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.

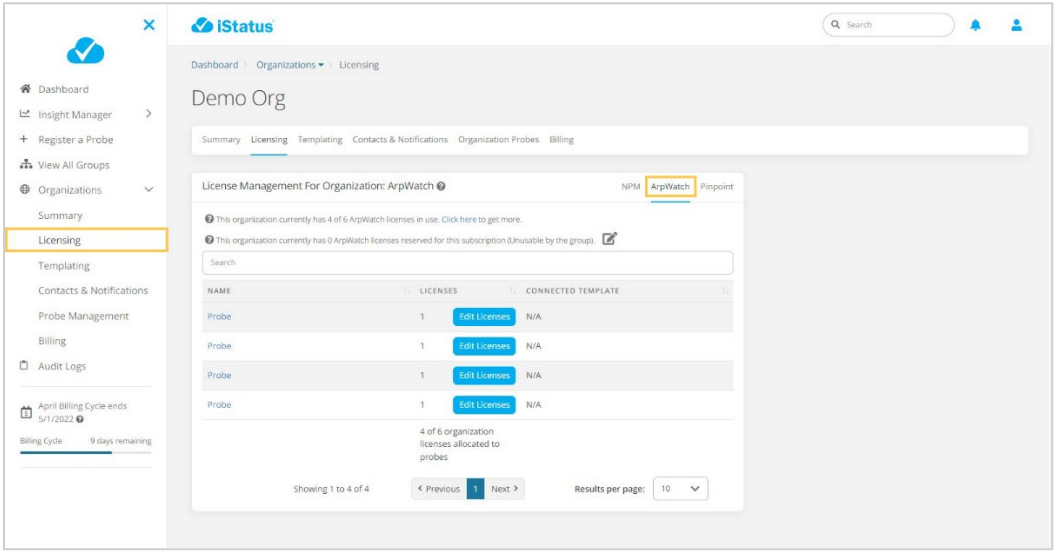
1. Select 'Organization' from the left-hand navigation menu in the iStatus Dashboard.

   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.



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.

