

iStatus ArpWatch[™] Setup Guide

About iStatus ArpWatch

iStatus ArpWatch allows you to easily establish a baseline of known/trusted devices on your LAN. When ArpWatch is enabled, it learns the devices on the network so that you can easily approve those devices. Importantly, it also notes the default gateway and DNS servers for an added layer of network monitoring.

After iStatus is deployed, ArpWatch continuously monitors the network for critical security changes and can detect rogue or unapproved devices when they are attached to your network. Many large corporations have been breached as a result of having unknown or unapproved devices on their network. iStatus can help detect changes to DNS servers (resulting from DNS poisoning attacks).

This brief guide will show you how to set up your ArpWatch discovery period and view your connected network devices detected by ArpWatch. Feel free to use the bookmarks to jump to your deseired section, such as ArpWatch Templating.

Assigning Licensing

NOTE: A Group must have an available license to assign to a probe before you can use ArpWatch or a create an ArpWatch template.

1. Select 'Organization' from the left-hand navigation menu in the iStatus Dashboard.

From the drop-down menu, select 'Licensing.'

Select 'ArpWatch' on the right-hand side of the 'License Management' box.

Here you can assign licensing from your pool to each Probe in iStatus, as well as connect an ArpWatch template. You can view how many licenses you have purchased and applied.

In the example, Demo Org has 4 of their 6 ArpWatch licenses applied to 4 Probes.

×	🐼 iStatus		Q Search
	Dashboard > Organizations - Licensing		
Dashboard	Demo Org		
Insight Manager			
Register a Probe	Summary Licensing Templating Contacts	& Notifications Organization Probes Billing	
View All Groups			
Organizations	License Management For Organization: /	ArpWatch @ NPM ArpWatch Pinpoint	
Summary	This organization currently has 4 of 6 ArpWatch li	censes in use. Click here to get more.	
Licensing	C This organization currently has 0 ArpWatch licens	es reserved for this subscription (Unusable by the group).	
Templating	Search		
Contacts & Notifications	NAME	LICENSES CONNECTED TEMPLATE	
Probe Management	Probe	1 Edit Licenses N/A	
Billing	Proha	1 Friit Licenses N/A	
Audit Logs			
	Probe	1 Edit Licenses N/A	
April Billing Cycle ends	Probe	1 Edit Licenses N/A	
lling Cycle 9 days remaining		4 of 6 organization licenses allocated to probes	



Once an ArpWatch license is assigned to a probe, it will automatically turn on and start monitoring for devices. It may take up to 12 minutes for it to fully turn on.

Creating a Template

1. In your 'Organization,' click on 'Templating' and then 'Create a new Template.' This will create a default template to edit for any licenses you may have.

There are additional options to check before finishing your 'Template.' Click the 😢 next to each to further explain these options.

2. Once created, click on 'Create' then select 'Edit' down below to change settings and set up your ArpWatch Targeting. There are several Settings here to set up deployment of the ArpWatch

Template you created. The 🕜 provides an explanation of each setting.

In the example, ABC Inc. has the settings applied, so this 'Template' is not automatically assigned to the new Probe and allows the Group to directly use any spare licenses not used in this Template.

) iStatus	
nboard > Organizations → > Templating	
BC INC.	
ummary Licensing Templating Contacts & Notifications Organization Probes Billing	
emplate Management for ABC INC. 🚱	Organization C View Group Templating
urrent Template: Default 🖋 ABC Standard Template	~
Delete	Create a new Template
efault NPM Configuration 🔞	NPM ±
iis Organization has used 0 out of 10 NPM licenses. @ nere are currently 0 NPM templated items in this Configuration out of a total of 10 NPM templated items To start, add an existing template or create a new template.	
Create a New NPM Template	
PM Settings	
Automatically apply Configuration to new Probes 🔞	
Use Organization Reserved Licenses 🚱	
If this is selected, any licenses reserved by the organization will not be usable at the group level directly.	×
Assign Alert Threshold to All Current Network Targets/Categories 😡	
Alert Threshold @	Never
Cancel	Save

🖗 Akative

3. Once you have created and saved your 'Template.' Go back to the 'Licensing' tab, and you can manually connect the template here if it wasn't automatically connected.

In the example, ABC Inc. has assigned 4 licenses to be used by Customer A. and has connected ABC Standard Template.

