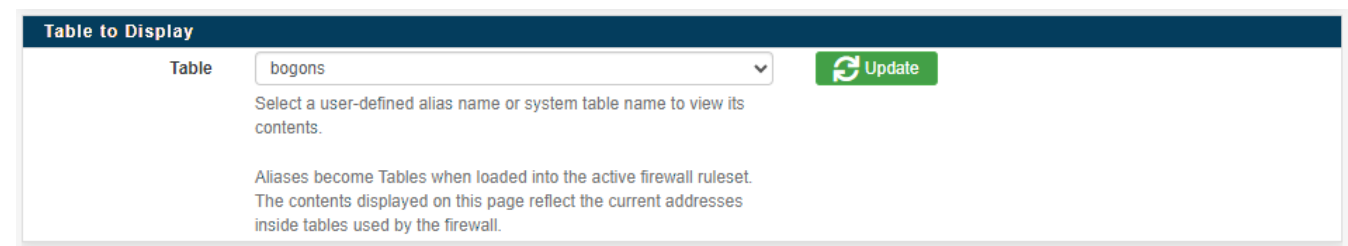


Table to Display of Diagnostics / Tables Page

- **Table:** A dropdown used to choose the user-defined alias name or system table name.
- **Update:** button is used to generate the contents of a table based on the selected user-defined alias name or system table name.

🚫 Date of last update of table



Date of last update of table is unknown. 10 records.

Bogons Table

IP Address

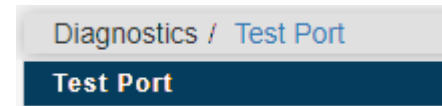
0.0.0.0/8
127.0.0.0/8
169.254.0.0/16
192.0.0.0/24
192.0.2.0/24
198.18.0.0/15
198.51.100.0/24
203.0.113.0/24
224.0.0.0/4
240.0.0.0/4

Bogons Table of Diagnostics / Tables Page

- **IP Address:** An Internet Protocol address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

Test Port

Overview



Diagnostics / Test Port

This section allows users to perform diagnostic tests on specific network ports. This page provides tools and utilities for analyzing the status, connectivity, and performance of individual ports on the device. The **Diagnostics / Test Port** page only has one section.

Test Port

Hostname

Hostname to look up.

Port

Port to test.

Source Port

Typically left blank.

Remote text

☐ Show remote text

Shows the text given by the server when connecting to the port. If checked it will take 10+ seconds to display in a panel below this form.

Source Address

Any

Select source address for the trace.

IP Protocol

IPv4

If IPv4 or IPv6 is forced and a hostname is used that does not contain a result using that protocol, it will result in an error. For example if IPv4 is forced and a hostname is used that only returns an AAAA IPv6 IP address, it will not work.

Test

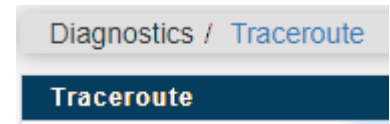
Test Port of Diagnostics / Test Port Page

- **Hostname:** A label assigned to a device connected to a computer network
- **Port:** A port refers to a logical construct used to identify specific applications or services running on a device within a network
- **Source Port:** A source port is a numerical identifier associated with the sending end of a network communication session
- **Remote Text:** Refers to the response or output received from the remote server or device when conducting a port test.
- **Source Address:** Refers to the unique identifier assigned to the device or host that initiates a communication session or sends data packets over a network. The source address identifies the origin or sender of the data packets.
- **IP Protocol:** A set of rules governing the format of data packets sent over the Internet or any network that uses the Internet Protocol suite

Below the **Test Port** section is the **Test** button to initiate the test per previous selections

Traceroutes

Overview



Diagnostics / Traceroute

This section has adjustable settings to perform traceroute operations for troubleshoot network connectivity issues, analyzing the path that packets take between a source and destination, and identifying potential points of failure or congestion in the network. The **Diagnostics / Traceroute** page only has one section.

Traceroute	
Hostname	Hostname to trace.
IP Protocol	IPv4 Select the protocol to use.
Source Address	Any Select source address for the trace.
Maximum number of hops	18 Select the maximum number of network hops to trace.
Reverse Address Lookup	☐ When checked, traceroute will attempt to perform a PTR lookup to locate hostnames for hops along the path. This will slow down the process as it has to wait for DNS replies.
Use ICMP	☐ By default, traceroute uses UDP but that may be blocked by some routers. Check this box to use ICMP instead, which may succeed.
 Traceroute	

Traceroute of Diagnostics / Traceroute Page

- **Hostname:** A label assigned to a device connected to a computer network
- **IP Protocol** The IP protocol is a fundamental communication protocol used for sending and receiving data packets across networks.
- **Source Address** The source address is a unique identifier assigned to the sending device or host in a communication session.
- **Maximum Number of Hops:** This value refers to the maximum number of intermediate devices, typically routers, that data packets can traverse as they travel from a source device to a destination device. Each hop represents a single network device that forwards packets along the path toward the destination.
- **Reverse Address Lookup:** This is a process used to determine the domain name or hostname associated with a given IP address.
- **Use ICMP:** Internet Control Message Protocol is a supporting protocol used by network devices, such as routers and hosts, to send error messages and operational information indicating network conditions or issues.

Below the **Traceroute** section is the **Traceroute** button to initiate the path tracking that the data packets take from source to destination device over the network based on the chosen criteria

Procedures Overview

Overview

This section will explain procedures for adding or editing elements in the Anybus Defender

Add A New Gateway

Overview

System / Routing / Gateways / Edit

↺

⏏

⌵

📊

☰

Edit Gateway

System / Routing / Gateways / Edit Page

This procedure will explain how to add a new Gateway to the Anybus Defender

Procedure

1. Navigate to [System/Routing/Gateways](#)
2. From the **Gateways** tab, click the **Add** button on the lower right of the **Gateways** table
3. An **Edit Gateway** page will load:

Edit Gateway

Disabled

☐ Disable this gateway

Set this option to disable this gateway without removing it from the list.

Interface

WAN

Choose which interface this gateway applies to.

Address Family

IPv4

Choose the Internet Protocol this gateway uses.

Name

Gateway name

Gateway

Gateway IP address

Gateway Monitoring

☐ Disable Gateway Monitoring

This will consider this gateway as always being up.

Gateway Action

☐ Disable Gateway Monitoring Action

No action will be taken on gateway events. The gateway is always considered up.

Monitor IP

Enter an alternative address here to be used to monitor the link. This is used for the quality RRD graphs as well as the load balancer entries. Use this if the gateway does not respond to ICMP echo requests (pings).

Force state

☐ Mark Gateway as Down

This will force this gateway to be considered down.

Description

A description may be entered here for reference (not parsed).

⚙️ Display Advanced

💾 Save

Edit Gateway of the System / Routing / Gateways Page

4. From the **Edit Gateway** configuration, adjust these options:

- **Disabled:** Does not send traffic to this gateway
- **Interface:** A dropdown box of all the enabled physical and virtual [Interfaces](#) on the system. Select the interface on which this gateway can be reached
- **Address Family:** A dropdown box to set IPv4 or IPv6 used for this gateway
- **Name:** A text entry for the gateway name

❗ The **Name** is for easy identification later and has no effect on the functionality

- **Gateway:** A text entry for the gateway IP address
- **Gateway Monitoring:** Disables gateway monitoring. If checked, it will disable gateway monitoring and will consider the gateway always up

❗ The **Gateway Monitor** is shown on the [Dashboard Gateway Widget](#)

- **Gateway Action:** Disables gateway action. If checked, it will still monitor the gateway, but disables any gateway actions based on the gateway status

❗ The **Gateway Action** is shown on the [Dashboard Gateway Widget](#)

- **Monitor IP:** An alternate address to monitor when checking gateway functionality. This is used for the quality RRD graphs as well as the load balancer entries

❗ **Monitor IP** is used for the quality RRD graphs as well as the load balancer entries

- **Force State:** Forces the gateway to be considered down
- **Description:** Optional description for this gateway
- **Display Advanced:** A button to display or hide the **Advanced Table**

5. From the **Advanced** section, these options can also be adjusted:

Advanced	
Weight	1 Weight for this gateway when used in a Gateway Group.
Data Payload	1 Define data payload to send on ICMP packets to gateway monitor IP.
Latency thresholds	200 500 Low and high thresholds for latency in milliseconds. Default is 200/500.
Packet Loss thresholds	10 20 Low and high thresholds for packet loss in %. Default is 10/20.
Probe Interval	500 How often an ICMP probe will be sent in milliseconds. Default is 500.
Loss Interval	2000 Time interval in milliseconds before packets are treated as lost. Default is 2000.
Time Period	60000 Time period in milliseconds over which results are averaged. Default is 60000.
Alert interval	1000 Time interval in milliseconds between checking for an alert condition. Default is 1000.
Additional information	The time period, probe interval and loss interval are closely related. The ratio between these values control the accuracy of the numbers reported and the timeliness of alerts. A longer time period will provide smoother results for round trip time and loss, but will increase the time before a latency or loss alert is triggered. A shorter probe interval will decrease the time required before a latency or loss alert is triggered, but will use more network resource. Longer probe intervals will degrade the accuracy of the quality graphs. The ratio of the probe interval to the time period (minus the loss interval) also controls the resolution of loss reporting. To determine the resolution, the following formula can be used: $100 * \text{probe interval} / (\text{time period} - \text{loss interval})$ Rounding up to the nearest whole number will yield the resolution of loss reporting in percent. The default values provide a resolution of 1%. The default settings are recommended for most use cases. However if changing the settings, please observe the following restrictions: - The time period must be greater than twice the probe interval plus the loss interval. This guarantees there is at least one completed probe at all times. - The alert interval must be greater than or equal to the probe interval. There is no point checking for alerts more often than probes are done. - The loss interval must be greater than or equal to the high latency threshold.
Use non-local gateway	☐ Use non-local gateway through interface specific route. This will allow use of a gateway outside of this interface's subnet. This is usually indicative of a configuration error, but is required for some scenarios.

 Save

Advanced of the System / Routing / Gateways Page

- **Weight:** A dropdown field to set the priority of a particular gateway
- **Data Payload:** The actual data being transmitted in a network packet or frame
- **Latency Thresholds:** A predefined limit on the amount of acceptable delay in a network or system before performance is considered unacceptably degraded. The Low and high thresholds for latency in milliseconds and the default is 200/500
- **Packet Loss Thresholds:** The maximum allowable percentage of packets that can be lost during transmission over a network before performance is considered degraded or unacceptable. The low and high thresholds for packet loss are in % and the default value is 10/20
- **Probe Interval:** How often the Anybus Defender will probe the gateway to check its status. It has no effect on other devices on the network. Probes will be sent in milliseconds and the default is 500
- **Loss Interval:** A specific period during which packet loss is measured or observed. The time interval is in milliseconds before packets are treated as lost and the default is 2000
- **Time Period:** A specific duration of time for gateway monitoring. The time period is in milliseconds over which results are averaged and the default is 60000
- **Alert Interval:** The specific periods between consecutive alerts generated by gateway monitoring. The time interval is in milliseconds between checking for an alert condition. The Default is 1000
- **Additional Information:** See section below
- **Use Non-Local Gateway:** Allows routing traffic through gateways that are not on the same local network segment or subnet as the Anybus Defender

6. Click the  **Save** button when all gateway setup is complete

After the new gateway is saved, the [Gateway of the System / Routing / Gateways Page](#) will load with the new gateway added to the table

Additional Information

This text-only information is also provided when viewing the Advanced area of the Gateway configuration (this is for monitoring traffic, not regular traffic being sent to the gateway):

Additional information	The time period, probe interval and loss interval are closely related. The ratio between these values control the accuracy of the numbers reported and the timeliness of alerts. A longer time period will provide smoother results for round trip time and loss, but will increase the time before a latency or loss alert is triggered. A shorter probe interval will decrease the time required before a latency or loss alert is triggered, but will use more network resource. Longer probe intervals will degrade the accuracy of the quality graphs. The ratio of the probe interval to the time period (minus the loss interval) also controls the resolution of loss reporting. To determine the resolution, the following formula can be used: $100 * \text{probe interval} / (\text{time period} - \text{loss interval})$ Rounding up to the nearest whole number will yield the resolution of loss reporting in percent. The default values provide a resolution of 1%. The default settings are recommended for most use cases. However if changing the settings, please observe the following restrictions: - The time period must be greater than twice the probe interval plus the loss interval. This guarantees there is at least one completed probe at all times. - The alert interval must be greater than or equal to the probe interval. There is no point checking for alerts more often than probes are done. - The loss interval must be greater than or equal to the high latency threshold.
-------------------------------	---

Advanced of the System / Routing / Gateways Page

For load balancing, giving a weight of 2 will make it get used twice as much as the first one. For every 3 connections, 1 will use the weight 1 gateway. Two connections will use the weight 2 gateway. If they are the same speed and should carry the same traffic, both should have a weight of 1. To put more traffic on your "main" link, set the main link with a weight of 2 and the other with a weight of 1. To be used more evenly but still prefer the first link, setup closer weights (ex.-5:4 instead of 2:1)

For failover, weights are not factored in. That is the Tier. For failover, set the preferred WAN to tier 1, the second to tier 2

Add A New Gateway Group

Overview



This procedure will explain how to add a new Gateway Group to the Anybus Defender

Procedure

1. Navigate to [System/Routing/Gateway Groups](#)
2. From the **Gateway Groups** tab, click the **Add** button on the lower right of the **Gateway Groups** table
3. An **Edit Gateway Group Entry** page will load:

The screenshot shows the 'Edit Gateway Group Entry' form. It has a dark blue header with the title 'Edit Gateway Group Entry'. The form contains several fields: 'Group Name' (text input), 'Gateway Priority' (text input), 'WAN_DHCP' (radio button), 'Never' (dropdown), 'Interface Address' (dropdown), and 'Interface WAN_DHCP Gateway' (radio button). Below these is a table with columns: Gateway, Tier, Virtual IP, and Description. The table has two rows: 'Link Priority' and 'Virtual IP'. The 'Link Priority' row has a description: 'The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted then the next available link(s) in the next priority level will be used.' The 'Virtual IP' row has a description: 'The virtual IP field selects which (virtual) IP should be used when this group applies to a local Dynamic DNS, IPsec or OpenVPN endpoint.' Below the table is a 'Trigger Level' dropdown menu with 'Member Down' selected. Below the dropdown is a text input field for 'Description'. At the bottom, there is a note: 'A description may be entered here for administrative reference (not parsed).'

Edit Gateway Group Entry of the System / Routing / Gateway Groups Page

1. From the **Gateway Group** configuration, adjust these options:
 - **Group Name:** A text entry for the gateway group name
 - **Gateway Priority:** The preference assigned to different gateways within a network to determine which gateway should be used for routing traffic under normal conditions and which should serve as backups or failover options
 - **Gateway:** A read-only text field showing the gateway
 - **Tier:** A dropdown to set the tier from never to tiers 1-5
 - **Virtual IP:** A dropdown for either the address on the interface defined in the gateway or a [Virtual IP](#)
 - **Trigger Level:** A dropdown field to select the event that would cause the exclusion of a member with events ranging from **Member Loss**, **Packet Loss**, **High Latency**, or both
 - **Description:** Optional description for this gateway group
2. Click the **Save** button when all gateway group setup is complete

After the new gateway group is saved, the [System/Routing/Gateway Groups](#) will load with the new gateway group added to the table

Add a New User

Overview

This procedure will explain how to add new users to the Anybus Defender. These may be used for WebGUI login purposes or tied to a [VPN User](#) for remote access

Procedure

1. Navigate to [System/User Manager/Users](#)
2. From the **Users** table, click the **+ Add** button
3. In the **User Properties** section, these options are available:

User Properties

Scope

Local

Warning: Changing this setting affects user behavior i.e. the user might be usable only for logging into services and not GUI

Disabled

☐ This user cannot login

Username

Password

Password

Confirm Password

Full name

User's full name, for administrative information only

Expiration date

Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings

☐ Use individual customized GUI options and dashboard layout for this user.

Group membership

admins

engineers

Not member of

Member of

>> Move to "Member of" list

<< Move to "Not member of" list

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate

☐ Click to create a user certificate

User Properties Section

Scope: Dropdown selection for the scope of the user database. **Local** uses an internal database where all privileges and actions are stored locally in the appliance. The **Remote** option allows for an external database, such as LDAP (including Active Directory) or RADIUS

ⓘ Changing this setting affects user behavior i.e. the user might be usable only for logging into services but not the WebGUI

Disabled: Checkbox to temporarily disable this user

Username: Text entry for the username.

ⓘ Only Alphanumeric characters and the underscore (_) are allowed

Password: Two text entries are used to enter a password and matching confirmation

Full name: Optional text entry for the user's full name

Expiration date: Text entry for an expiration date of this user. The date format is MM/DD/YYYY. Clicking in the text area will cause a calender dialog to appear allowing easy date selection:

07/17/2025

July 2025

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Date Selection Dialog

If left blank, this user will not expire

Custom Settings: Checkbox to all individualized custom GUI options and dashboard layout for this user. When this is checked, options will appear to set these customizations:

Top Navigation	Fixed (Remains visible at top of page) ▼			
	The fixed option is intended for large screens only.			
Dashboard Columns	2			
Interfaces Sort	☐ Sort Alphabetically If selected, lists of interfaces will be sorted by description, otherwise they are listed wan,lan,optn...			
Associated Panels Show/Hide	☐ Available Widgets Show the Available Widgets panel on the Dashboard.	☐ Log Filter Show the Log Filter panel in System Logs.	☐ Manage Log Show the Manage Log panel in System Logs.	☐ Monitoring Settings Show the Settings panel in Status Monitoring.
	These options allow certain panels to be automatically hidden on page load. A control is provided in the title bar to un-hide the panel.			
Left Column Labels	☐ Active If selected, clicking a label in the left column will select/toggle the first item of the group.			
Alias Popups	☐ Disable details in alias popups If selected, the details in alias popups will not be shown, just the alias description (e.g. in Firewall Rules).			
Browser tab text	☐ Display page name first in browser tab When this is unchecked, the browser tab shows the host name followed by the current page. Check this box to display the current page followed by the host name.			

Custom Settings

Group membership: Text selection boxes for **Not member of** and **Member of** to show which group this user is or isn't a member of respectively. Selections can be made in each text selector and the **>> Move to "Member of"** list and **<< Mover to "Not member of" list** buttons can be used to adjust groups accordingly

❗ Multiple selections are allowed by holding down the **Ctrl** and clicking on individual selections or the **Shift** button to click on a series of options

1. In the **Effective Privileges** section, privileges for this user can be added using the **+ Add** button:

Effective Privileges			
Inherited from	Name	Description	Action
			+ Add

Effective Privileges Section

From the **User Privileges** section, these options are available:

The Effective Privileges page shows a table of all privileges created\

Below the table is the **+ Add** button to add a new User Privilege, using these options:

User Privileges

User

D_12312

Assigned privileges

Asset Management

DCC

System - HA node sync

User - Config: Deny Config Write

User - Notices: View

User - Notices: View and Clear

User - Services: Captive Portal login

User - System: Copy files (scp)

User - System: Shell account access

User - System: SSH tunneling

User - VPN: IPsec xauth Dialin

User - VPN: L2TP Dialin

User - VPN: PPPOE Dialin

WebCfg - AJAX: Get Queue Stats

WebCfg - AJAX: Get Service Providers

WebCfg - AJAX: Get Stats

WebCfg - All pages

WebCfg - Crash reporter

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Filter

Show only the choices containing this term

Privilege information

The following privileges effectively give the user administrator-level access because the user gains access to execute general commands, edit system files, modify users, change passwords or similar:

User - System: Copy files (scp)

System - HA node sync

WebCfg - OpenVPN: Servers Edit Advanced

WebCfg - OpenVPN: Client Specific Override Edit Advanced

WebCfg - OpenVPN: Clients Edit Advanced

Please take care when granting these privileges.

Save

Filter

Clear

Indicates whether the user is able to login on the captive portal.