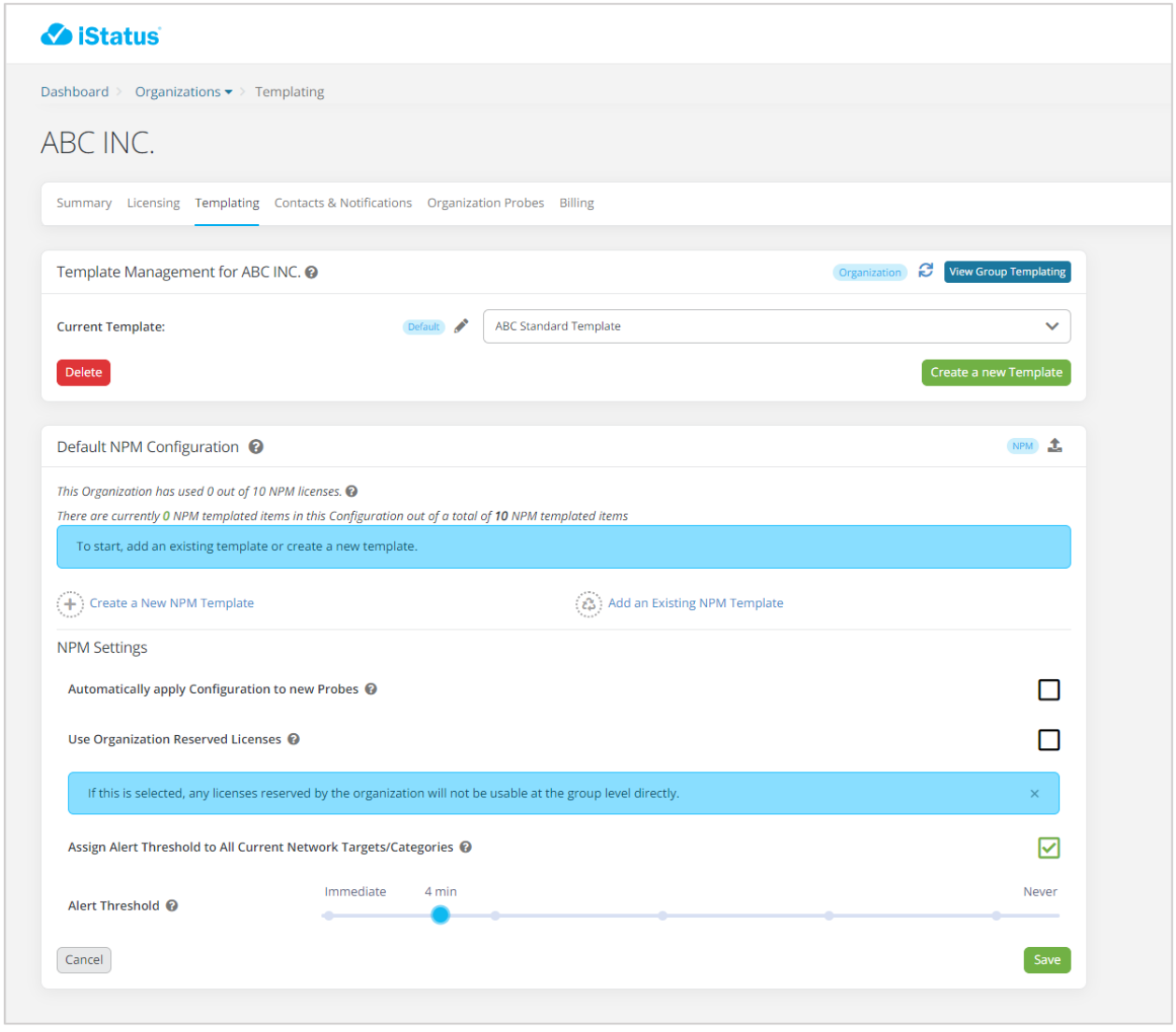
Creating a Template

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.

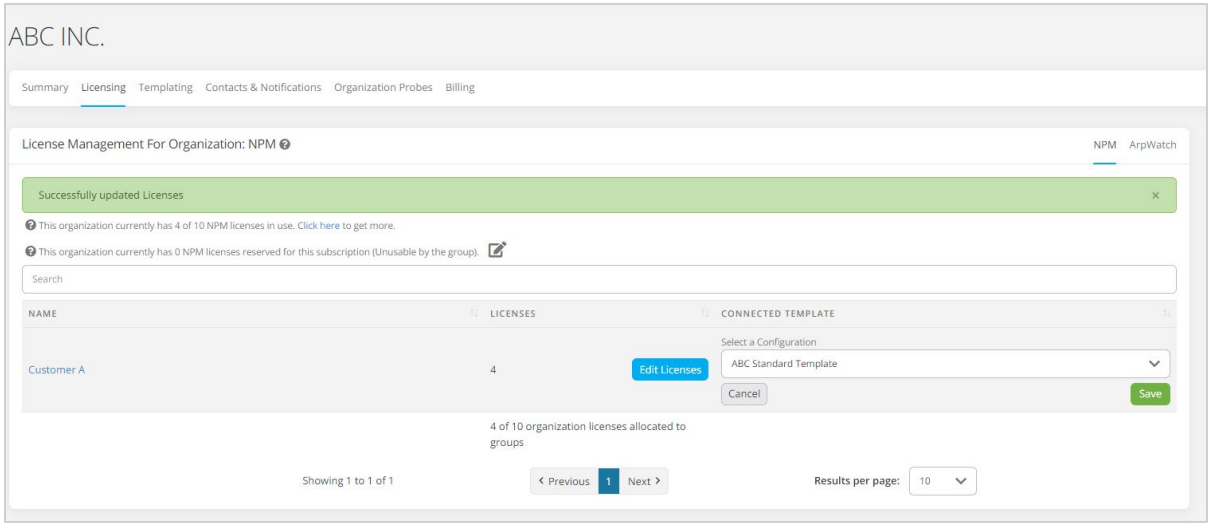
2. Once created, click on 'Create' then select 'Edit' down below to change settings and set up your ArpWatch Targeting. There are several Settings here to set up deployment of the ArpWatch Template you created. The ? provides an explanation of each setting.

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.



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.