ABC INC.					
Summary Licensing Templating Contacts & Notifications Organization Probes Billing					
License Management For Organization: NPM @				NPM	ArpWatch
Successfully updated Licenses					×
This organization currently has 4 of 10 NPM licenses in use. Click here to get more.					
This organization currently has 0 NPM licenses reserved for this subscription (Unusable by the group).					
Search					
NAME	LICENSES		CONNECTED TEMPLATE		
			Select a Configuration		
Customer A	4	Edit Licenses	ABC Standard Template	11 •	~
			Cancel		Save
	4 of 10 organization licenses allo groups	ocated to			
Showing 1 to 1 of 1	< Previous 1 Nex	×t >	Results per page: 10 V		

If allowed, a Group can create their own Template by following similar steps On the Group Page. A Group can only have Template connected. Those assigned at the Organization level cannot be edited or changed by the Group.

ArpWatch on the Probe Page

 View the ArpWatch page by navigating to the probe page and then clicking on the 'ArpWatch' tab in the horizontal bar under the Timeline. (You can navigate via the search box (Searching for the Probe's Probe ID, the owned location, etc.), the Organization Overview on the main dashboard page, from the Organization License page by clicking the probe name, or by going to the probe via the 'View All Groups' page located on the navigation bar.

	«	April 21st - 28th, 2023 11:08 am - 11:08 am	3		@ Zoon	n Q. Reset Hour Da	y 7 Days 30 Days	Custor
pand All +					1章 /	scending, Ordered by Default	Sort 🗸	ර
(0 events)	>	04/23	04/24	04/25	04/26	04/27	04/28	
ite: Scale bars are *1 day apart								N
	Displayed statistics a	are based on this probe. Applying filters or	selecting specific timelines will cha	nge these values. To show:	statistics for all visible timelines g	ick here.		
Uptime: 100%	Downtime: 0%	Failed Over: 0%	SD-WAN A	ctive: 0%	Issues	Event Bundle	No Data	

 Once your probe has an ArpWatch license, it should automatically activate and track your network's devices. By default, a learning period of 48 hours will be applied to this probe. This means that any ArpWatch events will not be triggered until we learn about your network for 48 hours.



NOTE: To disable this learning period, change the ArpWatch settings as detailed below. Currently, we do not support supernets greater than a /24. If ArpWatch is not enabled due to this restriction, it will need to be bound to a smaller network's probe.

3. After the ArpWatch learning period has concluded, your network device information will be visible. In the ArpWatch component, you can mark devices as known, unknown, or untrusted, give them names, and see what is currently active on your network and is not active.

Changing ArpWatch Settings

1. By default, ArpWatch is active with 'Medium' network settings – this means that IP Changes will be automatically accepted, and alerts will be generated for LAA MAC address devices. These settings can be changed on the ArpWatch tab of the probe page in the ArpWatch component.

Summary NPM • ArpWatch Pinpoint						
iStatus ArpWatch™ Network Security Monit	coring 🛛		Last Updated: Apr 15, 2022, 10:07:34 AM Options 🗸 🗸	Events @	March 16th - April 15th, 202	• T •
Contact List: Thinix Developers	Security Settings: Medium	Monitoring: Gateway Changes, New Devices, Untrusted Devices	⑦ Disabled €192,168,5,254 ∨	Dev. Probe 4 at Thinix Developers (network 14 days ago	mes) discovered a new device on the local	Ongoing
Contact List	Thinix Developers		~	Dev. Probe 4 at Thinix Developers (Ames) switched its default gateway	Ongoing
Monitoring Types	Monitor Gateway Changes, Wat	ch For New Devices, Monitor Untrusted Devices	⊠ *	U 14 days ago		Cingoing
Security Settings Advanced 😧	Low	Medium	High		View All	
Enable Learning Period 🚱 (Disabled)	1 Hours	2 Hours 24 Hours 24 Hours	3 Days Disabled			
Cancel			Save Changes			
Search for devices		Device Management 👻 Mark Ali A:	Known Export Devices as CSV 📓 Create Report			

The 7 provides an explanation of each setting.

2. By clicking 'Advanced,' you can see and select advanced settings individually.

iStatus ArpWatch™ Network Security Monit	oring 🚱		Last Updated: Apr 15, 2022, 10:07:34 AM	Options 🗸 🗸
Contact List: Thinix Developers	Security Settings: Medium Monitoring: Gateway Ch.	anges, New Devices, Untrusted Devices	Disabled 2192.1	68.3.254
Contact List	Thinix Developers			~
Monitoring Types	Monitor Gateway Changes, Watch For New Devices, Monitor	Untrusted Devices		
Security Settings Simple 🕑	Automatically accept IP changes?	Generate Alerts fo	r Locally Administered Address Dev	vices?
Enable Learning Period 😧 Disabled	1 Hours 2 Hours	4 Hours 24 Hours	3 Days	Disabled
Cancel				Save Changes

3. You can adjust which types of events to monitor on your network by changing the 'Monitoring Types' options in the monitoring types drop-down.