User Privileges Page

Assigned privileges: List selector of all the privileges allowed in the unit

- Multiple selections are allowed by holding down the **Ctrl** and clicking on individual selections or the **Shift** button to click on a series of options
- Click on an individual privilege to show a description of it in the blue banner at the bottom of this section

Filter: Text entry to filter the **Assigned privileges** list above. Type in the filter term and press Enter on your keyboard or use the **Filter** button at the bottom of this section

Click the **Save** button when the privilege assignment is complete. The **Users** page will load with the new assigned privileges on the table

- In the **User Certificates** section, Certificates for this user can be added using the **+ Add** button to [Create a New Certificate](#)

User Certificates	
Name	CA
+ Add	

User Certificates Section

i User Certificates can be used with [OpenVPN](#) for validating access. The [OpenVPN Client Procedure](#) explains how to set up clients for OpenVPN

2. In the **Keys** section, are these options:

- **Authorized SSH Keys:** Enter or paste the SSH Keys this user is authorized to use
- **IPsec Pre-Shared Key:** Enter or paste the IPsec Pre-Shared Key this user is authorized to use
- **Api Key:** Checkbox to allow the user to have access to the Anybus Defender REST API

i API Key does not function in the current version of Anybus Defender. It will be available in a future release

Keys	
Authorized SSH Keys	Enter authorized SSH keys for this user
IPsec Pre-Shared Key	
Api Key	☐ Allow this user to access the REST API

Keys Section

3. In the **Rule Templates** section are the [Rule Templates](#) available to move to and from the two list selectors. Use the **>> Move to "Apply Templates" list** and **<< Mover to "Available Templates of" list** buttons to adjust the rule templates accordingly

i The [Add Rule Template Procedure](#) explains how to set up these templates

4. Click the **Save** button when all user setup is complete

After the new user is saved, the [User Manager / Users Page](#) will load with the new user added to the table

Add a New User Group

Overview

This procedure will explain how to add new user groups to the Anybus Defender

Procedure

1. Navigate to [System/User Manager/Groups](#)
2. From the **Groups** table, click the **+ Add** button
3. In the **Group Properties** section, these options are available:

Group Properties

Group name

Scope

Local

Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description

Group description, for administrative information only

Group membership

D_12312
admin
mSmith999

Not members

>> Move to "Members"

Members

<< Move to "Not members"

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Group Properties Section

Group name: Text entry for the group name

Scope: Dropdown selection for the scope of the user database. **Local** uses an internal database where all privileges and actions are stored locally in the appliance. The **Remote** option allows for an external database, such as LDAP (including Active Directory) or RADIUS

ⓘ Changing this setting affects user behavior i.e. the user might be usable only for logging into services but not the WebGUI

Description: Text entry to add an optional description for this user group

Group membership: Two list selectors for **Not Members** and **Members** allow users to be added or removed from the group. Use the >> **Move to "Members"** and << **Move to "Not members"** to add and remove users as needed

ⓘ Multiple selections are allowed by holding down the **Ctrl** key and clicking on individual selections or the **Shift** button to click on a series of options

1. In the **Rule Templates** section, the options are available:

Rule Templates

Template selection

Sample_Template

Available Templates

>> Move to "Enabled Templates" list

Chosen Templates

<< Move to "Available Templates of" list

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Rule Templates Section

1. [Rule Templates](#) that are available to move to and from the two list selectors. Use the >> **Move to "Apply Templates" list** and << **Mover to "Available Templates of" list** buttons to adjust the rule templates accordingly

i The [Add Rule Template Procedure](#) explains how to set up these templates

2. Click the **Save** button when all user setup is complete

After the new user group is saved, the [System/User Manager/Groups](#) will load with the new user group added to the table

Add a New Authentication Server

Overview

This procedure will explain how to add a new authentication server to the Anybus Defender

Procedure

- 1. Navigate to [System/User Manager/Authentication Servers](#)
- 2. From the **Authentication Servers** table, click the **+ Add** button
- 3. In the **Server Settings** section, these options are available:

Server Settings	
Descriptive name	
Type	LDAP

Server Settings Section

Descriptive name: Enter a name for this server

Type: Dropdown to select either an LDAP (which includes Active Directory) or RADIUS server

- 1. If the Server Type selected above is **LDAP**, the **LDAP Server Settings** section will appear with these options:

LDAP Server Settings	
Hostname or IP address	NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.
Port value	389
Transport	Standard TCP
Peer Certificate Authority	Global Root CA List This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.
Protocol version	3
Server Timeout	25 Timeout for LDAP operations (seconds)
Search scope	Level One Level
Authentication containers	Containers Select a container Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component. Example: CN=Users,DC=example,DC=com or OU=Staff,OU=Freelancers
Extended query	☐ Enable extended query
Bind anonymous	☒ Use anonymous binds to resolve distinguished names
Initial Template	OpenLDAP
User naming attribute	cn
Group naming attribute	cn
Group member attribute	member
RFC 2307 Groups	☐ LDAP Server uses RFC 2307 style group membership RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).
Group Object Class	posixGroup Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".
Shell Authentication Group DN	If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login. Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com
UTF8 Encode	☐ UTF8 encode LDAP parameters before sending them to the server. Required to support international characters, but may not be supported by every LDAP server.
Username Alterations	☐ Do not strip away parts of the username after the @ symbol e.g. user@host becomes user when unchecked.
Allow unauthenticated bind	☒ Allow unauthenticated bind Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possibility to disable it.

LDAP Server Settings Section

Hostname or IP address: Enter the hostname or IP address of the LDAP server

ⓘ When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate

Port value: Enter the port number of the LDAP server

Transport: Dropdown to select which encryption to use: **Standard TCP** (none, not recommended), **STARTTLS Encrypted**, or **SSL/TLS Encrypted**

Peer Certificate Authority: Dropdown to select the Certificate Authority (CA) to use to validate the LDAP server certificate

ⓘ The CA is used only when **SSL/TLS Encrypted** or **STARTTLS Encrypted** Transport is active. This CA must match the CA used by the LDAP

Protocol version: Dropdown to select between LDAP 2 or LDAP 3

ⓘ LDAP 3 is compatible with LDAP 2. An LDAP 2 client can connect to an LDAP 3 server (this is a requirement of an LDAP 3 server). However, an LDAP 3 server can choose not to talk to an LDAP 2 client if LDAP 3 features are critical

Server Timeout: Enter a time in seconds for LDAP operations to timeout. If left blank, the default of 25 seconds will be used

Search scope: Dropdown to select the depth of the LDAP directory tree that should be searched. The **Base DN** text entry will serve as the starting point in the directory information tree (DIT). **One Level** will only search the base directory while **Entire Subtree** searches all sub-directories as well

Authentication containers: Text entry to enter directory entries that store user credentials and other authentication-related information

❗ Multiple entries are semi-colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc=component. Example: **CN=Users;DC=example,DC=com** or **OU=Staff;OU=Freelancers**

Extended query: Checkbox to enable extended queries

Bind anonymous: Checkbox to allow anonymous binds to resolve distinguished names

Initial Template: Dropdown to select the predefined structure or schema used to create and populate directory entries with default attributes and values. Available templates are: **OpenLDAP**, **Microsoft AD**, or **Novell eDirectory**

User naming attribute: Text entry for user entries in the directory. **cn** is entered as the default

Group naming attribute: Text entry for user group entries in the directory. **cn** is entered as the default

Group member attribute: Text entry for group members entries in the directory. **member** is entered as the default

RFC 2307 Groups: Checkbox if the LDAP Server uses RFC 2307 style group membership

❗ RFC 2307 style group membership has members listed on the group object rather than using groups listed on a user object. Leave unchecked for Active Directory style group membership (RFC 2307bis)

Group Object Class: Text entry for Object class used for groups in RFC2307 mode. If left blank, **posixGroup** will be used as default

Shell Authentication Group DN: Text entry for shell authentication via the LDAP server

❗ The user must be a member of this group and have a valid **posixAccount** attributes to be able to login
Example: **CN=Remoteshellusers,CN=Users,DC=example,DC=com**

UTF8 Encode: Checkbox for enable encoding LDAP parameters before being sent to the server

❗ This is required to support international characters, but may not be supported by every LDAP server

Username Alterations: Checkbox to prevent stripping away parts of the username after the @ symbol. When unchecked, e.g. **user@host** becomes **user**

Allow unauthenticated bind: Checkbox to allow unauthenticated binds

❗ Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any way to disable it

1. If the Server Type selected above is **RADIUS**, the **RADIUS Server Settings** section will appear with these options:

RADIUS Server Settings	
Protocol	MS-CHAPv2
Hostname or IP address	
Shared Secret	
Services offered	Authentication and Accounting
Authentication port	1812
Accounting port	1813
Authentication Timeout	
This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token.	
RADIUS NAS IP Attribute	WAN - 192.168.100.1
Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests. Please note that this choice won't change the interface used for contacting the RADIUS server.	

RADIUS Server Settings Section

Protocol: Dropdown to select the RADIUS protocol. Options are:

- PAP
- MD5-CHAP
- MS-CHAPv1
- MS-CHAPv2

Hostname or IP address: enter the hostname or IP address of the RADIUS server

Shared Secret: Enter the pre-configured, confidential key used to secure communication between the RADIUS client (such as a network access server) and the RADIUS server

Services offered: Dropdown to select which services are offered. Select from **Authentication and Accounting**, **Authentication**, or **Accounting**

Authentication port: Enter the port used for Authentication. 1812 is used by default

Accounting port: Enter the port used for Accounting. 1813 is used by default

Authentication Timeout: Enter a value, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds

i If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token

RADIUS NAS IP Attribute: Dropdown to select which configured interface will be used for contacting the RADIUS server

1. Click the **Save** button when all authentication server setup is complete

After the new authentication server is saved, the [System/User Manager/Authentication Servers](#) will load with the new server added to the table

Add New Interface Group

Overview

Interfaces / [Interface Groups](#) / [Edit](#)

Interfaces / Interface Groups / Edit

This procedure will explain how to add a new Industrial Profile Ruleset to the Anybus Defender

Procedure

1. Navigate to [Interfaces / Interface Assignments](#)
2. From the **Interface Groups** tab, click the **Add** button on the lower right corner of the **Interface Groups** table
3. An **Edit** page will load:

Interface Group Configuration

Group Name

Group Name

Only letters (A-Z), digits (0-9) and '_' are allowed. The group name cannot end with a digit.

Group Description

Group Description

A group description may be entered here for administrative reference (not parsed).

Group Members

WAN

LAN

VPN

DHCP_BETWEEN_VMLABSSERVER

NOTE: Rules for WAN type interfaces in groups do not contain the reply-to mechanism upon which Multi-WAN typically relies. [More Information](#)

Save

Interfaces / Interface Groups / Edit

1. From the **Interface Group** configuration, adjust these options:
 - **Group Name:** A text entry for the Interface Group name
 - **Description:** Optional description for the Interface Group
 - **Group Members:** Select the interfaces to be included in the interface group
2. Click the **Save** button when all configuration fields are complete

After the new Interface Group is saved, the [Interfaces / Interface Groups](#) will load with the new Interface Group added to the table

Add New VLAN Interface

Overview

Interfaces / VLANs / Edit

Interfaces / VLANs / Edit

This procedure will explain how to add a new Industrial Profile Ruleset to the Anybus Defender

Procedure

1. Navigate to [Interfaces / Interface Assignments](#)
2. From the **VLANs** tab, click the **Add** button on the lower right corner of the **VLAN Interface** table
3. An **Edit** page will load:

VLAN Configuration

Parent Interface

igb0 (00:0c:29:b3:d0:58) - wan

Only VLAN capable interfaces will be shown.

VLAN Tag

1

802.1Q VLAN tag (between 1 and 4094).

VLAN Priority

0

802.1Q VLAN Priority (between 0 and 7).

Description

Description

A group description may be entered here for administrative reference (not parsed).

Save

Interfaces / VLANs / Edit

1. From the **VLAN** configuration, adjust these options:
 - **Parent Interface:** Select the interface from which the VLAN will be created
 - **VLAN Tag:** Input a VLAN tag value from the range of 1 to 4094
 - **VLAN Priority:** Input the priority value from between 0 to 7

i

For more information on the priority value of the VLAN, navigate to [Interfaces / VLANs](#)

- **Description:** Optional description for the VLAN
2. Click the **Save** button when all configuration fields are complete

After the new VLAN is saved, the [Interfaces / VLANs](#) will load with the new VLAN added to the table

Add New Bridged Interface

Overview

Interfaces / Bridges / Edit

Interfaces / Bridges / Edit

This procedure will explain how to add a new Industrial Profile Ruleset to the Anybus Defender

Procedure

1. Navigate to [Interfaces / Interface Assignments](#)
2. From the **Bridges** tab, click the **Add** button on the lower right corner of the **Bridge Interfaces** table
3. An **Edit** page will load:

Bridge Configuration

Member Interfaces

WAN
LAN
VPN
DHCP_BETWEEN_VMLABSSERVER

Interfaces participating in the bridge.

Description

Advanced Options

Display Advanced

Save

Interfaces / Bridges / Edit

4. From the **Bridge** configuration, adjust these options:
 - **Member Interfaces:** Hold **Shift** and click the interfaces that will be bridged
 - **Description:** Optional description for the Bridge
 - **Display Advanced:** Selecting this button provides additional configuration options, allowing for more precise and customized settings. These advanced sections include:
 - **Advanced Configuration**
 - **RSTP/STP**
5. Click the **Save** button when all configuration fields are complete

After the new Bridged Interface is saved, the [Interfaces / Bridges](#) will load with the new Bridged Interface added to the table

ⓘ Bridging interfaces on a firewall can introduce several risks:

- **Security Bypass:** Bridging may bypass firewall security policies, allowing unchecked traffic
- **Network Loops:** Improper management can cause broadcast storms and network disruptions
- **Performance Impact:** Increased load on the firewall can degrade performance
- **Configuration Errors:** Misconfiguration can cause connectivity issues and unauthorized access
- **Complex Troubleshooting:** Bridging complicates diagnosing and resolving network issues

Add New LAGG

Overview

Interfaces / LAGGs / Edit

Interfaces / LAGGs / Edit

This procedure will explain how to add a new Industrial Profile Ruleset to the Anybus Defender

Procedure

1. Navigate to [Interfaces / Interface Assignments](#)
2. From the **LAGGs** tab, click the **Add** button on the lower right corner of the **LAGG Interfaces** table
3. An **Edit** page will load:

LAGG Configuration

Parent Interfaces

Choose the members that will be used for the link aggregation.

LAGG Protocol

NONE

- **NONE**
This protocol is intended to do nothing: it disables any traffic without disabling the lagg interface itself.
- **LACP**
Supports the IEEE 802.3ad Link Aggregation Control Protocol (LACP) and the Marker Protocol. LACP will negotiate a set of aggregable links with the peer in to one or more Link Aggregated Groups. Each LAG is composed of ports of the same speed, set to full-duplex operation. The traffic will be balanced across the ports in the LAG with the greatest total speed, in most cases there will only be one LAG which contains all ports. In the event of changes in physical connectivity, Link Aggregation will quickly converge to a new configuration.
- **FAILOVER**
Sends and receives traffic only through the master port. If the master port becomes unavailable, the next active port is used.
- **LOADBALANCE**
Balances outgoing traffic across the active ports based on hashed protocol header information and accepts incoming traffic from any active port. This is a static setup and does not negotiate aggregation with the peer or exchange frames to monitor the link. The hash includes the Ethernet source and destination address, and, if available, the VLAN tag, and the IP source and destination address.
- **ROUNDROBIN**
Distributes outgoing traffic using a round-robin scheduler through all active ports and accepts incoming traffic from any active port.

Description

Enter a description here for reference only (Not parsed).

Save

Interfaces / LAGGs / Edit

1. From the **LAGG** configuration, adjust these options:
 - **Parent Interfaces:** Select the interface from which the LAGG will be created
 - **LAGG Protocol:** Select the protocol from the dropdown that fits the desired configuration
- For more information on which protocol to select, reference the detailed breakdown below the dropdown box

 - **Description:** Optional description for the LAGG- 2. Click the **Save** button when all configuration fields are complete
- After the new LAGG is saved, the [Interfaces / LAGGs](#) will load with the new LAGG added to the table

Add a New IP Alias

Overview

This procedure will explain how to add an [Alias of IP Addresses](#) to the Anybus Defender. This can be useful to group similar devices together (PLCs, HMIs, etc) to minimize rule usage and allow for easier duplication of settings

Procedure

1. Navigate to [Firewall/Aliases](#)
2. From the **IP** tab, click the **Add** button
3. Enter information in the **Properties** section:

Firewall / Aliases / Edit

Properties	
Name	Vision_Cameras
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".	
Uuid	
Description	
A description may be entered here for administrative reference (not parsed).	
Type	Host(s) ▾

Aliases Properties Section

- **Name:** Enter a name for this alias

❗ The name can only consist of letters, numbers, and underscore (_) characters

- **Description:** Text entry for an optional description of this alias
- **Type:** Dropdown selection should be set to **Host(s)**

1. From the **Host(s)** section, enter the first device in the **IP or FQDN** row. Enter the IP address on the left text entry and an optional description in the right text entry:

Host(s)

Hint	Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.	
IP or FQDN	192.168.400.3	L_Front_Camera

Save

Export to file

+ Add Host

Aliases Properties Section

2. If more devices are to be added, click the **Add Host** button and repeat the previous step
3. When all devices are added, click the **Save** button
4. The [Firewall/Aliases](#) will load showing the new alias
5. Click the **Apply Changes** button to implement the changes to the Anybus Defender

❗ [Alias Nesting](#) is allowed to further group aliases

Usage

A typical use case for IP aliases are firewall rules that can be applied to all similar devices:

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Hint: Choose an Industrial Profile to send packets matching the flow for extra evaluation to the classifier.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

WAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Single host or alias

Vision_Cameras

/

Display Advanced

Rule Source with Alias Used

Add a New Port Alias

Overview

This procedure will explain how to add an [Alias of Ports](#) to the Anybus Defender. This can be useful to group ports together (HTTP, HTTPS) to minimize rule usage and allow for easier duplication of settings

Procedure

1. Navigate to [Firewall/Aliases](#)
2. From the **Ports** tab, click the **Add** button
3. Enter information in the **Properties** section:

Firewall / Aliases / Edit

Properties

Name	Web Ports
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".	
Description	
A description may be entered here for administrative reference (not parsed).	
Type	Port(s)

Aliases Properties Section

- **Name:** Enter a name for this alias

❗ The name can only consist of letters, numbers, and underscore (_) characters

- **Description:** Text entry for an optional description of this alias
- **Type:** Dropdown selection should be set to **Port(s)**

1. From the **Port(s)** section, enter the first port in the **Port** row. Enter the port number on the left text entry and an optional description in the right text entry:

Port(s)

Hint

Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

Port	80	HTTP
------	----	------

Save

+ Add Port

Aliases Properties Section

2. If more ports are to be added, click the **Add Port** button and repeat the previous step
3. When all ports are added, click the **Save** button
4. The [Firewall/Aliases](#) will load showing the new alias
5. Click the **Apply Changes** button to implement the changes to the Anybus Defender

❗ [Alias Nesting](#) is allowed to further group aliases

Usage

A typical usage for port aliases is a port forward setup:

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

Disabled

☐ Disable this rule

No RDR (NOT)

☐ Disable redirection for traffic matching this rule

This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface

WAN

Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Hide Advanced

Source

☐ Invert match.

Any

/

Source port range

Other

Web_Ports

Other

Web_Ports

From port

Custom

To port

Custom

Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (and should

Source Port Range with Alias Used

Nesting Aliases

Overview

This procedure will show how to create nest aliases in the Anybus Defender. This allows [IP Aliases](#) or [Port Aliases](#) to be combined for more efficient rule usage

Procedure

1. Go to either the [IP](#), [Port](#), or [URL](#) tabs from the [Firewall/Aliases](#) page
2. Click the **Add** button
3. Enter information in the **Properties** section:

Properties

Name

VisionDevices

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

A description may be entered here for administrative reference (not parsed).

Type

Host(s)

Aliases Properties Section

- **Name:** Enter a name for this alias
- **Description:** Text entry for an optional description of this alias
- **Type:** Dropdown selection should be set to the type of alias to be created (IP, Port, or URL)

4. In the section below, enter any previously-created aliases to the list using the **Add** button:

Host(s)

Hint

Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN

Vision_Cameras

Description

Delete

Scanners

Description

Delete

Save

Add Host

Aliases Properties Section

5. When all aliases are added, click the **Save** button
6. Click the **Apply Changes** button to implement the changes to the Anybus Defender

Usage

Nested aliases can be used anywhere individual aliases or items are used:

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Hint: Choose an Industrial Profile to send packets matching the flow for extra evaluation to the classifier.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

WAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Single host or alias

VisionDevices

/

Nested IP Alias used in a Firewall Rule

DPI Procedures Overview

Overview

DPI (Deep Packet Inspection) allows for packet inspection and filtering on any [Firewall Rule](#). It accomplishes this by adding a set of rules to a [Ruleset](#) and [Adding Rulesets to an Industrial Profile](#). This Industrial Profile can then be [Applied to Firewall Rules](#) which activates the DPI engine

To help with quickly and easily adding rules and rulesets to an Industrial Profile, the [Scheduled](#) or [Instant](#) Packet Capture procedure can be used to record device operations that can be blocked or allowed in a profile. The [Capture Analysis](#) can be used to filter the packet capture and add rules to [New Ruleset](#)

Rulesets can also be [Imported](#) or [Exported](#) for use in multiple Anybus Defender devices

Currently, the DPI engine works with these protocols:

- **EtherNetIP/CIP:** Used mostly by Rockwell Automation
- **Modbus TCP:** Used by a variety of manufacturers
- **S7 Classic/S7 Plus:** **S7 Classic** is used in older **Step 7 with SIMATIC Manager** software whereas **S7 Plus** is used in the newer **TIA Portal** environment

Add New Industrial Profile

Overview



This procedure will explain how to add a new Industrial Profile to the Anybus Defender

Procedure

1. Navigate to [Firewall / Industrial Protocols / Profile](#)
2. From the **Profiles** tab, click the **Add New Profile** button on the lower right corner of the **Profile Rules** table
3. An **Edit** page will load:

Firewall / Industrial Protocols / Profile / Edit

1. From the **Profile Options** configuration, adjust these options:
 - **Profile Name:** A text entry for the Industrial Profiles name
 - **Default Action for Packets:** A drop-down with the available options:
 - **Block:** Blocks Industrial Protocol packets that do not match any rules defined (used for whitelisting) in the Industrial Profile
 - **Pass:** Passes Industrial Protocol packets that do not match any rules defined (used for blacklisting) in the Industrial Profile
 - **Log:** Log Industrial Protocol packets that do not match any rules defined in the Industrial Profile
 - **Description:** Optional description for the Industrial Profile
2. From the **Profile Rules** configuration, each entry has three options:
 - **Default Action for Packets:** A drop-down with the available options:
 - **Block:** Blocks Industrial Protocol packets that match the rule or ruleset
 - **Pass:** Passes Industrial Protocol packets that match the rule or ruleset
 - **Log:** Log packets that match the rule or ruleset
 - **Industrial Protocol Rules:** A drop-down populated with rules or rulesets created using the DPI functionality
 - **Delete:** A delete button is available to remove any profile entries

ⓘ More entries can be added using the **Add another entry** button

3. Click the **Save** button when all configuration fields are complete

After the new Industrial Profile is saved, the [Firewall / Industrial Protocols / Profile](#) will load with the new Industrial Profile added to the table. For there, Industrial Profiles can be [Assigned to Firewall Rules](#)

Add New Ruleset

Overview

Firewall / Industrial Protocols / Ruleset / Edit

Firewall / Industrial Protocols / Ruleset / Edit

This procedure will explain how to add a new Industrial Profile Ruleset to the Anybus Defender

Procedure

1. Navigate to [Firewall / Industrial Protocols / Rulesets](#)
2. From the **Ruleset** tab, click the **Add New Ruleset** button on the lower left corner of the **Rulesets** table
3. An **Edit** page will load:

Profiles Options

Ruleset Name

The name of the ruleset may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

Description not parsed.