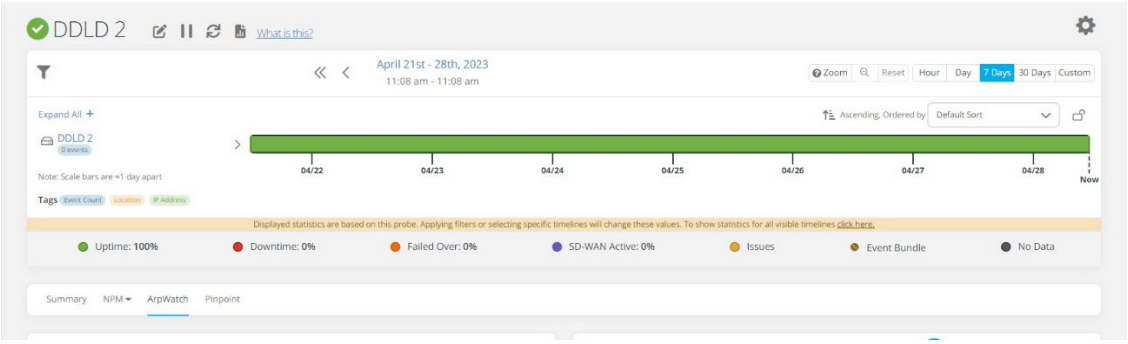
In the example, ABC Inc. has assigned 4 licenses to be used by Customer A. and has connected ABC Standard Template.



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

1. 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.



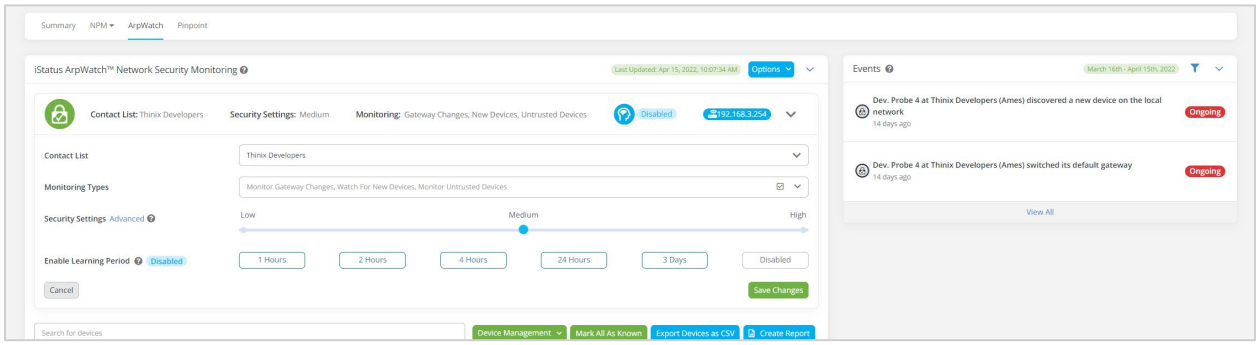
2. Once your probe has an ArpWatch license, it should automatically activate and track your network’s devices. **By default, a learning period of 48 hours will be applied to this probe. This means that any ArpWatch events will not be triggered until we learn about your network for 48 hours.**

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.

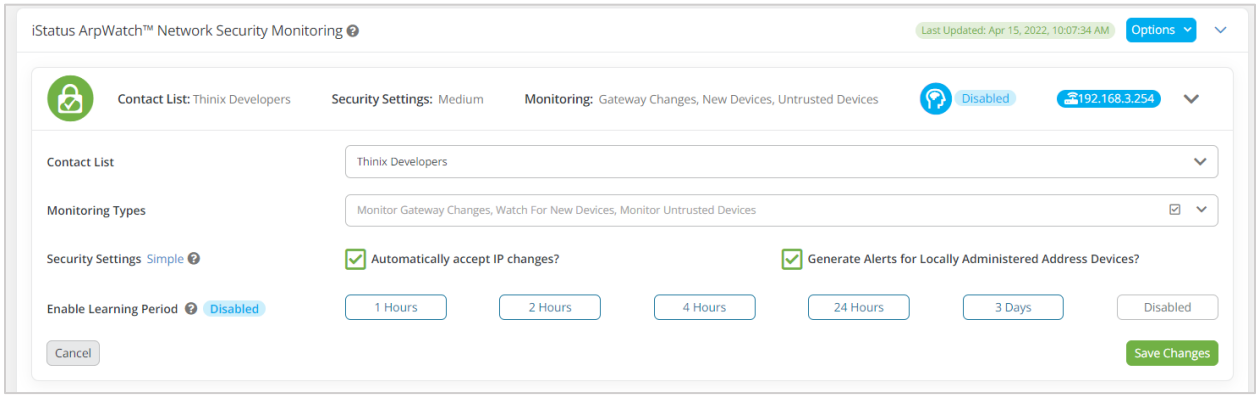
Changing ArpWatch Settings

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.