Monitoring Types	Monitor Gateway Changes, Watch For New Devices, Monitor Untrusted Devices	⊻ ∨
Socurity Settings Simple O	Monitor Gateway Changes	2 V 2 2 2 2
security settings simple	Monitor Untrusted Devices	
Enable Learning Period 😧 Disabled	Watch For New Devices	

4. You can search for specific devices in the search box located in the component.

🔊 Akative

as spread the month second monit			
Contact List: Thinix Developers	Security Settings: Medium Monitoring: Gateway Changes, New Devices, Untrusted Devices Disabled Ca192.168.3.254	~	Dev. netv 14 da
ontact List	Thinix Developers	~	Dev
Ionitoring Types	Monitor Gateway Changes, Watch For New Devices, Monitor Untrusted Devices		14 0
ecurity Settings Simple 🕢	Automatically accept IP changes?		
nable Learning Period 😧 Disabled	1 Hours 2 Hours 4 Hours 24 Hours 3 Days	isabled	
Cancel	Sav	e Changes	

In the 'Device Management' drop-down, you can create your own known device and read our tutorial on LAA MAC address devices.

earch for device	5			Device Management V Mark All As Known Export D	Devices as CSV 📓 Create Report
STATE 1	IP ADDRESS (HOSTNAME)	DEVICE NAME	MAC ADDRES	+ Add New Device (Static Non-LAA MAC Address)	SEEN 11 STATUS 11
		(Set Device Name)		P Configure Mobile Devices with LAA MAC Addresses	

You can also use these buttons to export devices and even create an ArpWatch report directly from the component!

The device status will tell you whether a device is new, known, untrusted, etc.

Naming ArpWatch Devices (Optional)

You can name a device by clicking on the device name in the ArpWatch component device table or by clicking the edit button (the square with the pencil).

Г	STATE	IP AUDRESS (HOSTNAM	E) 1	DEVICE NAME		MAC ADDRESS	DEVICE VENDOR	LAST SEEN		STATUS	
	•	192.168.3.254 🛛 🖀 Default (Sateway	(Set Device Name)	ľ	00:90:7f:00:40:ef	WatchGuard Technologies, Inc.	4/15/22, 1:56 P№	I.	New	
				Dev Probe 4							

Type in the name you want and then click 'Save,' and that's it!

STATE 1	IP ADDRESS (HOSTNAME)	DEVICE NA	ME 11 MAC ADD	ESS 1. DEVICE VENDOR		LAST SEEN	STATUS	U.
•	192.168.3.254 🛛 🖀 Default Gateway	Firewall	Save 00:90:7f:	.0:40:ef WatchGuard Technolo	ogies, Inc.	4/15/22, 1:56 PM	New ····	

Marking ArpWatch Devices as Known, Untrusted, Etc. (Optional)

By clicking the ellipses (three dots) on the table, you can mark a device as known, unknown, and untrusted. You can also remove the device from the table here. After removing a device, it will not show in your table until we detect it on your network again.

🐼 Akative

-			-					Mark as Known
•	192.168.3.16	(Set Device Name)	ß	f4:f2:6d:28:b2:ba	iStatus®	4/15/22, 1:56 PM	New	Mark as Unknown
•	192.168.3.18	(Set Device Name)	C	f4:f2:6d:28:b2:0c	iStatus®	4/15/22, 1:56 PM	New	Mark as Untrusted
•	192.168.3.21	(Set Device Name)	ď	e4:95:6e:4b:fa:2d	iStatus®	4/15/22, 1:56 PM	New	Delete

That's it!

You're all set up. When ArpWatch is working correctly, you will receive events like the one below (after the initial learning period has ended). You can mark devices as known, unknown, and untrusted within the event and name the device after you click acknowledge. This will also resolve the ongoing event.