Group Rules

Rule(s)

Industrial protocol rules.

Delete

Save

+ Add another entry

Firewall / Industrial Protocols / Ruleset / Edit

1. From the **Profile Options** configuration, adjust these options:
 - **Profile Name:** A text entry for the Industrial Profiles name
 - **Description:** Optional description for the Ruleset
 2. From the **Group Rules** configuration, each entry has a drop-down:
 - **Rule(s):** A drop-down populated by rules obtained when using the analyze capture feature located in [Firewall / Industrial Protocols / Analysis](#) or after use a [Scheduled](#) or [Instant](#) Packet Capture procedure[Packet Capture](#)
 - **Delete:** A delete button is available to remove any rule entries
- More entries can be added using the **Add another entry** button
3. Click the **Save** button when all configuration fields are complete

After the new Ruleset is saved, the [Firewall / Industrial Protocols / Ruleset](#) will load with the new Ruleset added to the table

Upload File For Capture Analysis

Overview

Firewall / Industrial Protocols / Analysis



Firewall / Industrial Protocols / Analysis

This procedure will explain how to analyze a packet capture using the Anybus Defender

❗ A [Scheduled](#) or [Instant](#) Packet Capture created in the Anybus Defender or external application such as **Wireshark** is required to use this procedure. This packet capture should have device operation packets that will be used in the actual rules and rulesets explain below

Procedure

1. Navigate to [Firewall / Industrial Protocols / Analysis](#)
2. From the **Analysis** tab, click the **Choose File** button in the lower left corner of the **Capture Analysis** section
3. Once the desired PCAP is selected, click the **Upload File** button and more information is prompted

❗ Depending on the size of the packet capture, it may take a few seconds to upload

❗ If the packet capture does not contain Industrial protocol packets(such as Modbus TCP or CIP), no rules will be generated

4. When the upload completes, additional sections appear:

Rules				
Select All ☐	Packet#	Proto	Proto Info	Description
☐	285	S7COMM_PLUS	AckData (0x03) OpCode: Response (0x32) Func: SetMultiVariables (0x0542)	(1) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	278	S7COMM_PLUS	AckData (0x03) OpCode: Request (0x31) Func: SetMultiVariables (0x0542)	(1) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	253	S7COMM_PLUS	AckData (0x03) OpCode: Response (0x32) Func: GetMultiVariables (0x054C)	(10) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	250	S7COMM_PLUS	AckData (0x03) OpCode: Request (0x31) Func: GetMultiVariables (0x054C)	(10) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	246	S7COMM_PLUS	AckData (0x03) OpCode: Response (0x32) Func: GetLink (0x0524)	(2) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	242	S7COMM_PLUS	AckData (0x03) OpCode: Request (0x31) Func: GetLink (0x0524)	(2) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	229	S7COMM_PLUS	AckData (0x03) OpCode: Response (0x32) Func: Invoke (0x056B)	(1) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	228	S7COMM_PLUS	AckData (0x03) OpCode: Request (0x31) Func: Invoke (0x056B)	(1) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	216	S7COMM_PLUS	AckData (0x03) OpCode: Notification (0x33)	(8) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	206	S7COMM_PLUS	AckData (0x03) OpCode: Response (0x32) Func: Explore (0x04BB)	(4) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	205	S7COMM_PLUS	AckData (0x03) OpCode: Request (0x31) Func: Explore (0x04BB)	(4) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	184	S7COMM_PLUS	AckData (0x03) OpCode: Response (0x32) Func: CreateObject (0x04CA)	(7) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	183	S7COMM_PLUS	AckData (0x03) OpCode: Request (0x31) Func: CreateObject (0x04CA)	(7) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	59	S7COMM_PLUS	AckData (0x03) OpCode: Response (0x32) Func: DeleteObject (0x04D4)	(12) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	58	S7COMM_PLUS	AckData (0x03) OpCode: Request (0x31) Func: DeleteObject (0x04D4)	(12) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	29	S7COMM_PLUS	Event (0xfe)	(9) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	16	S7COMM_PLUS	AckData (0x03) OpCode: Response (0x32) Func: GetVarSubStreamed (0x0586)	(37) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	15	S7COMM_PLUS	AckData (0x03) OpCode: Response (0x32) Func: SetVariable (0x04F2)	(11) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	14	S7COMM_PLUS	AckData (0x03) OpCode: Request (0x31) Func: GetVarSubStreamed (0x0586)	(37) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	14	S7COMM_PLUS	AckData (0x03) OpCode: Request (0x31) Func: SetVariable (0x04F2)	(11) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	11	S7COMM_PLUS	Ack (0x02) OpCode: Response (0x32) Func: SetMultiVariables (0x0542)	(5) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	10	S7COMM_PLUS	Ack (0x02) OpCode: Request (0x31) Func: SetMultiVariables (0x0542)	(5) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	7	S7COMM_PLUS	Job (0x01) OpCode: Response (0x32) Func: CreateObject (0x04CA)	(5) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
☐	6	S7COMM_PLUS	Job (0x01) OpCode: Request (0x31) Func: CreateObject (0x04CA)	(5) packets matched with this S7COMM PLUS data. (from packetcapture.pcap) +
Existing Rules (0)  Display				
Actions				
Add Rules	Add New Profile	Add New Ruleset	Add To Existing Profile	Add To Existing Ruleset
 Add New Rules				

Firewall / Industrial Protocols / Analysis

5. From the **Rules** and **Existing Rules** tables, these options are configurable:

- **Select Column:** This column is used to select individual rules or all rules. Once selected they can be added to the rules table or they can be added directly to a new ruleset
- **Plus Sign:** Selecting this button will just add the selected rule to the [Firewall / Industrial Protocols / Rules](#) table

i Only new rules that don't already exist will populate the **Rules** table. Existing rules will populate the **Existing Rules** table

6. From the **Actions** table, depending on the intended use for the selected rules these are the available options:

- **Add Rules:** Add the selected rules to the **Rules** table located on the [Firewall / Industrial Protocols / Rules](#) page by clicking the **Add New Profile** button
- **Add New Profile:** Add the selected rules to a new Industrial Protocol profile. These are the configurable fields available:
 - **New Profile Name:** A text box to name the profile

- **Profile Default Action:** Select the default action to **Pass** (Blacklist) or **Block** (Whitelist) Industrial Protocol packets that do not match any rule
 - **Profile Action On Above Rules:** Select the default action to **Pass** (Whitelist), **Block** (Blacklist), or **Log** for the Industrial Protocol packets that match any rule
 - **Description:** Optional description for the Industrial Profile
 - **Add New Ruleset:** Add the selected rules to a new Ruleset. These are the configurable fields available:
 - **Ruleset Name:** A text box to name the Ruleset
 - **Description:** Optional description for the Ruleset
 - **Add To Existing Profile:** Allows the selected rules to be added to an already existing Industrial Protocol profile. These are the configurable fields available:
 - **Choose Profile:** Select from the drop-down the profile these new rules will be added
 - **Profile Action on Above Rules:** Select the default action to **Pass** (Whitelist), **Block** (Blacklist), or **Log** for the Industrial Protocol packets that match any rule
 - **Add To Existing Ruleset:** Allows the selectable rules to be added to an already existing Industrial Protocol ruleset. These are the configurable fields available:
 - **Choose Ruleset:** Select the ruleset that the new rules will be added
7. Click the **Add** button when all configuration fields are complete on the respective tab

❗ Once the selected option is selected, navigate to the [Diagnostics / States](#) page. Select the **Reset the Firewall State Table** option and then click the **Reset** button

Export Industrial Profile Ruleset(s)

Overview

Firewall / Industrial Protocols / Ruleset / Backup/Restore

Firewall / Industrial Protocols / Ruleset / Backup/Restore

This procedure will explain how to export an Industrial Protocol Ruleset on the Anybus Defender

Procedure

1. Navigate to [Firewall / Industrial Protocols / Rulesets](#)
2. From the **Rulesets** tab, click the **Import/Export Selected Rulesets** button on the lower right corner of the **Rulesets** table
3. A **Backup/Restore** page will load:

Export Industrial Protocol Ruleset(s) Configuration

Encryption

☐ Encrypt this file.

Export Ruleset(s) as XML

Import Industrial Protocol Ruleset(s) Configuration

Open an Anybus Defender Ruleset configuration file and click the button below to import the configuration.

Configuration file

Choose File

S7_Plus_Online_Only.xml

Encryption

☐ Configuration file is encrypted.

Import Ruleset(s)

Import Ruleset configuration

Firewall / Industrial Protocols / Ruleset / Export and Import

1. From the **Export Industrial Protocol Ruleset(s)** configuration, there is an option that can be adjusted:
 - **Encryption:** Checking this box will encrypt the ruleset(s). Once checked, a text box to enter a custom password is prompted. This password is used when importing the ruleset backup
2. Click the **Export Ruleset(s) as XML** button when all configuration fields are complete

Import Industrial Profile Ruleset(s)

Overview

Firewall / Industrial Protocols / Ruleset / Backup/Restore



Firewall / Industrial Protocols / Ruleset / Backup/Restore

This procedure will explain how to import an Industrial Protocol Ruleset on the Anybus Defender

Procedure

1. Navigate to [Firewall / Industrial Protocols / Rulesets](#)
2. From the **Rulesets** tab, click the **Import/Export Selected Rulesets** button on the lower right corner of the **Rulesets** table
3. A **Backup/Restore** page will load:

Export Industrial Protocol Ruleset(s) Configuration	
Encryption	☐ Encrypt this file.
Export Ruleset(s) as XML	

Import Industrial Protocol Ruleset(s) Configuration	
Open an Anybus Defender Ruleset configuration file and click the button below to import the configuration.	
Configuration file	Choose File S7_Plus_Online_Only.xml
Encryption	☐ Configuration file is encrypted.
Import Ruleset(s)	
Import Ruleset configuration	

Firewall / Industrial Protocols / Ruleset / Backup/Restore

1. From the **Import Industrial Protocol Ruleset(s)** configuration, adjust the following options:
 - **Configuration File:** Select the **Choose File** button and locate the Rulesets configuration XML file
 - **Encryption:** Check the checkbox if the Rulesets configuration was encrypted during the export process. This will also require the password that was used to encrypt the file to be entered into a prompted text box

❗ If the password entered does not match the one that was set for the ruleset(s) backup, the process will prompt an error and the file will have to be re-uploaded using the **Choose File** button

2. Click the **Import Ruleset(s)** button when all configuration fields are complete

After the new Ruleset is saved, the [Firewall / Industrial Protocols / Ruleset](#) will load with the new Ruleset added to the table

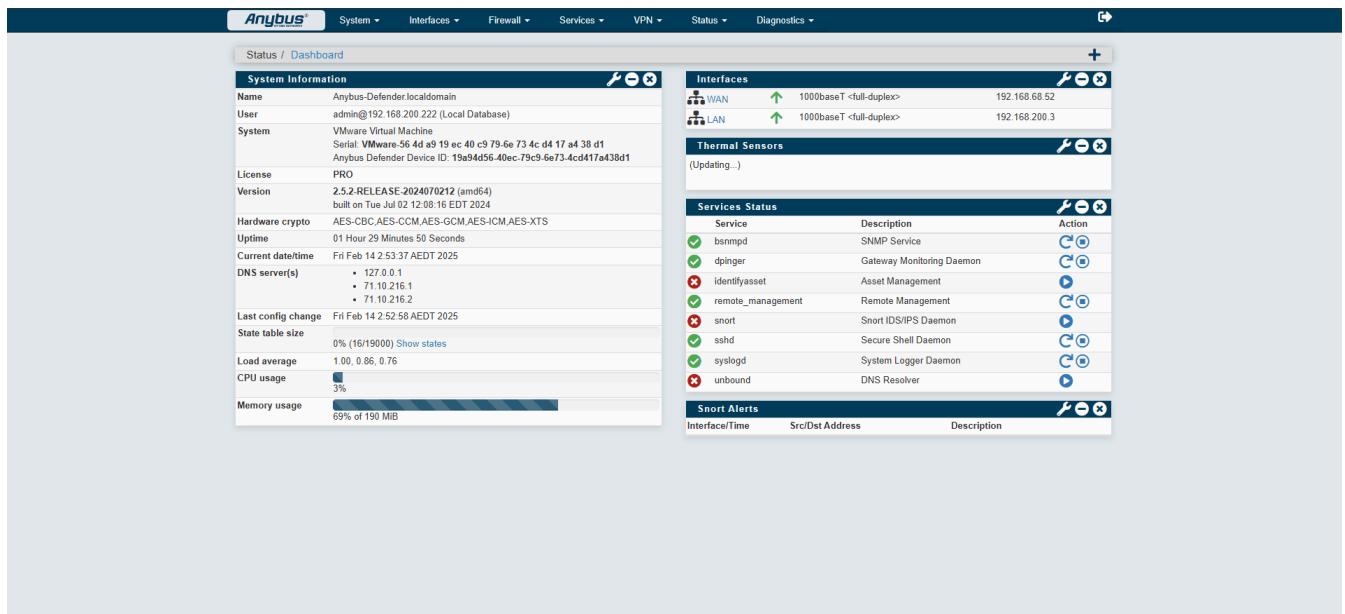
These rulesets can be [Added to an Industrial Profile](#)

Apply Industrial Profile to Rules

Overview

Once [Industrial Profiles](#) are created, they can be applied to [Firewall Rules](#)

Procedure



Screen Capture of Industrial Profile Added to a Rule

1. Navigate to **Firewall>Rules**
2. Select the appropriate rule from the interface
3. From the **Action** selection, change to **Industrial Profile**
4. From the **Industrial Profile** selection that appears, select the desired [Industrial Profile](#)

❗ The **Protocol** option cannot be set to **Any** when using Industrial Profiles. Set it to the appropriate protocol (usually TCP and/or UDP)

5. Apply the new changes

❗ If adding an Industrial Profile doesn't seem to work, perform a [Reset States](#) (this will temporary disable firewall traffic)

S7 (Siemens) Industrial Profile Example:

A ruleset was created with rules only allowing a user to go online and offline. Any changes to the project that require updating the PLC will cause the user to be taken offline:

Firewall / Rules / Edit

Edit Firewall Rule

Action

Industrial Profile

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Hint: Choose an Industrial Profile to send packets matching the flow for extra evaluation to the classifier.

Industrial Profile

S7_Online_Only

Hint: Choose a profile from the Industrial Profile use in validating controls traffic

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

WAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP/UDP

Choose which IP protocol this rule should match.

Siemens PLC on 1:1 NAT with the Industrial Profile Assigned to the Device's WAN Rule

Load results

?

Status and actions after downloading to device

Status	!	Target	Message	Action
		▼ PLC_2	Error while loading: Loading has been aborted!	Load 'PLC_2'
		▼ Download to device	Error downloading to device.	
			Error downloading to module "PLC_2".	

Failed Attempt to Download a Software Change in TIA Portal

Firewall Procedures Overview

Overview

This subsection shows procedures for the **Rules** menu selection of the Anybus Defender. These include:

- [NAT Port Forwarding](#)
- [Outbound NAT](#)
- [Interface and Floating Rules](#)
- [Firewall Scheduling](#)
- [Rule Templates and Template Rules](#)
- [Virtual IPs](#)

Add NAT Port Forward

Overview

Port Forward

1:1

Outbound

NPt

Simple NAT Wizard

Rules

☐	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
☐	☒	WAN	TCP	*	*	WAN address	21 (FTP)	192.168.74.33	21 (FTP)	FTP Port Forward

Add

Add

Delete

Save

Separator

Legend

Pass

Linked rule

Firewall / NAT / Port Forward / Edit

This procedure will explain how to add a new Port Forward to the Anybus Defender. Port forwards allows opening of a specific port, port range or protocol to a privately addressed device on the internal network

Procedure

1. Navigate to [Firewall / NAT / Port Forward](#)

2. From the **Port Forward** tab, click the **Add** button on the lower right corner of the **Rules** table
- Selecting the **Add** button with an up arrow adds a rule to the top of the list. Where the **Add** button with a down arrow adds a rule to the bottom of the list

3. An **Edit** page will load:

Edit Redirect Entry

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source Display Advanced

Destination ☐ Invert match. WAN address Type Address/mask

Destination port range FTP From port Custom FTP To port Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP Single host Type 10.17.200.5 Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80::) to local scope (::1)

Redirect target port FTP Port Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Description
A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync ☐ Do not automatically sync to other Hot Standby members
This prevents the rule on Master from automatically syncing to other Hot Standby members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection Use system default

Filter rule association Add associated filter rule
The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.

Save

Firewall / NAT / Port Forward / Edit Showing FTP Port Forward Example

4. From the **Edit Redirect Entry** configuration, adjust these options:

- **Disabled:** Selecting this checkbox disables the port forward rule
- **No RDR (NOT):** When checked, the behavior of the port forward is negated meaning that no redirection should be performed when the rule is matched, versus the default behavior of redirecting when the rule is matched. In most common configurations, this option remains unchecked
- **Interface:** Select an interface from the dropdown to apply the port forward. Typically, this will be set to the **WAN**
- **Address Family:** Select the internet protocol version from the dropdown. The recommended option is **IPv4**
- **Protocol:** Select a protocol from the dropdown that this rule will affect. This is usually **TCP** and/or **UDP**
- **Source:** By default, this option is set to **any** source. Selecting the **Display Advanced** button to access the option to specify the source type, address, and port range. Setting these will further restrict who can access this forwarded port
- **Destination:** Select an interface from the dropdown from which the external traffic will be forwarded
- **Destination Port Range:** Select the **From Port** and **To Port** from the dropdowns to specify the internal port that the external traffic will be set to access

❗ If selection is left as **Other**, ports can be entered manually in the To/From **Custom** text entries. Adjust each port dropdowns for pre-allocated ports (e.g. HTTP is port 80)

- **Redirect Target IP:** Select from the dropdown one of these options:
 - **Single Host:** Enter a custom IP. This option is recommended as this will be the internal device's IP that is being accessed from external traffic
 - **Interface:** Select an interface to be used

- **Redirect Target Port:** Select the port that the rule for redirection to the destination IP and port

❗ If selection is left as **Other**, ports can be entered manually in the To/From **Custom** text entries. Adjust each port dropdowns for pre-allocated ports

- **Description:** Optional description for the Port Forward
- **No XMLRPC Sync:** Checkbox to prevent the rule on the Master from automatically syncing to other Hot Standby members

❗ This does NOT prevent the rule from being overwritten on Slave

- **NAT reflection:** Allows **NAT Reflection** to be:
 - **Use system default**
 - Enable with **Pure NAT**
 - Enable with **NAT**
 - **Disabled**
- **Filter rule association:** Drop to allow associating a rule to the port forwarding. Options are:
 - **None**
 - **Add associated filter rule**
 - **Add Unassociated filter rule**
 - **Pass**

5. Click the **Save** button when all configuration fields are complete

After the new Industrial Profile is saved, the [Firewall / NAT / Port Forward](#) will load with the new Port Forward added to the table

Add Outbound NAT

Overview

Firewall / NAT / Outbound

Port Forward1:1OutboundNPTSimple NAT Wizard

Outbound NAT Mode

Mode

☐

Automatic outbound NAT rule generation.
(IPsec passthrough included)

☒

Hybrid Outbound NAT rule generation.
(Automatic Outbound NAT + rules below)

☐

Manual Outbound NAT rule generation.
(AON - Advanced Outbound NAT)

☐

Disable Outbound NAT rule generation.
(No Outbound NAT rules)

Save

Mappings

☐	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
☒	WAN	10.2.14.22/32	tcp/*	174.34.24.22/32	tcp/ 1433	4.4.4.4	*	✓		

AddAddDeleteSave

Automatic Rules:

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓	WAN	127.0.0.0/8 ::1/28 192.168.200.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓	WAN	127.0.0.0/8 ::1/28 192.168.200.0/24	*	*	*	WAN address	*	✗	Auto created rule

Firewall / NAT / Outbound / Edit Showing a Mapping (see below)

This procedure will explain how to add a new Outbound NAT to the Anybus Defender. This allows LAN-type hosts to access public ones.