What Happened	A new device has been discovered on your probe's network (Borsheim Home).
Common Causes and Potential Solutions	iStatus ArpWatch™ is configured on your network and monitors the network by alerting you when any new devices are discovered.
	This alert was triggered because we discovered the device listed below. This type of alert normally occurs when you introduce any new devic on your network, such as a workstation, printer, smartphone, or IoT appliance.
	Note that the device vendor listed below may not match the brand-name of the device you have added. For example, if you add a computer from Hewlett Packard, it may show up as Intel or another vendor.
Monitoring Type	New Device Detected
Discovered	Apr 12, 2022, 9:30:04 PM
Acknowledgement 🛛	
Note: Before acknowledging a new device and trust this device. The "Mark as Unkno recognize and do not trust this device.	, please make sure to select the desired status of the device. The default "Mark as Known Device" option should be selected if you recognize $ imes$ wn Device" option should be selected if you do not recognize this device. The "Mark as Untrusted Device" option should be selected if you
Note: Before acknowledging a new device and trust this device. The "Mark as Unkno recognize and do not trust this device. New Name for Device	, please make sure to select the desired status of the device. The default "Mark as Known Device" option should be selected if you recognize × wn Device" option should be selected if you do not recognize this device. The "Mark as Untrusted Device" option should be selected if you
Note: Before acknowledging a new device and trust this device. The "Mark as Unkno recognize and do not trust this device. New Name for Device Message	, please make sure to select the desired status of the device. The default "Mark as Known Device" option should be selected if you recognize × wn Device" option should be selected if you do not recognize this device. The "Mark as Untrusted Device" option should be selected if you Enter a name for the device (Optional) Enter a description of how the event is being resolved (Optional)
Note: Before acknowledging a new device and trust this device. The "Mark as Unkno recognize and do not trust this device. New Name for Device Message	, please make sure to select the desired status of the device. The default "Mark as Known Device" option should be selected if you recognize × wn Device" option should be selected if you do not recognize this device. The "Mark as Untrusted Device" option should be selected if you Enter a name for the device (Optional) Enter a description of how the event is being resolved (Optional)
Note: Before acknowledging a new device and trust this device. The "Mark as Unkno recognize and do not trust this device. New Name for Device Message Choose an Option (Required)	c, please make sure to select the desired status of the device. The default "Mark as Known Device" option should be selected if you recognize × wn Device" option should be selected if you do not recognize this device. The "Mark as Untrusted Device" option should be selected if you Enter a name for the device (Optional) Enter a description of how the event is being resolved (Optional) Mark as Untrusted Device Mark as Unknown Device Mark as Untrusted Device Mark as Unknown Device
Note: Before acknowledging a new device and trust this device. The "Mark as Unkno recognize and do not trust this device. New Name for Device Message Choose an Option (Required)	c, please make sure to select the desired status of the device. The default "Mark as Known Device" option should be selected if you recognize × wn Device" option should be selected if you on ot recognize this device. The "Mark as Untrusted Device" option should be selected if you Enter a name for the device (Optional) Enter a description of how the event is being resolved (Optional) Mark as Untrusted Device Mark as Known Device Mark as Untrusted Device Mark as Unknown Device Acknowledge
Note: Before acknowledging a new device and trust this device. The "Mark as Unkno recognize and do not trust this device. New Name for Device Message Choose an Option (Required)	, please make sure to select the desired status of the device. The default "Mark as Known Device" option should be selected if you recognize × wn Device" option should be selected if you do not recognize this device. The "Mark as Untrusted Device" option should be selected if you Enter a name for the device (Optional) Enter a description of how the event is being resolved (Optional) Mark as Untrusted Device Mark as Unknown Device Mark as Known Device Acknowledg
Note: Before acknowledging a new device and trust this device. The "Mark as Unkno recognize and do not trust this device. New Name for Device Message Choose an Option (Required) Additional Details Device IP	, please make sure to select the desired status of the device. The default "Mark as Known Device" option should be selected if you recognize × wn Device" option should be selected if you do not recognize this device. The "Mark as Untrusted Device" option should be selected if you Enter a name for the device (Optional) Enter a description of how the event is being resolved (Optional) Mark as Untrusted Device Mark as Unknown Device Mark as Known Device Acknowledge 192.168.129.216
Note: Before acknowledging a new device and trust this device. The "Mark as Unkno recognize and do not trust this device. New Name for Device Message Choose an Option (Required) Additional Details Device IP Device MAC	c) please make sure to select the desired status of the device. The default "Mark as Known Device" option should be selected if you recognize × wn Device" option should be selected if you do not recognize this device. The "Mark as Untrusted Device" option should be selected if you Enter a name for the device (Optional) Enter a description of how the event is being resolved (Optional) Mark as Untrusted Device Acknowledge 192.168.129.216 72:7a:57:1f:2a:c6
Note: Before acknowledging a new device and trust this device. The "Mark as Unkno recognize and do not trust this device. New Name for Device Message Choose an Option (Required) Additional Details Device IP Device MAC Device Vendor	c) please make sure to select the desired status of the device. The default "Mark as Known Device" option should be selected if you recognize × wn Device" option should be selected if you recognize × wn Device" option should be selected if you

If ArpWatch is configured correctly, you will begin getting events like this if your security settings allow it