Procedure

1. Navigate to [Firewall / NAT / Outbound](#)
2. Determine which **Mode** to use before adding any new **Mappings**. Options are:
 - **Automatic:** A mapping is automatically generated (in the **Automatic Rules** section) for each interface's subnet (except WAN-type connections) and the rules on the **Mappings** section of this page are ignored
 - **Hybrid:** Mappings specified on this page will be used, followed by the automatically generated ones
 - **Manual:** Outbound NAT rules will not be automatically generated and only the mappings specified on the **Mappings** section will be used
 - **Disable:** No rules will be used

If a target address other than an interface's IP address is used, then depending on the way the WAN connection is setup, a Virtual IP may also be required

3. From the **Outbound** tab, click the **Add** button on the lower right corner of the **Mappings** table

Selecting the **Add** button with an up arrow adds a rule to the top of the list. Where the **Add** button with a down arrow adds a rule to the bottom of the list

4. An **Edit Advanced Outbound NAT Entry** page will load. Here is an example of a remote connection to a corporate database on a remote site:

Edit Advanced Outbound NAT Entry			
Disabled	☐ Disable this rule		
Do not NAT	☐ Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules In most cases this option is not required.		
Interface	WAN		
The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.			
Address Family	IPv4+IPv6		
Select the Internet Protocol version this rule applies to.			
Protocol	TCP		
Choose which protocol this rule should match. In most cases "any" is specified.			
Source	Network	10.2.14.22 / 32	
Type		Source network for the outbound NAT mapping.	
Destination	Network	174.34.24.22 / 32	1433
Type		Destination network for the outbound NAT mapping.	
☐ Not		Port or Range	
Invert the sense of the destination match.			
Translation			
Address	4.4.4.4 (WAN_VirtIP_4_4_4_4)		
Connections matching this rule will be mapped to the specified Address. The Address can be an Interface, a Host-type Alias, or a Virtual IP address.			
Port or Range			☒ Static Port
Enter the external source Port or Range used for remapping the original source port on connections matching the rule. Port ranges are a low port and high port number separated by "-". Leave blank when Static Port is checked.			
Misc			
No XMLRPC Sync	☐		
Prevents the rule on Master from automatically syncing to other Hot Standby members. This does NOT prevent the rule from being overwritten on Slave.			
Description			
A description may be entered here for administrative reference (not parsed).			
Rule Information			
Created	10/16/24 14:29:42 by admin@192.168.200.222 (Local Database)		
Updated	10/16/24 14:29:42 by admin@192.168.200.222 (Local Database)		
			

Firewall / NAT / Outbound / Edit Example Showing Local IP to Outbound Connection to a Corporate MSSQL Database

i As mentioned above, a **Virtual IP** was needed to allow remote access to the Database

- From the **Edit Advanced Outbound NAT Entry** configuration, adjust these options:
 - Disabled:** Selecting this checkbox disables the NAT 1:1 rule
 - Interface:** Select the interface from the dropdown where the Outbound NAT will be applied
 - Address Family:** Select the internet protocol version from the dropdown. The recommended option is IPv4
 - Protocol:** Select the protocol from the dropdown to which this rule will apply. The recommended option would be to leave this as **Any**
 - Source:** Select from the dropdown the internal network or IP address that will be translated when communicating with the external network
 - Destination:** Select from the dropdown the external network or IP address for where the translated traffic will be directed
- From the **Translation** configuration, adjust these options:
 - Address:** Select the address or alias from the dropdown. Connections matching this rule will be mapped to the specified address
 - Port or Range:** Input the external port or port range which will be used for translating the internal source for connections matching the rule. When the **Static** checkbox is selected, leave the textbox empty
- Click the **Save** button when all configuration fields are complete

After the new Industrial Profile is saved, the [Firewall / NAT / Outbound](#) will load with the new Outbound NAT added to the table

Add Interface Rule

Overview

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Hint: Choose an Industrial Profile to send packets matching the flow for extra evaluation to the classifier.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

WAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Single host or alias

70.111.23.45

/

Display Advanced

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination

☐ Invert match

LAN net

Destination Address

/

Destination Port Range

EIP (44818)

From

Custom

To

EIP (44818)

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Firewall WAN Rule Example allowing 1 WAN Device Access To LAN Network VIA Ethernet/IP

This procedure will explain how to add a new rule to an interface on the Anybus Defender

❗ This procedure applies to all interfaces configured in the Anybus Defender

This also includes [Floating Rules](#) which will be used on all interfaces

❗ Interface rules are usually meant for ingress or egress from or to an interface. **Floating Rules** break this convention and should only be used under specific circumstances

Procedure

1. Navigate to [Firewall / Rules / WAN](#) or other appropriate interface tab
2. From the **WAN** tab, click the **Add** button on the lower right corner of the **Rules** table

❗ Selecting the **Add** button with an up arrow adds a rule to the top of the list. Where the **Add** button with a down arrow adds a rule to the bottom of the list

3. An **Edit** page will load:

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Hint: Choose an Industrial Profile to send packets matching the flow for extra evaluation to the classifier.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

WAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

any

Source Address

/

Display Advanced

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination

☐ Invert match

any

Destination Address

/

Destination Port Range

(other)

From

Custom

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Save

Firewall / Rules / Edit

1. From the **Edit Firewall Rule** configuration, adjust these options:

- **Action:** A dropdown populated with the available options:
 - **Pass:** Allow the specified traffic
 - **Block:** Deny the specified traffic
 - **Reject:** Deny the specified traffic while returning a TCP RST or equivalent packet to notify the connection has been disconnected
 - **Industrial Profile:** Selecting this option will prompt another dropdown allowing for the selection of a configured industrial profile
- **Interface:** A dropdown that is auto-populated based on which interface the **Add** button was selected. Ensure this is not changed while configuring the rest of the rule
- **Address Family:** Select the internet protocol version from the dropdown. The recommended option is IPv4
- **Protocol:** Select the protocol which the rule will match

2. From the **Source** configuration, it is recommended to leave this section as the default value of **Any**

3. From the **Destination** configuration, adjust these options:

- **Destination:** Select from a dropdown the type of destination this rule will be applied
- **Destination Port Range:** Select from the **From** dropdown to specify a port for the rule. The **To** dropdown may be left empty if only filtering for a single port

4. Click the **Save** button when all configuration fields are complete

After the new Industrial Profile is saved, the [Firewall / Rules / WAN](#) will load with the new Industrial Profile added to the table

Add Firewall Schedule

Overview

This procedure will explain how to add a new firewall schedule to the Anybus Defender

Procedure

1. Navigate to [Firewall / Schedules](#)
2. From the **Schedules** page, click the **Add** button on the lower right corner of the **Profile Rules** table
3. An **Edit** page will load:

Schedule Information

Schedule Name

The name of the schedule may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

A description may be entered here for administrative reference (not parsed).

Month

July_24

Date

July_2024

Mon	Tue	Wed	Thu	Fri	Sat	Sun
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Click individual date to select that date only. Click the appropriate weekday Header to select all occurrences of that weekday.

Time

0

00

23

59

Start Hrs

Start Mins

Stop Hrs

Stop Mins

Select the time range for the day(s) selected on the Month(s) above. A full day is 0:00-23:59.

Time range description

A description may be entered here for administrative reference (not parsed).

+ Add Time

Clear selection

Configured Ranges

Save

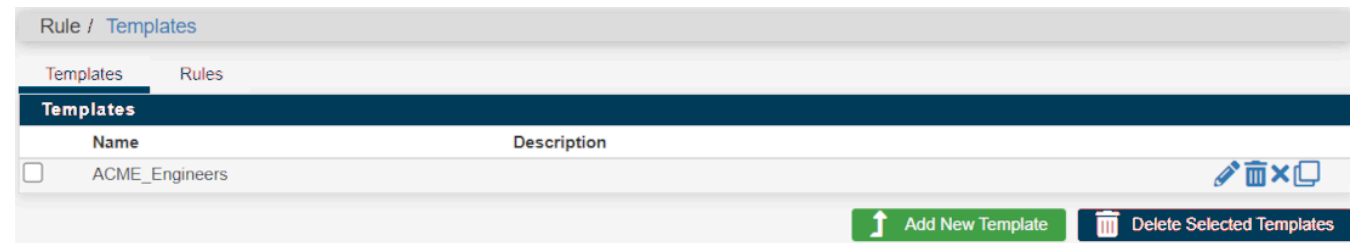
1. From the **Schedule Information** configuration, adjust these options:
 - **Schedule Name:** A text entry for the Schedule name
 - **Description:** Optional description for the Schedule
 - **Month:** Select the month in which this schedule will take place
 - **Date:** Select from a calendar the day(s) this schedule will take place
 - **Time:** Select from the dropdowns the start hours, start minutes, stop hours, and stop minutes the task this schedule is assigned to will take place
 - **Time Range Description:** Optional description for the Schedule Time Range

1. Click the **Add Time** button when all configuration fields are complete adding the time range to the **Configured Ranges** section
2. Click the **Save** button when all the desired time ranges are configured for the schedule

After the new Schedule is saved, the [Firewall / Schedules](#) will load with the new Schedule added to the table

Add a New Rule Template

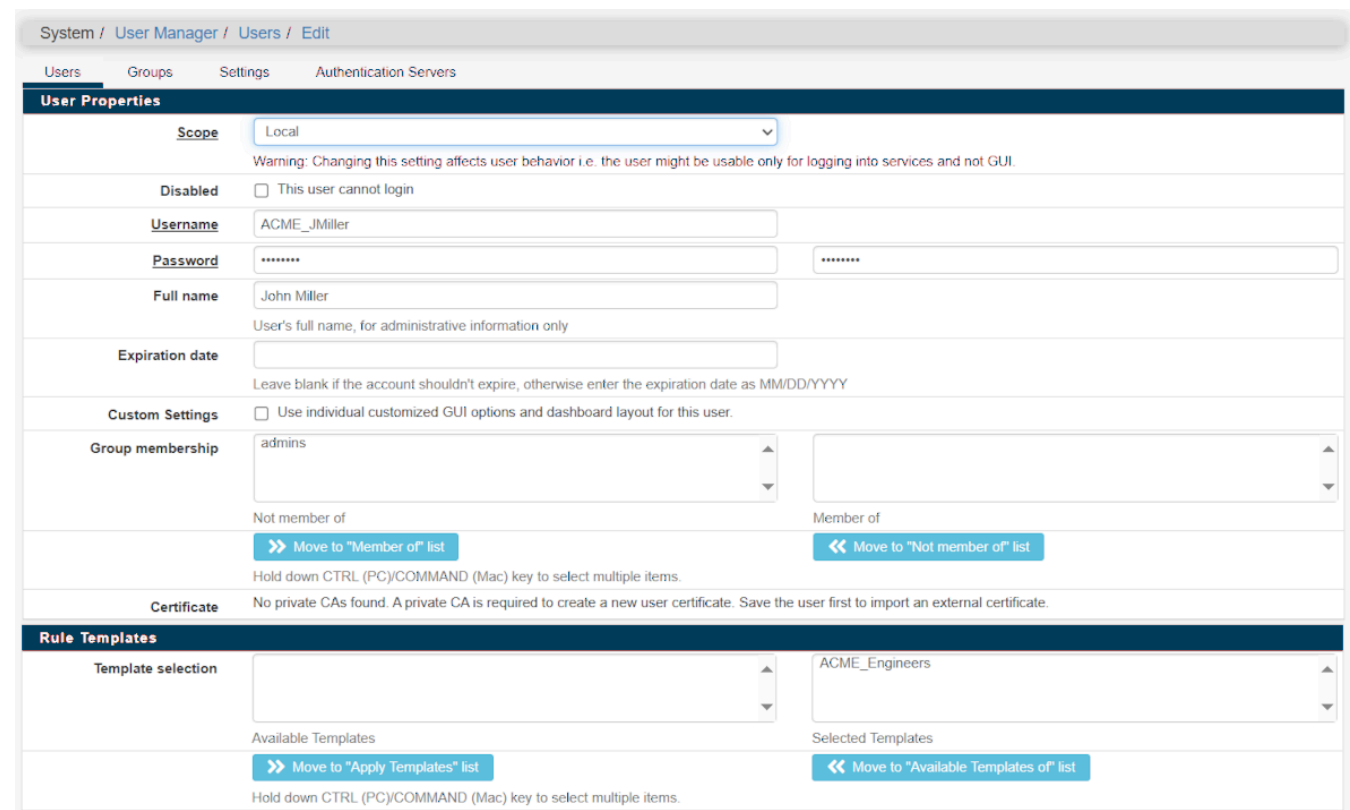
Overview



Firewall / Rule / Templates Showing Sample Rule Template

This procedure will explain how to add a new template to the Anybus Defender. Templates can be used with the [Users](#) created for local or [OpenVPN](#) access to customize rules based on that user

❗ With templates created as shown in the image above, they can be assigned to Users to restrict access to interface devices:

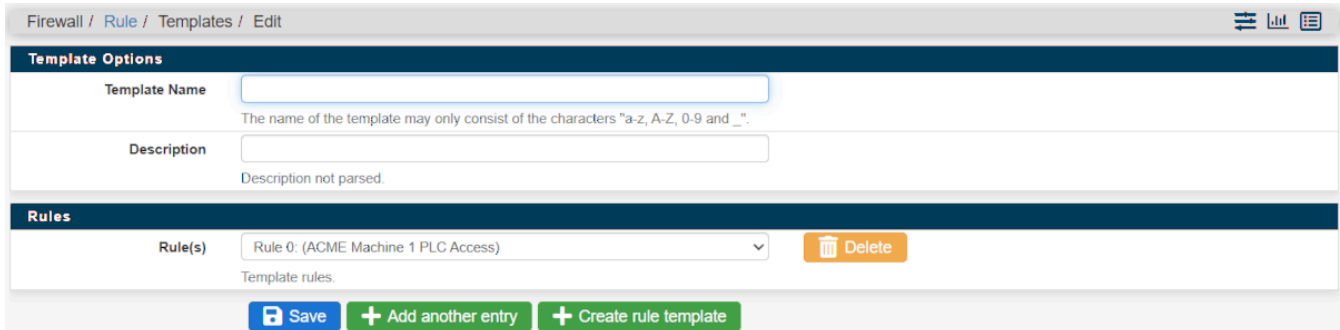


User Creation with Rule Template Added

Below are two procedures: one for adding a new Rule Template and another for adding rules used in templates

New Rule Template Procedure

1. Navigate to [Firewall / Template Rules](#)
2. Click the **Add New Template** button on the lower right corner of the **Templates** table
3. An **Edit** page will load:



Firewall / Industrial Protocols / Profile / Edit

1. From the **Template Options** section, adjust these options:
 - **Template Name:** A text entry for the Rule Template name
 - **Description:** Optional description for the template
2. From the **Rules** section, template rules can be added using the **+ Add another entry** which allows adding rules that have already been created

❗ New Rules can be added using the **+ Create rule template** button (see procedure below)

3. Click the **Save** button when all **Template Options** and **Rules Entries** are completed

After the new Industrial Profile is saved, the [Rule Template](#) page will load with the new Rule Template added to the table

New Rules for Template Use Procedure

❗ Rules can be created and used on any Template. These rules can be created for any interface used in the Anybus Defender

This also includes [Floating Rules](#) which will be used on all interfaces

❗ Interface rules are usually meant for ingress or egress from or to an interface. **Floating Rules** break this convention and should only be used under specific circumstances

1. Navigation to **Template Rules** can be done in these ways:
 - Navigate to **Firewall / Template Rules** and click the **Rules** tab
 - When editing a **Rule Template**(see above), click the **+ Create rule template** button
2. Select the appropriate [Interface](#) to use for the rule
3. From the **Edit Firewall Rule** section, edit these items:
 - **Action:** Select either **Pass**, **Block**, **Reject** (Blocks but notifies sender), or [Industrial Profile](#)
 - **Protocol:** Adjust the protocol if needed (usually **TCP** and/or **UDP**)
4. From the **Destination** section, adjust the drop down from **any** to match the type of destination (usually a **Single Host**)

- From the **Destination Port Range** row, adjust the **From** and **To** ports to use defined ports (ex-44818 for Ethernet/IP) or a custom port
- From the **Extra Options** section, check the **Log packets that are handled by the rule** if logging is needed
- Click the **Save** button
- The **Template/Rules** page will reload with the new rules added to the table:

Rule / Templates / WAN												≡ ▮ ☰
Floating WireGuard WAN LAN												
Rules (Drag to Change Order)												
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
☐	✓ 0 / 0 B	IPv4 TCP	/	*	192.168.200.77	44818 (EIP)	*	none		ACME Machine 1 PLC Access	    	
☐	✓ 0 / 0 B	IPv4 TCP	/	*	192.168.200.78	44818 (EIP)	*	none		ACME Machine 2 PLC Access	    	
☐	✓ 0 / 0 B	IPv4 TCP	/	*	192.168.200.79	44818 (EIP)	*	none		ACME Machine 3 PLC Access	    	

Sample Set of Template Rules for Acme Template Allowing Access to 3 Rockwell PLCs

Add New Traffic Shaper Limiter

Overview

This procedure will explain how to add a new Limiter to the Anybus Defender

Procedure

1. Navigate to [Firewall / Traffic Shaper / Limiters](#)
2. From the **Limiters** tab, click the **New Limiter** button on the lower left corner of the **Limiters** table
3. An **Edit** sections will load:

Limiters

Enable

☐ Enable limiter and its children

Name

new

Bandwidth

Bandwidth

0

Bw type

Mbit/s

Schedule

none

Delete

+ Add Schedule

Mask

None

If "source" or "destination" slots is chosen a dynamic pipe with the bandwidth, delay, packet loss and queue size given above will be created for each source/destination IP address encountered, respectively. This makes it possible to easily specify bandwidth limits per host or subnet.

32

IPv4 mask bits

255.255.255.255/?

128

IPv6 mask bits

ffff:ffff:ffff:ffff:ffff:ffff:ffff:/?

Description

A description may be entered here for administrative reference (not parsed).

Queue

Queue Management Algorithm

Tail Drop

Active queue management (AQM) is the intelligent drop of network packets inside the limiter, when it becomes full or gets close to becoming full, with the goal of reducing network congestion.

No parameters for selected algorithm.

Specifies the queue management algorithm parameters.

Scheduler

Worst-case Weighted fair Queueing (default)

The scheduler manages the sequence of network packets in the limiter's queue.

No parameters for selected algorithm.

Specifies the scheduler parameters.

Queue length

Specifies the length of the limiter's queue, which the scheduler and AQM are responsible for. This field may be left empty.

ECN

☐ Enable Explicit Congestion Notification (ECN)

ECN sets a reserved TCP flag when the queue is nearing or exceeding capacity. Not all AQMs or schedulers support this.

Advanced Options

Delay (ms)

In most cases, zero (0) should specified here (or leave the field empty).

Packet Loss Rate

In most cases, zero (0) should be specified here (or leave the field empty). A value of 0.001 means one packet in 1000 gets dropped.

Bucket size (slots)

In most cases, this field should be left empty. It increases the hash size set.

Save

1. From the **Limiters** configuration, adjust these options:

- **Enable:** Selecting the checkbox will enable the limiter and its children to be configured once it is saved
- **Name:** A text entry for the Limiters name
- **Bandwidth:** Present in this section are these options:
 - **Bandwidth:** Input a value for the bandwidth that will be the limit imposed
 - **Bw Type:** Select the type of bandwidth this will be quantified. These are the available options in the dropdown:
 - **KBits/s**
 - **MBits/s**
 - **Bits/s**
 - **Schedule:** Select the desired configured schedule that this limiter will be in effect

❗ Additional Bandwidth limits based on a different schedule can be added by selecting the **Add Schedule** button

- **Mask:** Select from these options in the dropdown:
 - **None:** Select this if the limiter should affect every host or subnet
 - **Source Addresses:** Select this if the limiter only needs to affect host or subnet source addresses
 - Select the IPv4 and IPv6 mask bits that will be affected
 - **Destination Addresses:** Select this if the limiter only needs to affect host or subnet destination addresses
 - Select the IPv4 and IPv6 mask bits that will be affected
- **Description:** Optional description for the Limiter

2. Click the **Save** button when all configuration fields are complete

After the new Traffic Shaper is saved, the [Firewall / Traffic Shaper / Limiters](#) will load with the new Traffic Shaper Limiter added to the table

Add Virtual IPs

Overview

Firewall / Virtual IPs / Edit

Firewall / Virtual IPs / Edit

This procedure will explain how to add a new Virtual IP to the Anybus Defender

Some procedures, such as the [SimpleNAT Wizard](#) will create virtual IPs automatically, while others, such as the [Outboard NAT Procedure](#), will require manual virtual IP creation

Procedure

1. Navigate to [Firewall / Virtual IPs](#)
2. From the **Virtual IPs** page, click the **Add** button on the lower right corner of the **Virtual IP Address** table
3. An **Edit** page will load:

Edit Virtual IP

Type

☐ IP Alias☐ Hot Standby☐ Proxy ARP☐ Other

Interface

WAN

Address type

Single address

Address(es)

/ 128

Expansion

☐ Disable expansion of this entry into IPs on NAT lists (e.g. 192.168.1.0/24 expands to 256 entries.)

Virtual IP Password

Virtual IP Password

Enter the VHID group password.

Virtual IP Password

Confirm

VHID Group

5

Enter the VHID group that the machines will share.

Advertising frequency

1

0

BaseSkew

The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description

A description may be entered here for administrative reference (not parsed).

Save

Firewall / Virtual IPs / Edit

1. From the **Edit Virtual IP** configuration, adjust these options:
 - **Type:** Select the type of the Virtual IP. These are the selectable options:
 - **IP Alias:** Selecting this option will prompt these fields to be configured:
 - **Interface:** Select the interface from the dropdown where the Virtual IP will be applied
 - **Address(es):** Configure the desired IP and subnet mask
 - **Description:** Optional description for the Virtual IP
 - **Hot Standby:** Selecting this option will prompt these fields to be configured:
 - **Interface:** Select the interface from the dropdown where the Virtual IP will be applied
 - **Address(es):** Configure the desired IP and subnet mask
 - **Virtual IP Password:** Configure the desired **VHID Group** password for the Virtual IP
 - **VHID Group:** Configure the group ID which acts as an identifier for when multiple users are sharing the same IP. Typically set as the last octet of the respective IP address

- **Advertising Frequency:** Configure the rate at which a heartbeat advertisement is sent out. Recommended to leave the default values of **1** and **0**
- **Description:** Optional description for the Virtual IP
- **Proxy ARP:** Selecting this option will prompt these fields to be configured:
 - **Interface:** Select the interface from the dropdown where the Virtual IP will be applied
 - **Address Type:** Select from the dropdown if the Proxy ARP is a **Single Address** or **Network**
 - **Address(es):** Configure the desired IP and subnet mask for the **Single Address** or **Network** that encompasses an entire subnet
 - **Expansion:** Select the checkbox to prevent the Network option from expanding to the entire 256 IPs based on the IP and subnet that is configured
 - **Description:** Optional description for the Virtual IP
- **Other:** Selecting this option will prompt these fields to be configured:
 - **Interface:** Select the interface from the dropdown where the Virtual IP will be applied
 - **Address Type:** Select from the dropdown if the Proxy ARP is a **Single Address** or **Network**
 - **Address(es):** Configure the desired IP and subnet mask for the **Single Address** or **Network** that encompasses an entire subnet
 - **Expansion:** Select the checkbox to prevent the Network option from expanding to the entire 256 IPs based on the IP and subnet that is configured
 - **Description:** Optional description for the Virtual IP

2. Click the **Save** button when all configuration fields are complete

After the new Virtual IP is saved, the [Firewall / Virtual IPs](#) will load with the new Virtual IP added to the table

Create an OpenVPN Server

Overview

This procedure shows setting up an OpenVPN server. This procedure will focus on creating the server itself. Other procedures will explain [Adding Client Users to the OpenVPN Server](#) and [Exporting Client User Settings](#).

Procedure

1. Navigate to [VPN/OpenVPN/Wizards](#) tab
2. From the **Type of Server** dropdown, keep the selection as **Local User Access** and click the **>> Next**
3. In the **Create a New Certificate Authority (CA) Certificate** section, update these settings:

Create a New Certificate Authority (CA) Certificate	
Descriptive name	CA_ACME A name for administrative reference, to identify this certificate. This is the same as common-name field for other Certificates.
Key length	2048 bit Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com
Lifetime	3650 Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)
Country Code	US Two-letter ISO country code (e.g. US, AU, CA)
State or Province	Michigan Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
City	Ann Arbor City or other Locality name (e.g. Louisville, Indianapolis, Toronto).
Organization	ACME Co Organization name, often the Company or Group name.
E-mail	acme@acme.com E-mail address for the Certificate contact. Often the e-mail of the person generating the certificate.
Add new CA	

New CA Settings

- **Descriptive name:** Identity of this Certificate Authority (CA)

❗ It is recommended to use "CA_" as a prefix to this identity to easily identify the certificate type

- **Country Code:** Use the two-letter country code
- **State or Province:** Use the Full State or Province name
- **City:** Full name of the City or other Locality name
- **Organization:** Name of the Company or Group
- **E-mail:** E-mail address of the Certificate Contact. This is usually the person generating this CA

4. Click the **>> Add new CA** button

5. In the **Create a New Server Certificate** section, update these settings:

Create a New Server Certificate	
Descriptive name	SC_ACME A name for administrative reference, to identify this certificate. This is also known as the certificate's "Common Name."
Key length	2048 bit Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com
Lifetime	398 Lifetime in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.
Country Code	US Two-letter ISO country code (e.g. US, AU, CA)
State or Province	Michigan Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
City	Ann Arbor City or other Locality name (e.g. Louisville, Indianapolis, Toronto).
Organization	ACME Co Organization name, often the Company or Group name.
E-mail	acme@racme.com E-mail address for the Certificate contact. Often the e-mail of the person generating the certificate.
>> Create new Certificate	

New Server Certificate Settings

- **Descriptive Name:** Identity of this Server Certificate

❗ It is recommended to use "SC_" as a prefix to this identity to easily identify the certificate type

❗ The same, Country, State, City, Organization, and E-mail settings from the previous Certificate Authority settings will appear here

6. Click the >> **Create new Certificate** button

7. In the **General OpenVPN Server Information** section adjust these settings as needed:

General OpenVPN Server Information	
Interface	WAN The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocol	UDP on IPv4 only Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.
Local Port	1194 Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.
Description	A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

General OpenVPN Server Information Settings

- **Interface:** Usually set to **WAN** for incoming connections, but any [Interface](#) can be used
- **Protocol:** Should be left on **UDP on IPv4 only**
- **Local port:** For UDP, the default port is 1194. If TCP is used, the port should be changed to 443

8. In the **Tunnel Settings** section, update these settings:

Tunnel Settings	
Tunnel Network	10.0.8.0/24 This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.
Redirect Gateway	☐ Force all client generated traffic through the tunnel.
Local Network	192.168.222.0/24 This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Concurrent Connections	 Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression	Refuse any non-stub compression (Most secure)
Compression	Disable Compression [Omit Preference] Allow compression to be used with this VPN instance, which is potentially insecure.
Type-of-Service	☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication	☐ Allow communication between clients connected to this server.
Duplicate Connections	☐ Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.

New Server Certificate Settings

- **Tunnel Network:** This is the range of addresses that clients will be assigned when they connect to the server. Usually should be kept at the default 10.0.8.0/24 but can be changed if needed
- **Local Network:** This controls what routes are pushed to the clients, and in combination with firewall rules, controls what they have access to
- **Duplicate Connections:** Can be enabled to allow a user to concurrent connections, if required

9. Click the >> **Next** button

10. From the next section on Rule creations, ensure the **Firewall Rule** and **OpenVPN Rule** are enabled and click the >> **Next** button

11. From the **New User Creation** section, click on the >> **Continue** button

❗ If Users need to be added, click the [Add new User](#) instead and follow that procedure

12. Click the >> **Finish** button and the new OpenVPN Server will appear in the [List of OpenVPN Servers](#)

Create an OpenVPN User

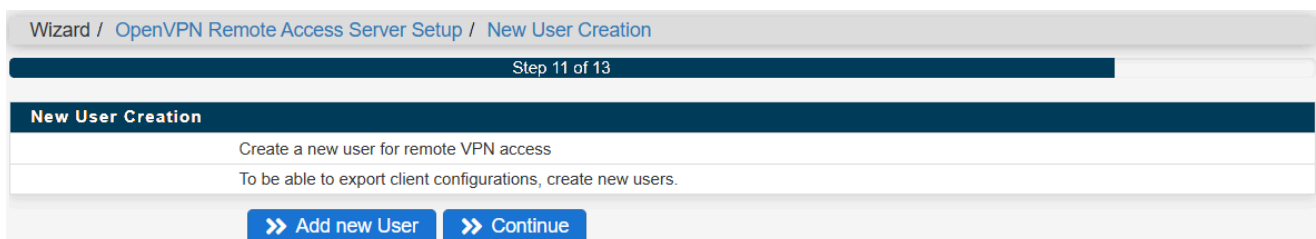
Overview

This procedure will show how to create a client user for an [OpenVPN Server](#). This procedure requires an [OpenVPN Server created via the Wizard](#) or manually

❗ OpenVPN client users can be created via the [OpenVPN Server Wizard](#) or from [Newly-created users](#) or existing users. Both procedures will be shown below

Procedure for Client Users via the OpenVPN Wizard

1. In Step 11 of the [OpenVPN Server Setup Wizard](#), click the >> **Add new User** button:



New CA Settings

2. In the **VPN new User creation** section, enter:
 - **User name:** User name for login
 - **User password:** User password for login
 - **Confirm User password:** Re-type the user password
 - **User Full Name:** The User's full name
3. Click the >> **Add User** button
4. The **New User Creation** section will reappear showing **Users to be created**

Procedure for Client Users via the User Manager

1. Navigate to [System/User Manager](#)
2. If this is a new user, click the **Add** button. For existing users, click the **Edit user** () for that user

For New Users

1. At the bottom of the **User Properties** section, enable the **Click to create a user certificate** checkbox:

Certificate

☒ Click to create a user certificate

Create Certificate for User

Descriptive name

Certificate authority

CA_Acme

Key type

RSA

2048

The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm

sha256

The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime

3650

2. The **Create Certificate for User** section will appear. Adjust these settings:

- **Descriptive name:** Name of this user certificate
 - **Certificate authority:** Set the CA that was created in the [OpenVPN Server Setup Wizard](#)
3. Complete the new user setup
4. Click the **Save** button

For Existing Users

1. In the **User Certificates** section, click the **Add** button:

User Certificates		
Name	CN	CA
+ Add		

User Certificates Section

2. From the Certification edit page, update these settings in the **Add/Sign a New Certificate** section:

- **Method:** Set dropdown to **Create an internal Certificate**
3. Update these settings in the **Internal Certificate** section:
- **Certificate authority:** Set the CA that was created in the [OpenVPN Server Setup Wizard](#)
 - **Common Name:** Enter a Common Name(CN) for this certification. This entry is required
 - **Country Code, State or Province, City, Organization** entries will auto-populate from the **Certificate authority** selected above. Adjust if required
4. Click the **Save** button

The resulting certificate will appear on the User Certificates section of the Users Edit page:

User Certificates			
Name	CN	CA	
JDoe	JDoe_UC	CA_Acme	
+ Add			

User Certificates Section Showing New Certificate

Create an OpenVPN Client Export

Overview

This procedure will show how to export the [OpenVPN Client](#) software to be used on the client's system. For clients who already have the OpenVPN Client software, config files can just be sent to add to their software configuration

❗ These procedures will require that an [OpenVPN Server](#) has already been created manually or via the [OpenVPN Server Setup Wizard](#)

A procedure for exporting an entire OpenVPN client software with the credentials included and one for just the configuration only will be included below

Procedure for Exporting the OpenVPN Client Software

1. Navigate to [VPN/OpenVPN](#)
2. Click on the **Client Export** tab
3. Scroll down to the **OpenVPN Clients** section
4. Locate the client to be used for export

❗ If the client is missing, be sure a client user certificate was added. If not, use the [Add OpenVPN Client Procedure](#) to create one

5. Depending on the operating system of the client, click on the appropriate Installer button on the right side of the client row. Options include:

- **Windows Current Installers:** Click on either the **64-bit** or **32-bit** button. This will install the **2.5.2** version of the OpenVPN client
- **Legacy Windows Installers:** Click on either the **10/2016/2019** or **7/8/8.1/2012r2** button. This will install the **2.4.11** version of the OpenVPN client

❗ Each OpenVPN client works the same. The Current version has an updated UI but may be less compatible with earlier versions of Windows (less than Windows 10)

- **Viscosity:** Click on either to **Viscosity Bundle** or **Viscosity Inline Config** button to use the [Viscosity OpenVPN Client](#) software which is compatible with Windows and MacOS (not explained in this procedure). This is paid software and will require purchasing

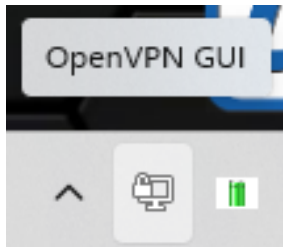
6. After a short delay, the browser will be prompted to download .exe file

❗ Most modern browsers will require extra steps to actually download an .exe file. Be sure to allow the file to be downloaded before continuing to the next step

7. Send the resulting file to the target client

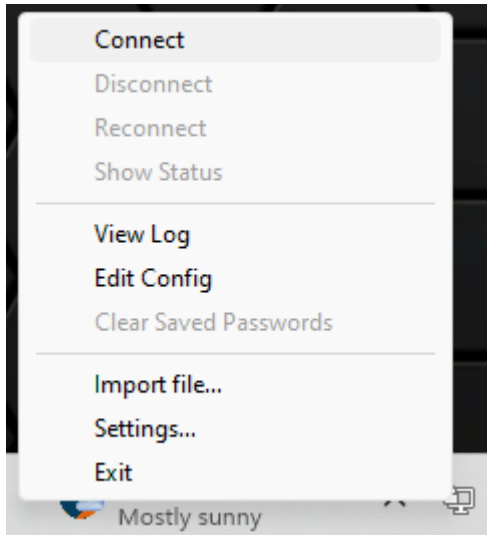
❗ Zipping or archiving the .exe file is recommended since many places will not allow direct executable files to be downloaded

8. The client just needs to run the executable file and follow the typical steps for installing most software
9. The client will also need to know the username and password for this account
10. After the installation has completed, an icon in the system tray will appear for easy access to the OpenVPN Client:



OpenVPN Taskbar Icon

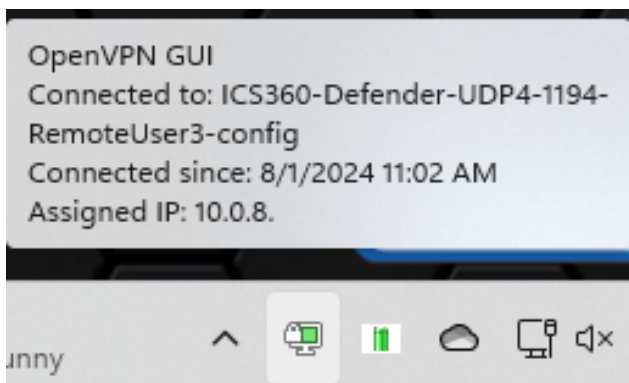
11. Right-click on the icon and select **Connect**:



Right-click Options Showing Connect

12. The client will then enter the username and password provided

13. When successfully connected, the icon should turn green (a mouseover of the icon will show connection information):



Successful Connection Indicator with Connection Info

Procedure for Exporting an OpenVPN User Configuration

❗ Use this procedure for users who already have the OpenVPN client installed

❗ If there are any security concerns about older versions of the [OpenVPN Client Software](#), use this procedure to only update the client configuration files after a update is installed

1. Navigate to [VPN/OpenVPN](#)
2. Click on the **Client Export** tab
3. Scroll down to the **OpenVPN Clients** section

4. Locate the client to be used for export

❗ If the client is missing, be sure a client user certificate was added. If not, use the [Add OpenVPN Client Procedure](#) to create one

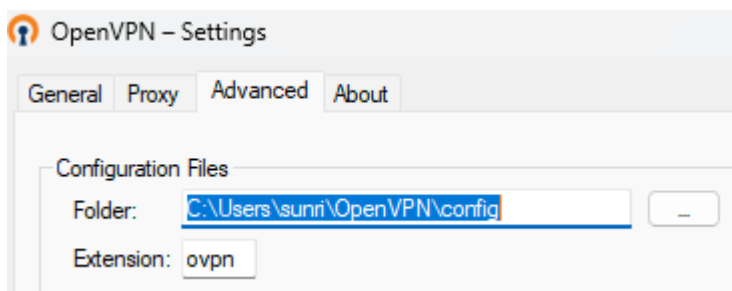
5. Click the **Archive** button from the - **Bundled Configurations:** section

6. When prompted, download the zip file

7. Send the zip file to the client user, along with the username and password

8. Instruct the client user to unzip the archive to the Config folder of the OpenVPN client, which is installed on the C:\ drive would be: **C:\Program Files\OpenVPN\config**

❗ In the OpenVPN Client settings as an option to select another location outside of the **Program Files** location (which can cause permission issues with some users). Right-click on the OpenVPN icon and select **Settings**. Choose the **Advanced** tab and use or adjust the **Configuration Files** Folder as needed:



Successful Connection Indicator with Connection Info

The client users can use that folder location to place the bundled archive

9. Client users can then right-click on the OpenVPN icon and Connect as explained in the procedure above

WireGuard Peer-to-Peer Setup

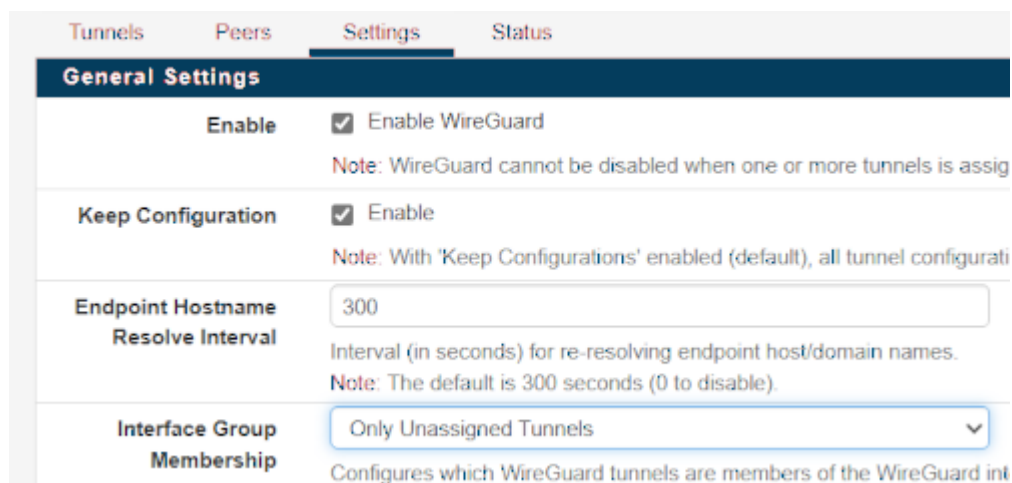
Overview

This procedure will show how to set up peer-to-peer communication in [WireGuard](#) on 2 sites using 2 Anybus Defenders

Procedure 1: Creating Site Tunnels

❶ These steps must be done on both of the Anybus Defenders involved

1. Go to the [VPN / WireGuard](#) page
2. Navigate to the [Settings Tab](#)
3. Check the **Enable WireGuard** checkbox
4. Change the **Interface Group Membership** to **Only Unassigned Tunnels**



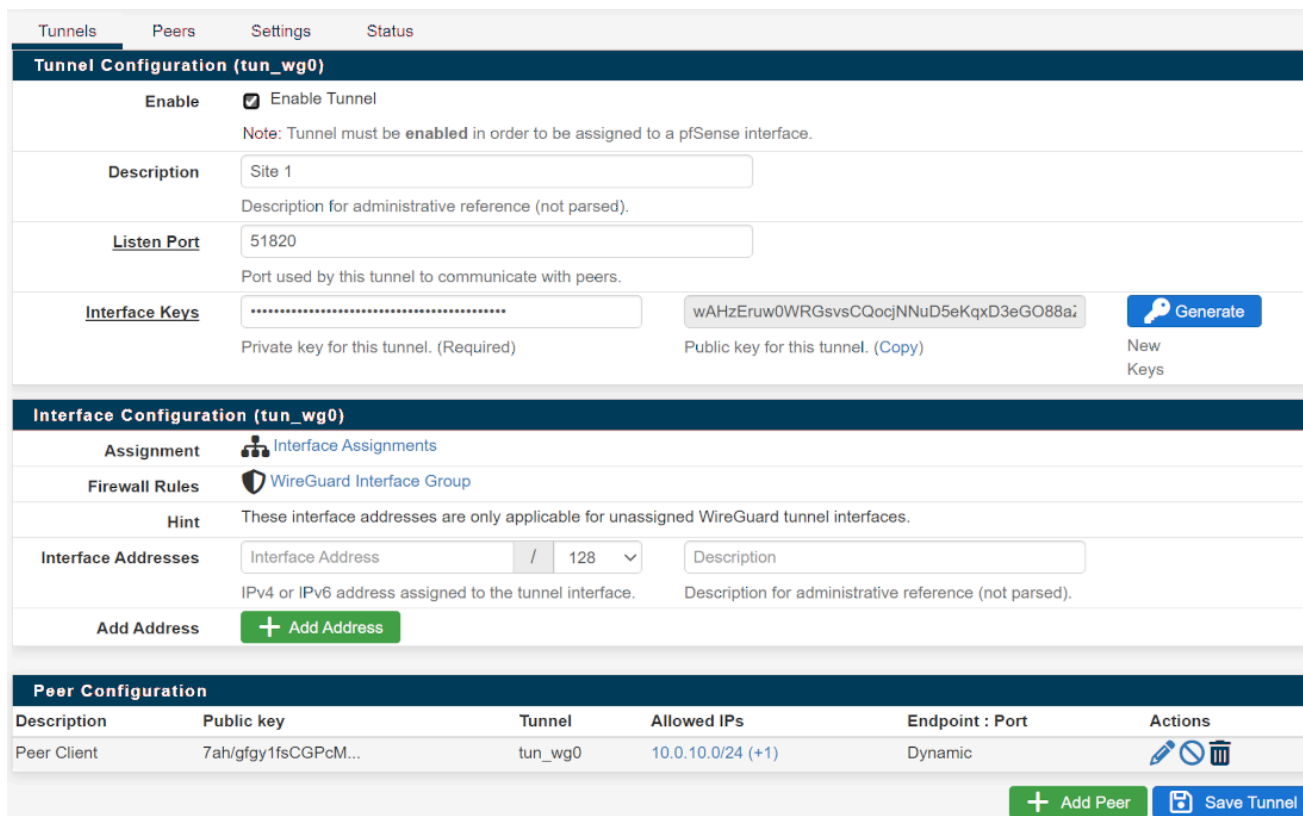
The screenshot shows the 'Settings' tab of the WireGuard configuration page. It features a 'General Settings' section with the following options:

- Enable**: A checkbox labeled 'Enable WireGuard' is checked. A note below it states: 'Note: WireGuard cannot be disabled when one or more tunnels is assigned.'
- Keep Configuration**: A checkbox labeled 'Enable' is checked. A note below it states: 'Note: With 'Keep Configurations' enabled (default), all tunnel configurations are preserved.'
- Endpoint Hostname**: A text input field containing the value '300'.
- Resolve Interval**: A text input field containing the value '300'. A note below it states: 'Interval (in seconds) for re-resolving endpoint host/domain names. Note: The default is 300 seconds (0 to disable).'
- Interface Group Membership**: A dropdown menu is set to 'Only Unassigned Tunnels'. A note below it states: 'Configures which WireGuard tunnels are members of the WireGuard interface group.'

WireGuard Settings

5. Navigate to the [Tunnels Tab](#)
6. Click the **+ Add Tunnel** button to add a new tunnel
7. On the Tunnel edit page, adjust these settings:
 - Check the **Enable Tunnel**
 - Add a **Description**
 - Set a **Listen Port** or keep it at the default of **51820**
 - Click the **Generate** button to create a public and private key. Copy and paste the public keys for each site tunnel

8. Click the  **Save Tunnel** button



Tunnel Configuration (tun_wg0)

Enable ☒ **Enable Tunnel**
Note: Tunnel must be **enabled** in order to be assigned to a pfSense interface.

Description Site 1
Description for administrative reference (not parsed).

Listen Port 51820
Port used by this tunnel to communicate with peers.

Interface Keys
Private key for this tunnel. (Required) wAHzEruw0WRGsvsCQocjNNuD5eKqxD3eGO88a... **Generate**
Public key for this tunnel. (Copy) New Keys

Interface Configuration (tun_wg0)

Assignment  [Interface Assignments](#)

Firewall Rules  [WireGuard Interface Group](#)

Hint These interface addresses are only applicable for unassigned WireGuard tunnel interfaces.

Interface Addresses Interface Address / 128 Description
IPv4 or IPv6 address assigned to the tunnel interface. Description for administrative reference (not parsed).

Add Address  **Add Address**

Peer Configuration

Description	Public key	Tunnel	Allowed IPs	Endpoint : Port	Actions
Peer Client	7ah/gfgy1fsCGPcM...	tun_wg0	10.0.10.0/24 (+1)	Dynamic	  

+ Add Peer **Save Tunnel**

Tunnel Settings

Procedure 2: Adding Peers to Each WireGuard Site

 These steps must be done on both of the Anybus Defenders involved

For Tunnel Site 1:

1. Navigate to the [VPN / Peers](#) page
2. Click the **+ Add Peer** button
3. On the Peers edit page, adjust these settings:
 - Check the **Enable Peer**
 - Set the **Tunnel** to the tunnel created above
 - Add a **Description**
 - Uncheck the **Dynamic Endpoint**
 - Set the **Endpoint** to the interface IP address for **Site 2** and the **Port** (leave blank for the default port number of **51820**)

 This will usually be an IP address on the WAN interface network

- Paste the public key for **Site 2** created above into the **Public Key** setting
- In the **Allowed IPs** section, add IP addresses for the WireGuard tunnel and the [LAN Network](#)

 The **Tunnel** IP address is internal and will be assigned to each Peer upon connection. Any unused virtual network can be assigned, such as **10.0.x.0**, as shown in the image below

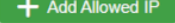
4. Click the  **Save Peer** button

Tunnels	Peers	Settings	Status
---------	-------	----------	--------

Peer Configuration

Enable	☒ Enable Peer Note: Uncheck this option to disable this peer without removing it from the list.		
Tunnel	tun_wg0 (Server)  WireGuard tunnel for this peer. (Create a New Tunnel)		
Description	Peer Client Peer description for administrative reference (not parsed).		
Dynamic Endpoint	☐ Dynamic Note: Uncheck this option to assign an endpoint address and port for this peer.		
Endpoint	177.22.54.100 Hostname, IPv4, or IPv6 address of this peer. Leave endpoint and port blank if unknown (dynamic endpoints).	Endpoint Port Port used by this peer. Leave blank for default (51820).	
Keep Alive	Keep Alive Interval (in seconds) for Keep Alive packets sent to this peer. Default is empty (disabled).		
Public Key	7ah/gfgy1fsCGPcM/19+QeDtZj/SQ8glf+8IPMD9nw=- WireGuard public key for this peer.		
Pre-shared Key	Pre-shared Key Optional pre-shared key for this tunnel. (Copy)	 Generate New Pre-shared Key	

Address Configuration

Hint	Allowed IP entries here will be transformed into proper subnet start boundaries prior to validating and saving.		
Allowed IPs	10.0.10.0 / 24 	tunnel	 Delete
	192.168.222.15 / 32 	Description	 Delete
	IPv4 or IPv6 subnet or host reachable via this peer. Description for administrative reference (not parsed).		
Add Allowed IP			

 **Save Peer**

Peer Settings

For Tunnel Site 2:

1. Repeat the same steps for **Site 2** which these updates:

- Set the **Endpoint** Interface IP address for **Site 1**
- In the **Allowed IPs** section, add the same WireGuard tunnel IP address created for **Site 1**, but the **LAN** network IP address for **Site 1**
- Paste in the **Public Key** for **Site 1** created above into the **Public Key** setting

2. Click the  **Save Peer** button

Procedure 3: Assign Interfaces to Each WireGuard Site

❗ These steps must be done on both of the Anybus Defenders involved

1. Navigate to the [Interfaces / Assignments](#) page
2. From the **Available network ports** dropdown, select the WireGuard tunnel created in the procedure above:

Interfaces / Interface Assignments

Interface Assignments Interface Groups VLANs PPPs GREs GIFs Bridges LAGGs

Interface	Network port
PLANT	igb0 (3c:ec:ef:d4:06:2c)
CONTROLS	igb1 (3c:ec:ef:d4:06:2d)

Available network ports:

tun_wg0 (tun_wg0)

Save

Delete

+ Add

Interface Assignments Settings

3. Click the **+ Add** button
4. Click on the resulting Interface created to load its configuration page
5. From the **General Configuration** section update these settings:
 - Enable the Interface
 - Add an appropriate description
 - Set the **IPv4 Configuration Type** to **Static IPv4**
6. In the **Static IPv4 Configuration** section, adjust these settings:
 - Set the **IPv4 Address** to the **10.0.x.0** network created in the Peer procedure above

❗ This address must be unique on the virtual network (**10.0.x.0** in this example) used. See the image below

- Set the subnet to /24

Interfaces / OPT1 (tun_wg0)

General Configuration

Enable	☒ Enable interface
Description	WireGuard_Site1 Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xxxxxxxxxxxx This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxx:xxxx:xxxx or leave blank.
MTU	 If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	 If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Static IPv4 Configuration

IPv4 Address	10.0.10.1	/ 24
IPv4 Upstream gateway	None	+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking [here](#).

Interface Settings

- Click the **+ Add a new gateway** button
- From the **New IPv4 Gateway** dialog window, fill in the **Gateway IPv4** address with the IP Address that will be assigned to the other WireGuard site:

New IPv4 Gateway

Default	☐ Default gateway
Gateway name	OPT1GW
Gateway IPv4	10.0.10.2
Description	

[+ Add](#) [Cancel](#)

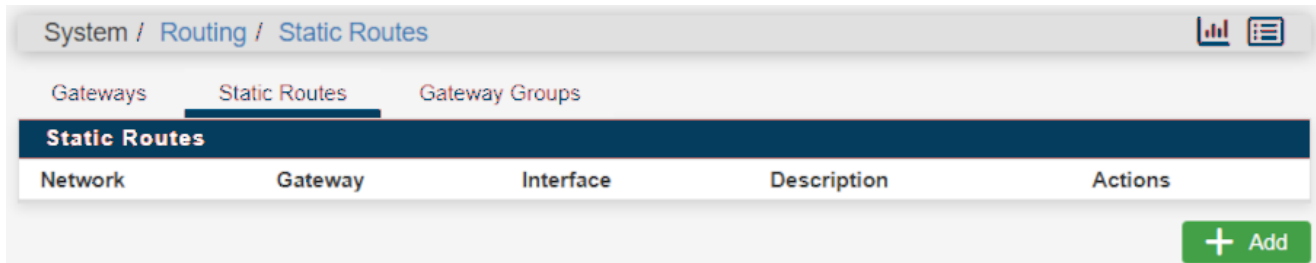
new Gateway Settings

- Click the **+ Add** button to create the new Gateway
- Click the **Save Peer** button to save the interface settings
- Repeat these steps on the other WireGuard site adjusting these settings:
 - Set the Static **IPv4 Address** to the IP address of the other site
 - Add a new Gateway using the other site's tunnel address

Procedure 4: Create Static Routes on Each WireGuard Site

❗ These steps must be done on both of the Anybus Defenders involved

1. Navigate to [System / Routing](#) and click the **Static Routes** tab:



Static Routes Tab

2. Click the **+ Add** button to create the new Static Route

3. On the **Static Route Edit** page, adjust the settings:

- **Destination network:** The **LAN** network of the other WireGuard site
- **Gateway:** The Gateway created in the previous procedure

The screenshot shows the 'Edit Route Entry' form. The breadcrumb path is 'System / Routing / Static Routes / Edit'. The form has several fields: 'Destination network' with the value '192.168.222.0' and a dropdown for '24'; 'Gateway' with a dropdown showing 'PLANT_DHCP - 192.168.68.1'; 'Disabled' with a checkbox and the text 'Disable this static route'; and 'Description' with a text area. At the bottom, there is a blue 'Save' button.

New Static Route Page

4. Click the **Save** button to save the new Static Route

5. Repeat these steps for the other WireGuard site adjusting these settings:

- **Destination network:** The **LAN** network of the other WireGuard site
- **Gateway:** The Gateway created in the previous procedure

Procedure complete and each Anybus Defender should be able to communicate with each other

Add DHCP Server

Overview

This procedure will explain how to enable and configure a new DHCP Server on WAN or LAN of the Anybus Defender



Procedure

1. Navigate to [Services / DHCP Server / LAN or /WAN](#)

i The DHCP Server configuration is virtually the same on WAN or LAN. The example below will show a LAN DHCP Server configuration

2. Click on either the **WAN**, **LAN**, or any other configured interface tab to configure the appropriate interface
3. Adjust these settings for the **General Options** section:

General Options	
Enable	☐ Enable DHCP server on LAN interface
BOOTP	☐ Ignore BOOTP queries
Deny unknown clients	Allow all clients When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.
Ignore denied clients	☐ Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore client identifiers	☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Subnet	192.168.200.0
Subnet mask	255.255.255.0
Available range	192.168.200.1 - 192.168.200.254
Range	192.168.200.11 From To

General Options

- **Enable:** Checkbox to enable the DHCP instance
- **BOOTP:** Checkbox to ignore any BOOTP requests
- **Deny unknown clients:** Dropdown to handle connections from unknown clients. Options are:
 - **Allow all clients:** Any DHCP client will get an IP address within this interface
 - **Allow known clients from any interface:** Any DHCP client with a MAC address listed on any interface will get an IP address
 - **Allow known clients from only this interface:** Only MAC addresses configured in the [Static Mapping for this Interface](#) will get an IP address

- **Ignore denied clients:** Checkbox to silently drop packets that do not match the criteria instead of returning a rejection packet to the client

❗ This option is not compatible with failover and cannot be enabled when Failover Peer IP address is configured

- **Ignore client identifiers:** Checkbox to ignore the Unique Identifier (UID) in a DHCP request

❗ This may be useful when a client can dual boot using different client identifiers from the same hardware MAC address. This violates the official DHCP specification, however

- **Subnet:** Read-only display of the interface's subnet
- **Subnet mask:** Read-only display of the interface's subnet mask
- **Available range:** Read-only display of the current range of IP addresses used to assign to clients
- **Range: From** and **To** text entries to set the range of IP addresses used by connecting clients

4. Adjust these settings for the **Additional Pools** section:

Additional Pools			
Add	+ Add pool		
If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.			
Pool Start	Pool End	Description	Actions

- **Add Post** Button to allow adding a pool of addresses inside this subnet but outside of the above range

5. Adjust these settings for the **Servers** section:

Servers	
WINS servers	WINS Server 1
	WINS Server 2
DNS servers	DNS Server 1
	DNS Server 2
	DNS Server 3
	DNS Server 4
Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.	

- **WINS servers:** Two text entries to add custom WINS servers
- **DNS servers:** Four text entries to add custom DNS servers

❗ If DNS server entries are left blank, the system's default DNS servers are used

6. Adjust these settings for the **OMAPI** section:

OMAPI	
OMAPI Port	OMAPI Port Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable. Only the first OMAPI configuration is used.
OMAPI Key	OMAPI Key ☐ Generate New Key Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint. Generate a new key based on the selected algorithm.
Key Algorithm	HMAC-SHA256 (current bind9 default) Set the algorithm that OMAPI key will use.

- **OMAPI Port:** Text entry of the Port that OMAPI will listen on. If left blank, OMAPI will be disabled

❗ The default port is 7911

- **OMAPI Key:** Text entry for the key that matches the **Key Algorithm** selected below

- **Generate New Key:** Checkbox to allow a new OMAPI Key to be generated using the **Key Algorithm** selected below
 - **Key Algorithm:** Dropdown to select the algorithm used by the **OMAPI Key** above. Options are:
 - HMAC-MD5 (legacy default)
 - HMAC-SHA1
 - HMAC-SHA224
 - HMAC-SHA256 (current bind9 default)
 - HMAC-SHA384
 - HMAC-SHA512 (most secure)
7. Adjust these **Other Options** as needed:

Other Options	
Gateway	 The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.
Domain name	 The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.
Domain search list	 The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.
Default lease time	 This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum lease time	 This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Failover peer IP	 Leave blank to disable. Enter the interface IP address of the other machine. Machines must be using Hot Standby. Interface's advskew determines whether the DHCPd process is Primary or Secondary. Ensure one machine's advskew < 20 (and the other is > 20).
Static ARP	☐ Enable Static ARP entries This option persists even if DHCP server is disabled. Only the machines listed below will be able to communicate with the firewall on this interface.
Time format change	☐ Change DHCP display lease time from UTC to local time By default DHCP leases are displayed in UTC time. By checking this box DHCP lease time will be displayed in local time and set to the time zone selected. This will be used for all DHCP interfaces lease time.
Statistics graphs	☐ Enable RRD statistics graphs Enable this to add DHCP leases statistics to the RRD graphs. Disabled by default.
Ping check	☐ Disable ping check When enabled dhcpd sends a ping to the address being assigned, and if no response has been heard, it assigns the address. Enabled by default.
Dynamic DNS	Display Advanced
MAC address control	Display Advanced
NTP	Display Advanced
TFTP	Display Advanced
LDAP	Display Advanced
Network Booting	Display Advanced
Additional BOOTP/DHCP Options	Display Advanced

i If these options are needed, check the [DHCP Server Service Settings](#) for more information

8. Add any [DHCP Static Mappings](#) as needed

At the bottom of all sections is a **Save** button to make any pending changes permanent

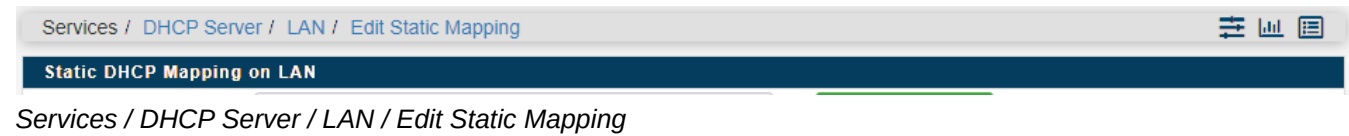
Add DHCP Static Map

Overview

This procedure will explain how to add and configure new DHCP Static mappings on WAN or LAN to the Anybus Defender

❗ The [Procedure for DHCP Server Setup](#) will explain how to enable and configure the DHCP Server

From the bottom of the [DHCP Server Page](#) for the WAN or LAN tab page, are the **DHCP Static Mappings for this Interface** section:



Procedure

1. Navigate to [Services / DHCP Server / LAN or /WAN](#)

❗ The DHCP Server configuration is virtually the same on WAN or LAN. The example below will show a LAN DHCP Server configuration

- 2. From the **DHCP Static Mappings for this Interface** table, click the **Add** button on the lower right of that table
- 3. A **Static Mappings on LAN** or **WAN** page will load depending on which interface is being configured:

Static DHCP Mapping on LAN	
MAC Address	xxxxxxxxxx Copy My MAC MAC address (6 hex octets separated by colons)
Client Identifier	
IP Address	If an IPv4 address is entered, the address must be outside of the pool. If no IPv4 address is given, one will be dynamically allocated from the pool. The same IP address may be assigned to multiple mappings.
Hostname	Name of the host, without domain part.
Description	A description may be entered here for administrative reference (not parsed).
ARP Table Static Entry	☐ Create an ARP Table Static Entry for this MAC & IP Address pair.
WINS Servers	WINS 1 WINS 2
DNS Servers	DNS 1 DNS 2 DNS 3 DNS 4 Note: leave blank to use the system default DNS servers - this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the General page.
Gateway	The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network.
Domain name	The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.
Domain search list	The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.
Default lease time (Seconds)	Used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum lease time (Seconds)	This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.

Static DHCP Mapping on WAN/LAN of the Services / DHCP Server / LAN / Edit Static Mapping Page

1. From there, these settings can be adjusted:

- **MAC Address:** Text entry for the MAC (Media Access Control) address of the DHCP client assigned to this mapping

i The **Copy My MAC** button can be used to easily copy the MAC address to the computer's clipboard

- **Client Identifier:** Text entry for the client ID of the DHCP client assigned to this reservation
- **IP Address:** Text entry for the IP address that will be assigned to this device when it requests a reservation

i For IPV4, the IP address must be outside the pool allocation configured in the [DHCP Server Setup](#). If this is left blank, it will be dynamically allocated by the pool

- **Hostname:** Text entry for the hostname of the DHCP client assigned to this reservation
- **Description:** Optional description of this reservation for administrative references
- **ARP Table Static Entry:** Checkbox to create an ARP Table Static Entry table for this MAC and IP address pair when this device is connected
- **WINS Servers:** These two text fields will override the [WINS Settings in the DHCP Server](#) for this DHCP client
- **DNS Servers:** These four text fields will override the [DNS Settings in the DHCP Server](#) for this DHCP client
- **Gateway:** Text entry for the Gateway to be provided to the DHCP client. Typically, this is the IP address of the Anybus Defender on the same interface as the DHCP server
- **Domain Name:** Text entry for an alternative domain name to be provided to the DHCP client. If left blank, the domain name of this system will be used

- **Domain Search List:** Text entry for domain search lists to be provided to the DHCP client. Use the semicolon (;) character as a separator for each domain name on the list
- **Default Lease Time (Seconds):** Text entry to specify a specific expiration time for this DHCP client if it does not ask for it. The default is 720 seconds
- **Maximum Lease Time (Seconds):** Text entry to specify the maximum lease time for this DHCP client. The default maximum lease time is 86400 seconds

Dynamic DNS	Hide Advanced
DHCP Registration	☐ Enable registration of DHCP client names in DNS.
DDNS Hostname	☐ Make dynamic DNS registered hostname the same as Hostname above.
DDNS Domain	 Leave blank to disable dynamic DNS registration. Enter the dynamic DNS domain which will be used to register client names in the DNS server. Only the first defined set of option for each domain will be honored if it is used for multiple interfaces/entries.
Primary DDNS address	 Primary domain name server IP address for the dynamic domain name.
Secondary DDNS address	 Secondary domain name server IP address for the dynamic domain name.
DDNS Domain Key name	 Enter the dynamic DNS domain key name which will be used to register client names in the DNS server.
Key algorithm	HMAC-MD5 (legacy default) ▼
DDNS Domain Key secret	 Enter the dynamic DNS domain key secret which will be used to register client names in the DNS server.

- **Dynamic DNS:** A button to either show or hide the **Dynamic DNS** advanced options
 - **DHCP Registration:** Checkbox to enable registration of DHCP client names in DNS
 - **DDNS Hostname:** Checkbox that makes dynamic DNS registered hostname the same as the Hostname above
 - **DDNS Domain:** Text entry to register client names in the DNS server. If left blank, dynamic DNS registration will be disabled
 - **Primary DDNS Address:** Text entry to set the main domain name or subdomain that is dynamically updated to reflect the changing IP address of a device or server
 - **Secondary DDNS Address:** Text entry to set the secondary DDNS IP address
 - **DDNS Domain Key Name:** text entry for a unique identifier used in the configuration and authentication processes when setting up and updating DDNS services
 - **Key Algorithm:** Dropdown box to select a particular HMAC-SHA cryptographic algorithm. Options are:
 - HMAC-MD5 (legacy default)
 - HMAC-SHA1
 - HMAC-SHA224
 - HMAC-SHA256(current bind9 default)
 - HMAC-SHA384
 - HMAC-SHA512(most secure)
 - **DDNS Domain Key Secret:** text entry for the dynamic DNS domain key name to securely authenticate and authorize updates to the DNS records associated with a dynamic IP address

NTP servers	Hide Advanced
NTP Servers	NTP 1 NTP 2 NTP 3
TFTP servers	Hide Advanced
TFTP Server	 Leave blank to disable. Enter a full hostname or IP for the TFTP server.
LDAP	Hide Advanced
LDAP Server URI	 Leave blank to disable. Enter a full URI for the LDAP server in the form ldap://ldap.example.com/dc=example,dc=com

- **NTP Servers:** A button to either show or hide the **NTP Servers** advanced options
 - **NTP Servers:** Text entry to enter the IP addresses of the NTP Servers 1-3
- **TFTP Servers:** A button to either show or hide the **TFTP Servers**
 - **TFTP Servers:** Text entry to enable and configure a TFTP server. If left blank, the TFTP Server will be disabled
- **LDAP:** A button to either show or hide the **LDAP** advanced options
 - **LDAP Server URI:** Text entry to enable and configure a full Uniform Resource Identifier (URI) for an LDAP server

❗ Example URI path: **ldap://ldap.example.com/dc=example,dc=com**

If left blank, the LDAP Server connection will be disabled

Network Booting	
Enable	☐ Enables network booting
Next Server	 Enter the IP address of the next server
Default BIOS file name	
UEFI 32 bit file name	
UEFI 64 bit file name	
ARM 32 bit file name	
ARM 64 bit file name	 Both a filename and a boot server must be configured for this to work! All five filenames and a configured boot server are necessary for UEFI & ARM to work!
Root path	 string-format: iscsi:{servername}:{protocol}:{port}:{LUN}:targetname

- **Network Booting:** A button to either show or hide the **Network Booting** advanced options
 - **Enable:** Checkbox to enable network booting
 - **Next Server:** Text entry to enter the IP Address of the Next server
 - **Default BIOS File Name:** Text entry for the default BIOS file name which will often end with .ROM, .BIN, or .WPH extensions
 - **UEFI 32 Bit File Name:** Text entry for a 32-bit UEFI bootloader, which is typically the default file name **BOOTIA32.EFI**
 - **UEFI 64 Bit File Name:** Text entry for a 64-bit UEFI bootloader, which is typically the default file name **BOOTX64.EFI**
 - **ARM 32 Bit File Name:** Text entry for an ARM 32-bit UEFI bootloader, which is typically the default file name **BOOTARM.EFI**
 - **ARM 64 Bit File Name:** Text entry for a 64-bit UEFI bootloader, which is typically the default file name **BOOTAA64.EFI**
 - **Root Path:** Text entry for the base or starting point for network configuration and organization, including static DHCP mappings

Additional BOOTP/DHCP Options

Hide Advanced

Additional BOOTP/DHCP Options

Enter the DHCP option number and the value for each item to include in the DHCP lease information. For a list of available options please visit this URL.

Option		Text	
	Number	Type	Value

Add

+ Add

◦ **Additional BOOTP/DHCP Options:** A button to either show or hide the **Additional BOOTP/DHCP** advanced options

- **Option:** These are additional parameters that can be included in the DHCP or BOOTP messages to provide additional configuration information to the client devices
 - **Number:** Text entry for the option number for the DHCP lease
 - **Type:** Dropdown to set the option type such as text, string, boolean, integer type, or IP address
 - **Value:** Text entry for the specific data associated with a particular option
- **Add:** The **Add** button allows for the additional options to be added to the Additional BOOTP/DHCP Table

Below the **Static DHCP Mapping on WAN/LAN** and **Additional BOOTP/DHCP Options** table is a **Save** button to make any pending changes permanent

Add IGMP Proxy

Overview

This section is used to manage multicast traffic within a network. It allows multicast traffic to be distributed from one segment of a network to another, facilitating the efficient use of bandwidth for applications that deliver data to multiple recipients simultaneously

Services / IGMP Proxy / Edit

IGMP Proxy Edit

IGMP Proxy Edit

IGMP Proxy Edit	
Interface	WAN
Description	A description may be entered here for administrative reference (not parsed).
Type	Upstream Interface The upstream network interface is the outgoing interface which is responsible for communicating to available multicast data sources. There can only be one upstream interface. Downstream network interfaces are the distribution interfaces to the destination networks, where multicast clients can join groups and receive multicast data. One or more downstream interfaces must be configured.
Threshold	Defines the TTL threshold for the network interface. Packets with a lower TTL than the threshold value will be ignored. This setting is optional, and by default the threshold is 1.
Networks	/ 32 Delete Network/CIDR
Add network	+ Add network

- Interface:** A dropdown to select either WAN or LAN network type
- Description:** A text field to specify a descriptive word or phrase to be used as an administrative reference
- Type:** A dropdown to select either upstream interface to downstream interface
- Threshold:** A text field to define the TTL threshold value for the network interface. Packets with a lower TTL than the threshold will be ignored. This setting is optional, and by default the threshold is 1.
- Network:** A text field to declare the IP address and a dropdown number field to declare the prefix size
- Add Network:** A button to add a new line to define another Network IP address and its prefix size

Below the **IGMP Proxy Edit** table there is a **Save** button to make any pending changes permanent

Packet Capture Procedures Overview

Overview

Packet captures can be done in 2 ways with the procedure links:

- [Scheduled Packet Capture](#)
- [Instant Packet Capture](#)

Add Scheduled Captures

Overview

Diagnostics / Packet Capture / Edit

Diagnostics / Packet Capture / Edit

This procedure will explain how to add a new Scheduled Packet Capture to the Anybus Defender

Prerequisite for Scheduled Packets

❗ Firewall schedules must be created before a scheduled packet capture can be performed

This procedure will show how to create a schedule:

1. Navigate to [Firewall/Schedules](#)
2. Click the **+ Add** button
3. From the Schedules/Edit page, adjust these settings:
 - **Schedule Name:** Name of the schedule (this will be used in the actual **Scheduled Packet Capture** procedure below)
 - **Description:** Optional description text
 - **Month:** Dropdown to select the Month and Year in a **MonthName_YY** format
 - **Date:** Calendar that allows days to be selected
 - **Time:** Series of dropdowns to select the hour and minute to start and stop the schedule execution
 - **Time range description:** optional description for the time range
4. Click the **+ Add Time** to add the current settings to a **Configured Ranges** section that appears below the **Schedule Information** section:

description

A description may be entered here for administrative reference (not parsed).

+ Add Time

Clear selection

Configured Ranges

October 1, October 9,	3:00	4:59		Delete
Day(s)	Start time	Stop time	Description	

Save

Configured Ranges Section

5. Repeat steps **3** and **4** to create multiple **Configured Ranges** as needed
6. Click the **Save** button to save all the scheduled ranges created

Scheduled Packet Capture Procedure

1. Navigate to [Diagnostics / Packet Capture](#)
2. From the **Package Capture** page, click the **Add New Scheduled Capture** button on the lower right corner of the **Scheduled Captures** table

3. An **Edit** page will load:

Packet Capture Options	
Disable	☐ Disable Scheduled Capture Disable this scheduled capture for now
Interface	WAN Select the interface on which to capture traffic.
Promiscuous	☐ Enable promiscuous mode The packet capture will be performed using promiscuous mode. Note: Some network adapters do not support or work well in promiscuous mode. More: Packet capture
Address Family	Any Select the type of traffic to be captured.
Protocol	Any Select the protocol to capture, or "Any".
Host Address	This value is either the Source or Destination IP address or subnet in CIDR notation. The packet capture will look for this address in either field. Matching can be negated by preceding the value with "!". Multiple IP addresses or CIDR subnets may be specified. Comma (",") separated values perform a boolean "AND". Separating with a pipe (" ") performs a boolean "OR". If this field is left blank, all packets on the specified interface will be captured.
Port	The port can be either the source or destination port. The packet capture will look for this port in either field. Leave blank if not filtering by port.
Packet Length	0 The Packet length is the number of bytes of each packet that will be captured. Default value is 0, which will capture the entire frame regardless of its size.
Count	This is the number of packets the packet capture will grab. Default value is 1000. Enter 0 (zero) for no count limit.
Schedule	none Leave as 'none' to leave the rule enabled all the time.
Save	

Diagnostics / Packet Capture / Edit

4. From the **Packet Capture** configuration, adjust these options:

- **Interface:** Select from a drop-down which interface traffic should be captured on
- **Address Family:** Set to **IPv4 Only** (IPv6 addressing is also allowed)
- **Protocol:** Use the drop-down to select **Any**, **TCP** or **UDP** or other specialized protocols as needed

❗ Each protocol also has an **Exclude <protocol>** that captures all traffic except that protocol

- **Host Address:** If only one IP address (or multiple as described in its help text) is needed for capture, enter it here. Otherwise, leave it blank to capture all IP addresses from the selected interfaces
- **Port:** Enter into the text box to filter for a specific port. Leave blank to not filter for a specific port
- **Packet Length:** Specify the maximum length in bytes packets will be captured. Any bytes past this will be ignored. If left as zero, every packet size will be captured
- **Count:** The default value of 1000 packets should be increased if capture traffic will be busy or lengthy
- **Schedule:** Select from a drop-down the scheduled times the capture will commence

❗ This is a required field. If this shows **none**, refer to the **Prerequisite for Scheduled Packets** procedure above for creating schedules

5. Click the **Save** button when all configuration fields are complete

After the new Scheduled Capture is saved, the [Diagnostics / Packet Capture](#) will load with the new Scheduled Capture added to the table

Start Instant Capture

Overview

This procedure will explain how to start an Instant Packet Capture on the Anybus Defender

Procedure

1. Navigate to [Diagnostics / Packet Capture](#)
2. From the **Package Capture** page, click the **Start Instant Capture** button on the lower right corner of the **Instant Capture** table
3. A **Capture** page will load:

Packet Capture Options

Interface

WAN

Select the interface on which to capture traffic.

Promiscuous

☐ Enable promiscuous mode

The packet capture will be performed using promiscuous mode.
Note: Some network adapters do not support or work well in promiscuous mode.
More: [Packet capture](#)

Address Family

Any

Select the type of traffic to be captured.

Protocol

Any

Select the protocol to capture, or "Any".

Host Address

This value is either the Source or Destination IP address or subnet in CIDR notation. The packet capture will look for this address in either field. Matching can be negated by preceding the value with "!". Multiple IP addresses or CIDR subnets may be specified. Comma (",") separated values perform a boolean "AND". Separating with a pipe ("|") performs a boolean "OR".
If this field is left blank, all packets on the specified interface will be captured.

Port

The port can be either the source or destination port. The packet capture will look for this port in either field. Leave blank if not filtering by port.

Packet Length

0

The Packet length is the number of bytes of each packet that will be captured. Default value is 0, which will capture the entire frame regardless of its size.

Count

1000

This is the number of packets the packet capture will grab. Default value is 1000.
Enter 0 (zero) for no count limit.

Level of detail

Normal

This is the level of detail that will be displayed after hitting "Stop" when the packets have been captured.
This option does not affect the level of detail when downloading the packet capture.

Reverse DNS Lookup

☐ Do reverse DNS lookup

The packet capture will perform a reverse DNS lookup associated with all IP addresses.
This option can cause delays for large packet captures.

Last capture

July 12th, 2024 3:15:48 pm.

Start

Analyze Capture

Download Capture

4. From the **Packet Capture** options, adjust these options:
 - **Interface:** Select from a drop-down which interface traffic should be captured on

- **Promiscuous:** Select the checkbox to enable this option. When enabled it captures all traffic on the local network even if the traffic is not intended for the destination IP address
- **Address Family:** Set to **IPv4 Only** (IPv6 addressing is also allowed)
- **Protocol:** Use the drop-down to select **Any**, **TCP** or **UDP** or other specialized protocols as needed

i Each protocol also has an **Exclude <protocol>** that captures all traffic except that protocol

- **Host Address:** If only one IP address (or multiple as described in its help text) is needed for capture, enter it here. Otherwise, leave it blank to capture all IP addresses from the selected interfaces
- **Port:** Enter into the text box to filter for a specific port. Leave blank to not filter for a specific port
- **Packet Length:** Specify the maximum length in bytes packets will be captured. Any bytes past this will be ignored. If left as zero, every packet size will be captured
- **Count:** The default value of 1000 packets should be increased if capture traffic will be busy or lengthy

5. Click the **Start** button when all configuration fields are complete

If there has been a previous packet capture, there will be additional buttons available:

- **Analyze Capture:** Analyzes the capture for Industrial Protocols and auto-generate rules. More information can be found at [Firewall / Industrial Protocols / Analysis](#)
- **Download Capture:** Downloads the most recent packet capture to the host system accessing the Anybus Defender

USB Method

Overview

This procedure will show how to do a system update on the Anybus Defender using the USB port and a USB storage media device

❗ It is highly recommended that the running configuration be backed up. Anybus Defender should flash and restart with the currently running configuration, but care should be taken to avoid unexpected issues with a backup

❗ It is recommended the existing version is noted before doing this procedure to be sure the new update is a newer version. The [Dashboard System Information Widget](#) will display the **Version** information:

System Information		  
Name	Anybus-Defender-ST02.localdomain	
User	admin@192.168.200.222 (Local Database)	
System	VMware Virtual Machine Serial: VMware-56 4d b4 c8 ea dc 2d 22-b9 d0 72 5f 11 e1 3b 3f Anybus Defender Device ID: 564db4c8-eadc-2d22-b9d0-725f11e13b3f	
License	PRO	
Version	2.5.2-RELEASE-2025042412 (amd64) built on Thu Apr 24 12:10:18 EDT 2025	

Dashboard System Information Showing Version Information

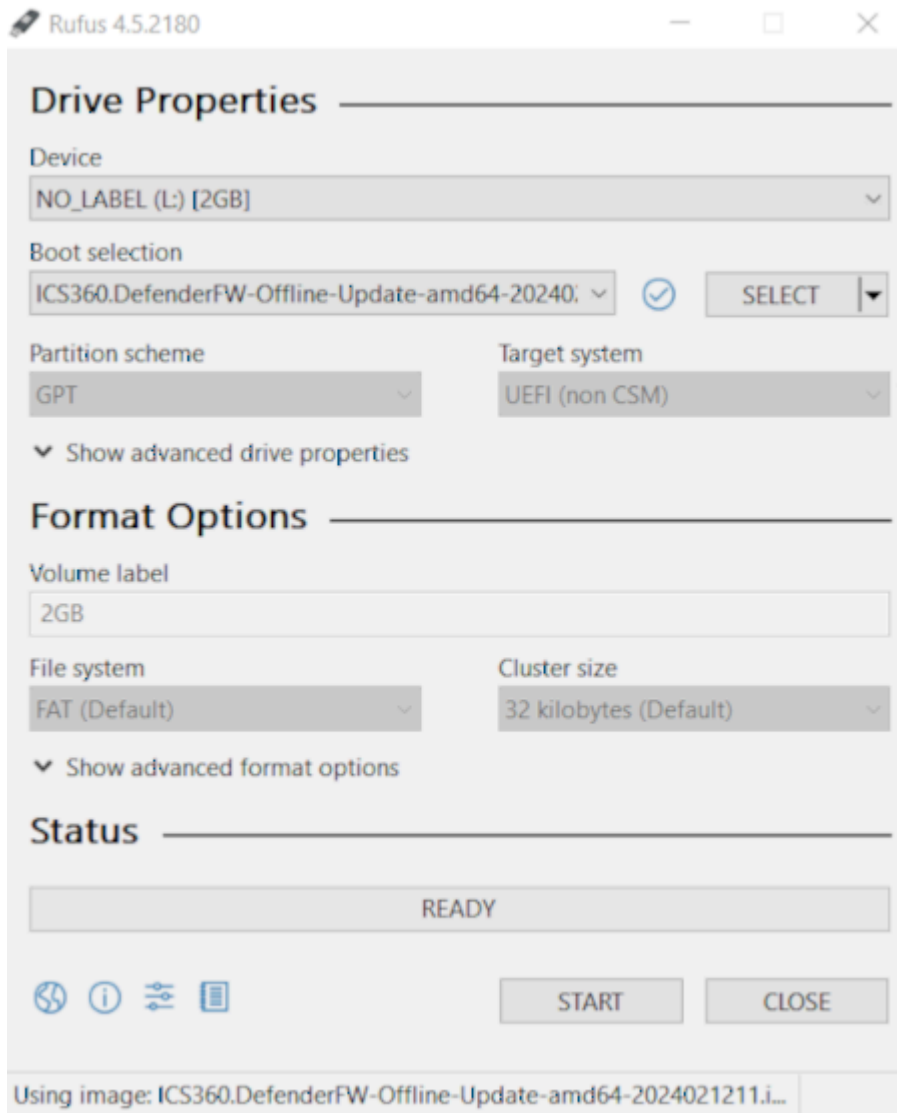
Prerequisites

USB updates are performed using USB storage media flashed with firmware from HMS. A drive can also be created using the **Creating a System Update USB Drive** section below

Creating a System Update USB Drive

A USB drive can be created by using a free disk utility named [Rufus](#). With this, only the system update image file is needed to create a system update drive

After opening Rufus, select the proper USB drive from the **Device** dropdown. Load the proper **.img** file from the **SELECT** button file picker:



Rufus with Drive and Image File Loaded

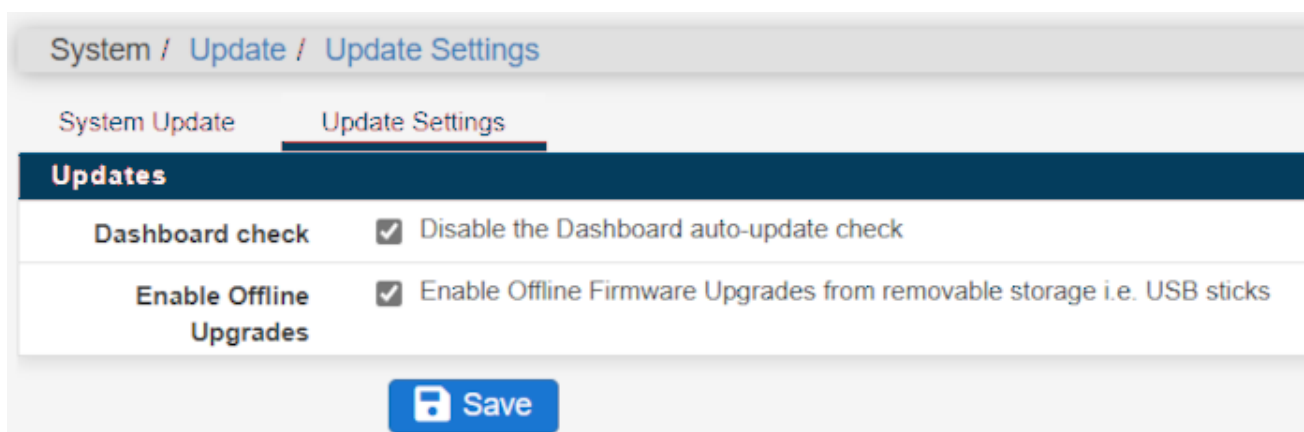
Click the **START** button and wait for it to finish

After completion, the USB storage media can be removed from the PC and the procedure below can be used

Procedure

1. Insert the USB into any USB port of the Anybus Defender
2. Navigate to [System / Update/ Update Settings](#)

3. From the **Update Settings** tab, Check the **Enable Offline Upgrades** option:



System / Update / Update Settings

System Update **Update Settings**

Updates

Dashboard check ☒ Disable the Dashboard auto-update check

Enable Offline Upgrades ☒ Enable Offline Firmware Upgrades from removable storage i.e. USB sticks

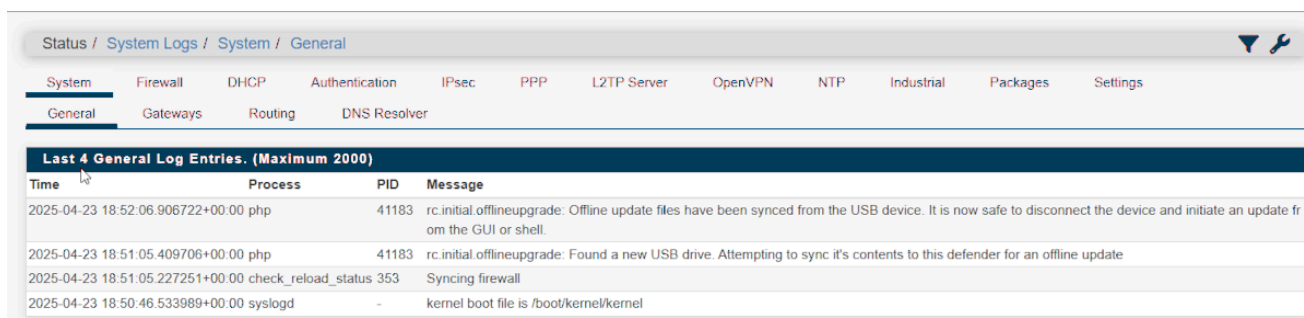
 Save

Enable Offline Upgrades Checked in Update Settings

❗ At this point, the USB storage media will be accessed and checked. Once confirmed that the update is from HMS and safe, the necessary files will be transferred to the Anybus Defender

4. Click the **Save** button

5. Navigate to the [Status / System Logs / System General Log](#) page and verify the USB device entries appear:



Status / System Logs / System / General

System Firewall DHCP Authentication IPsec PPP L2TP Server OpenVPN NTP Industrial Packages Settings

General Gateways Routing DNS Resolver

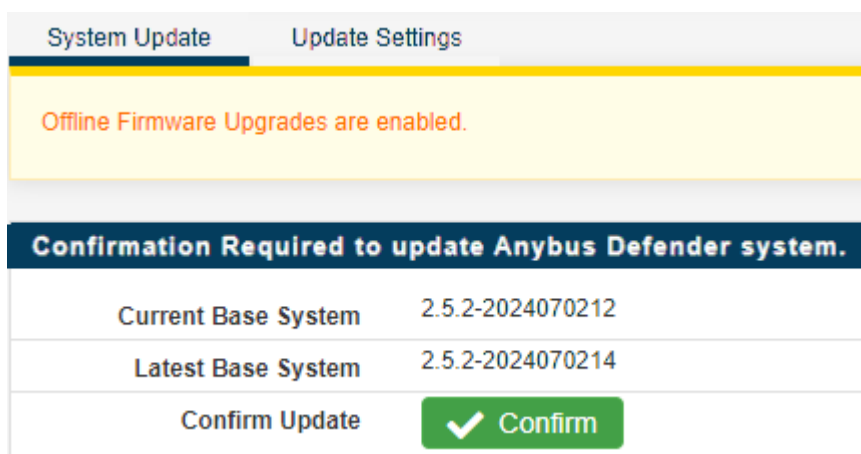
Last 4 General Log Entries. (Maximum 2000)

Time	Process	PID	Message
2025-04-23 18:52:06.906722+00:00	php	41183	rc.initial.offlineupgrade: Offline update files have been synced from the USB device. It is now safe to disconnect the device and initiate an update from the GUI or shell.
2025-04-23 18:51:05.409706+00:00	php	41183	rc.initial.offlineupgrade: Found a new USB drive. Attempting to sync it's contents to this defender for an offline update
2025-04-23 18:51:05.227251+00:00	check_reload_status	353	Syncing firewall
2025-04-23 18:50:46.533989+00:00	syslogd	-	kernel boot file is /boot/kernel/kernel

Status / System Log Showing Completed USB File Sync

❗ Be sure the log entry `Offline updates have been synced from the USB device...` entry appears before removing the USB storage device (it is recommended to keep the device plugged in until the update is complete). Refresh the page periodically if needed

6. Navigate back to the **System Update** page. The **Current Base System** should show the current system version while the **Latest Base System** should show the version on the USB storage media:



System Update Update Settings

Offline Firmware Upgrades are enabled.

Confirmation Required to update Anybus Defender system.

Current Base System	2.5.2-2024070212
Latest Base System	2.5.2-2024070214

Confirm Update  Confirm

System Update Tab with Newer Latest Base System

7. Click the **Confirm** button to update the Anybus Defender. The unit will update and then reboot

❗ As noted during the update, be sure NOT to leave or refresh the current web page

8. Verify the Anybus Defender successfully updated by referencing the [Dashboard System Information Widget](#) will then show the updated system version

Online Portal Method

Overview

This procedure will show how to do a system update on the Anybus Defender using the online update portal. The system will attempt to reach the update portal and check the unit's version against the version available on the portal

❗ Online updates require a support and maintenance agreement

❗ It is highly recommended that the running configuration is backed up prior to updating the unit. Anybus Defender should flash and restart with the currently running configuration, but care should be taken to avoid unexpected issues with a backup

❗ It is recommended the existing version is noted. This can be checked when a different version is installed to verify a proper update. The [Dashboard System Information Widget](#) will display the **Version** information:

System Information  	
Name	Anybus-Defender-ST02.localdomain
User	admin@192.168.200.222 (Local Database)
System	VMware Virtual Machine Serial: VMware-56 4d b4 c8 ea dc 2d 22-b9 d0 72 5f 11 e1 3b 3f Anybus Defender Device ID: 564db4c8-eadc-2d22-b9d0-725f11e13b3f
License	PRO
Version	2.5.2-RELEASE-2025042412 (amd64) built on Thu Apr 24 12:10:18 EDT 2025

Dashboard System Information Showing Version Information

Prerequisites

Internet access to **pkg.ics-defender.com** is required for this system update. If this is not possible, refer to the [Offline via USB Method](#) instead

Procedure

1. Navigate to [System / Update/ System Update](#)
2. From the **System Update** tab, the latest system update version should appear (or an **Up to date** message will appear and no further action is required):

System Update	Update Settings
Confirmation Required to update Anybus Defender system.	
Current Base System	2.5.2-2024070212
Latest Base System	2.5.2-2024070214
Confirm Update	☒ Confirm

Online Update with Updated Base System

3. Click the **Confirm** button to update the Anybus Defender. The unit will then reboot

⚠ As noted during the update, be sure NOT to leave or refresh the current web page

4. Verify the Anybus Defender successfully updated by referencing the [Dashboard System Information Widget](#)

Offline Packages Update

Overview

This procedure will show how to do offline updates of the [Packages](#) on the Anybus Defender using the USB port and a USB storage media device

❗ The file used for updating the packages is the same one used for the [Offline USB System Update](#)

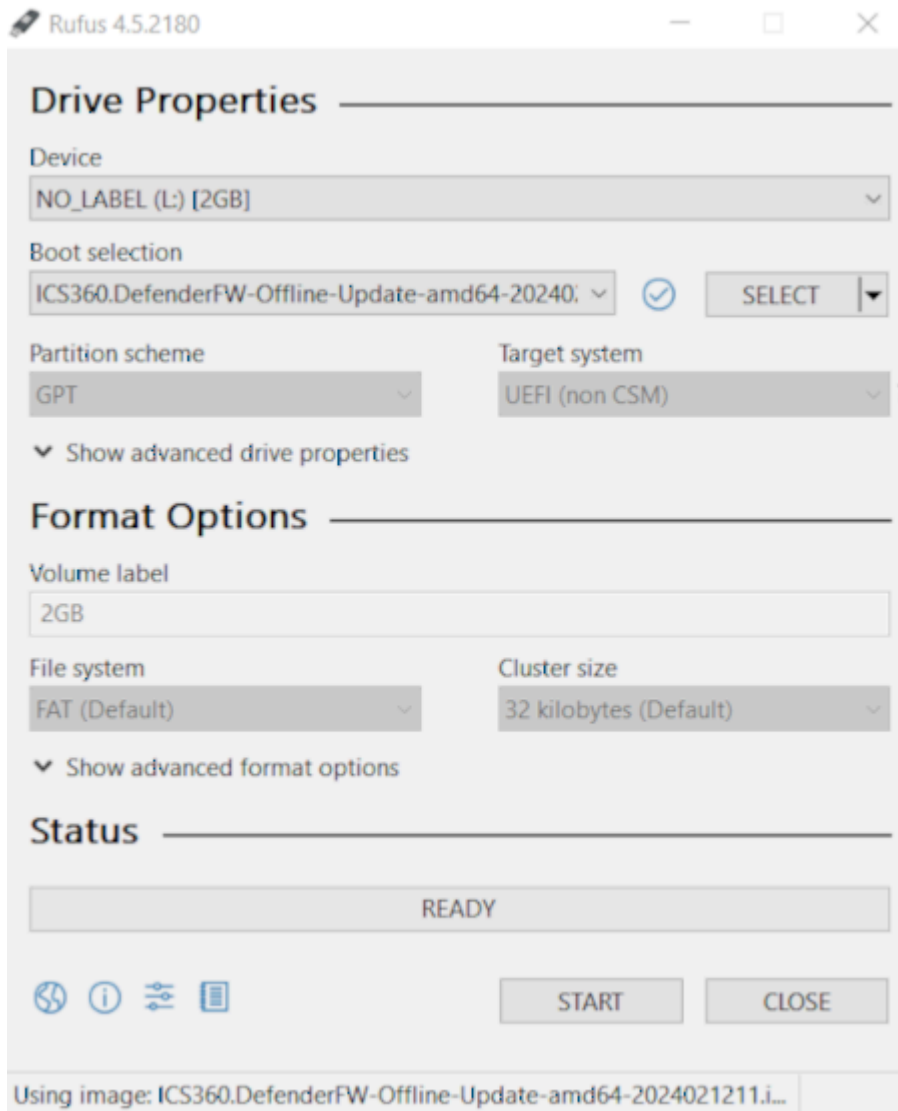
Prerequisites

Offline packages updates are performed using USB storage media with the system file (which includes the packages) provided from HMS. A drive can also be created using the **Creating a System Update USB Drive** section below

Creating a Offline Packages USB Drive

A USB drive can be created by using a free disk utility named [Rufus](#). With this, only the offline packages image file is needed to create a system update drive

After opening Rufus, select the proper USB drive from the **Device** dropdown. Load the proper **.img** file from the **SELECT** button file picker:



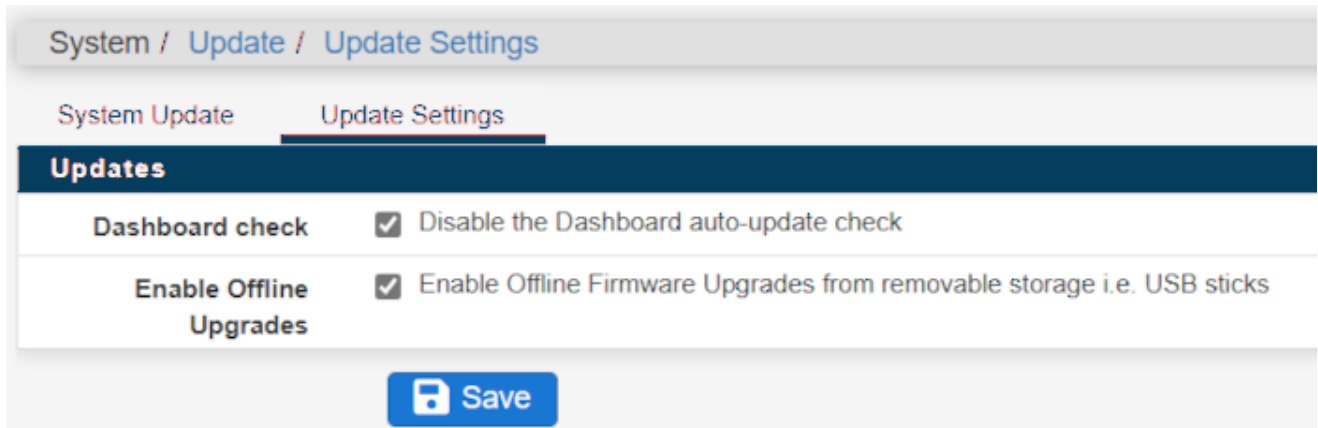
Rufus with Drive and Image File Loaded

Click the **START** button and wait for it to finish

After completion, the USB storage media can be removed from the PC and the procedure below can be used

Procedure

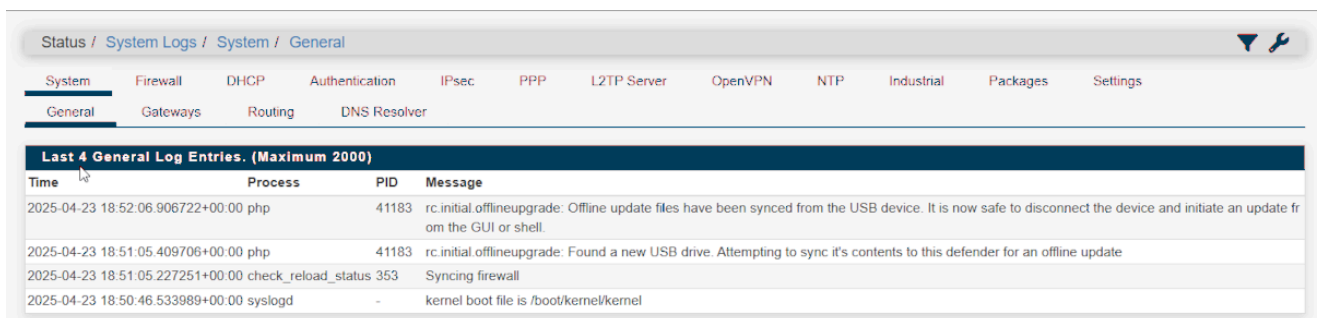
1. Insert the USB into any USB port of the Anybus Defender
2. Navigate to [System / Update/ Update Settings](#)
3. From the **Update Settings** tab, Check the **Enable Offline Upgrades** option:



Enable Offline Upgrades Checked in Update Settings

❗ At this point, the USB storage media will be accessed and checked. Once confirmed that the update is from HMS and safe, the necessary files will be transferred to the Anybus Defender

4. Click the **Save** button
5. Navigate to the [Status / System Logs / System General Log](#) page and verify the USB device entries appear:



Status / System Log Showing Completed USB File Sync

❗ Be sure the log entry `Offline updates have been synced from the USB device...` appears before removing the USB storage device (it is recommended to keep the device plugged in until the update is complete). Refresh the page periodically if needed

6. Navigate to the [System / Package Manager / Available Packages](#) page. There should be a list of packages that can be installed:

System / [Package Manager](#) / [Available Packages](#)

[Installed Packages](#)
[Available Packages](#)

Search

Search term

Both

Search

Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages			
Name	Version	Description	
Apcupsd	0.3.92_10	"apcupsd" can be used for controlling all APC UPS models It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN	+ Install
Arping	1.2.3_2	Broadcasts a who-has ARP packet on the network and prints answers.	+ Install
Arpwatch	0.2.1_6	This package contains tools that monitors ethernet activity and maintains a database of ethernet/ip address pairings. It also reports certain changes via email.	+ Install
Bandwidthd	0.7.5_5	BandwidthD tracks usage of TCP/IP network subnets and builds html files with graphs to display utilization. Charts are built by individual IPs, and by default display utilization over 2 day, 8 day, 40 day, and 400 day periods. Furthermore, each IP address's utilization can be logged out in CDF format, or to a backend database server. HTTP, TCP, UDP, ICMP, VPN, and P2P traffic are color coded.	+ Install
Freeradius3	0.15.8_32	A free implementation of the RADIUS protocol. Supports MySQL, PostgreSQL, LDAP, Kerberos.	+ Install
Frr	1.1.0_15	FRR routing daemon for BGP, OSPF, and OSPF6 Conflicts with Quagga OSPF and OpenBGPD. These packages cannot be installed at the same time.	+ Install
Ftp client proxy	0.3.1_7	Basic FTP Client Proxy using ftp-proxy from FreeBSD.	+ Install
Haproxy	0.61.1_3	The Reliable, High Performance TCP/HTTP(S) Load Balancer. This package implements the TCP, HTTP and HTTPS balancing features from haproxy. Supports ACLs for smart backend switching.	+ Install
Iperf	3.0.3_5	Iperf is a tool for testing network throughput, loss, and jitter.	+ Install
Ladvd	1.2.3_2	Send and decode link layer advertisements. Support for LLDP (Link Layer Discovery Protocol), CDP (Cisco Discovery Protocol), EDP (Extreme Discovery Protocol) and NDP (Nortel Discovery Protocol).	+ Install
Lldpd	0.9.12	lldpd provies support for the 802.1ab Link Layer Discovery Protocol (LLDP), as well as support for several proprietary discovery protocols including Cisco Discovery Protocol (CDP), Extreme Discovery Protocol (EDP), Foundry Discovery Protocol (FDP), and Nortel Discovery Protocol (NDP / SONMP).	+ Install
Mailreport	3.6.3_3	Allows you to setup periodic e-mail reports containing command output, and log file contents	+ Install
Mtr nox11	0.85.7_2	Enhanced traceroute replacement. mtr combines the functionality of the traceroute and ping programs in a single network diagnostic tool.	+ Install
Net snmp	0.1.6_9	A GUI for the NET-SNMP Daemon.	+ Install
Nmap	1.4.5_2	NMap is a utility for network exploration or security auditing.	+ Install

Available Packages showing Offline Items

7. Install any packages necessary

8. Verify the packages by navigating to the [System / Package Manager / Installed Packages](#)

Overview

Supplemental Overview

The supplemental section has reference information including these items:

- [Default Packages](#)
- [FAQ](#)

Overview

Default Package List

Here is a list of the default [Packages](#) installed in the Anybus Defender:

Package Name	Description
API	PROVIDES MODULAR RESTFUL APIS FOR USE BY A REMOTE SERVER
AssetMgmt	Asset Management that scans hosts on the network and identifies OS and/or Industrial Protocol information
RemoteMgmt	Integrates with a remote management server to allow remote control/visibility of this instance
WireGuard	An extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography

API

Overview

The **API** packages allows remote software, such as **Anybus Cybersecurity Console**, to interface with the **Anybus Defender**

❗ The [RemoteMgmt](#) package is also required for **Anybus Cybersecurity Console** to properly connect to the **Anybus Defender**

Asset Management

Overview

The [Asset Management](#) package adds the ability to scan devices on a network and generate a list of these devices

Remote Management

Overview

The **Remote Management** packages allows remote software, such as **Anybus Cybersecurity Console**, to interface with the **Anybus Defender**

❗ The [API](#) package is also required for **Anybus Cybersecurity Console** to properly connect to the **Anybus Defender**

Wire Guard

Overview

The **WireGuard** packages allows using the [WireGuard VPN](#) in **Anybus Defender**

Typically, WireGuard is used for [Peer-to-Peer Networks](#) for linking 2 sites

FAQ

Overview

This FAQ (Frequently-asked Questions) will answer common questions and items that might arise when configuring the **Anybus Defender**

1:1 NAT

1. Why does my PLC not work correctly when using the [1:1 Simple NAT Wizard](#)? **Within the ethernet settings of the PLC, the LAN side gateway address must be set. Example:**

General Port Configuration

Network Configuration Type

☒ Static ☐ Dynamic

☐ Use DHCP to obtain network configuration.

☐ Use BOOTP to obtain network configuration.

IP Address: 192 . 168 . 200 . 202

Network Mask: 255 . 255 . 255 . 0

Gateway Address: 192 . 168 . 200 . 1

Rockwell PLC Example Using the Default 192.168.200.1 LAN Gateway Address

Packages:Suricata

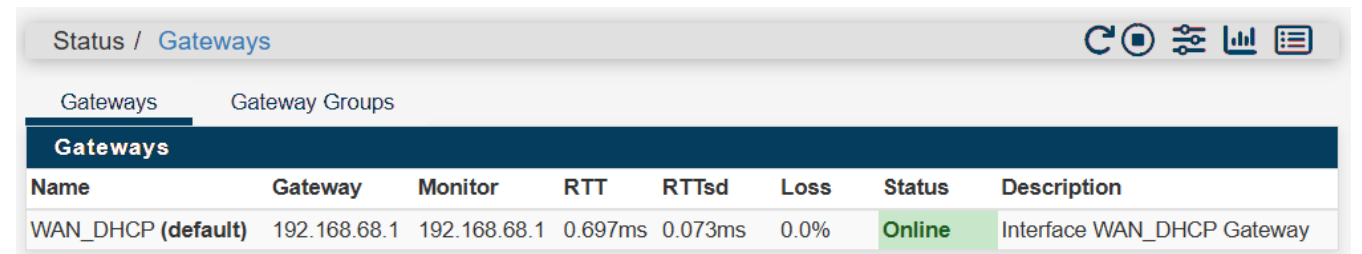
1. Why does using the **ETOpen Emerging Threats Rules** option in the **Global Settings** not download the Suricata rules? Depending on the version of the **Anybus Defender** or **Suricata** installed, the **ETOpen** may not download correctly. As a work-around, set the **Use a custom URL for ETOpen downloads** checkbox and paste in this URL in the **ETOpen Custom Rule Download URL** area:

```
https://rules.emergingthreatspro.com/open/old/suricata-4.0/emerging-  
all.rules.tar.gz
```

Then navigate to **Update** tab and click the **✓ Update** button to update the rule sets

Top Banner Buttons

Top Banner Buttons



Sample Header Buttons on Gateway Edit

Most sections within the Web GUI of the Anybus Defender will have a series of buttons on the upper right of the header bar. As shown in the example above, the [Gateways Edit Page](#) has 5 buttons in its navigation banner:



Sample Header Buttons on Gateway



Other Specialized Buttons

The table below will show all possible buttons that may be present on any page's top banner:

Button	Name	Description
	RESTART SERVICE	IF THIS IS OR RELATED TO A SERVICE , THIS WILL RESTART IT
	Stop Service	If this is or related to a service, this will stop it
	Related Settings	If there is a settings page associated with the current page, this navigates to that page
	Related Status	If the is a status page associated with the current page, this navigates to that page
	Related Log Entries	If there is a Logs page and section associated with the current one, this navigates to that page
	Settings	This will load a settings page
	Filter	On the System Logs section, this allows for a filter section to appear
	Export	On the Status / Monitoring section, a graph can be exported