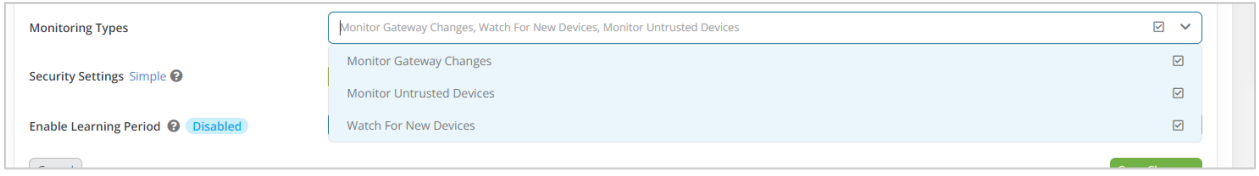


The ? provides an explanation of each setting.

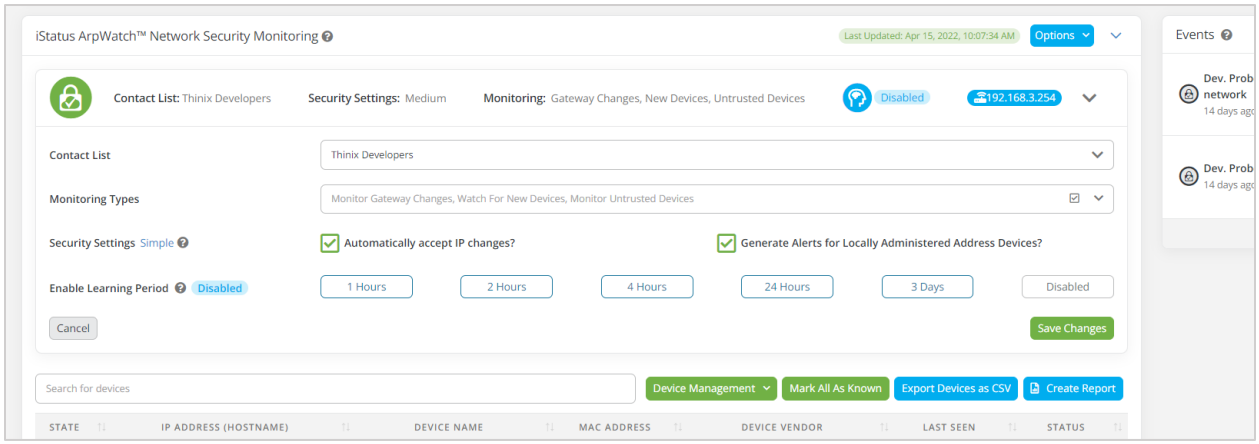
2. By clicking 'Advanced,' you can see and select advanced settings individually.



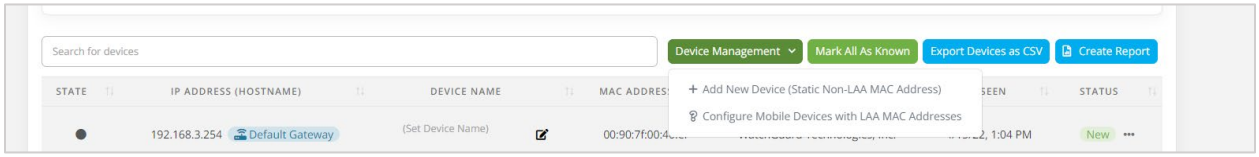
3. You can adjust which types of events to monitor on your network by changing the 'Monitoring Types' options in the monitoring types drop-down.



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



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

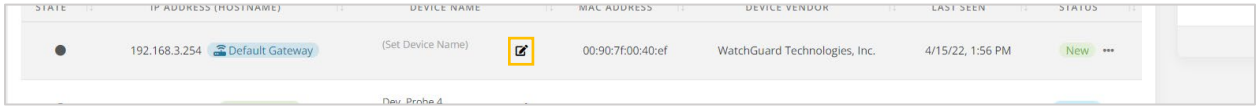


You can also use these buttons to export devices and even create an ArpWatch report directly from the component!

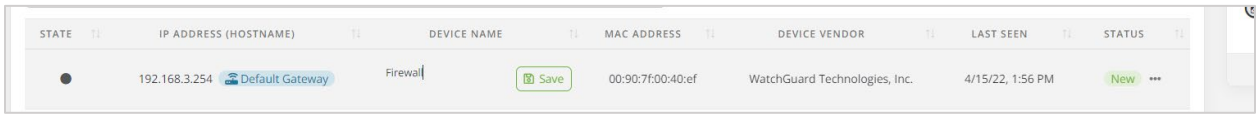
The device status will tell you whether a device is new, known, untrusted, etc.

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).



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

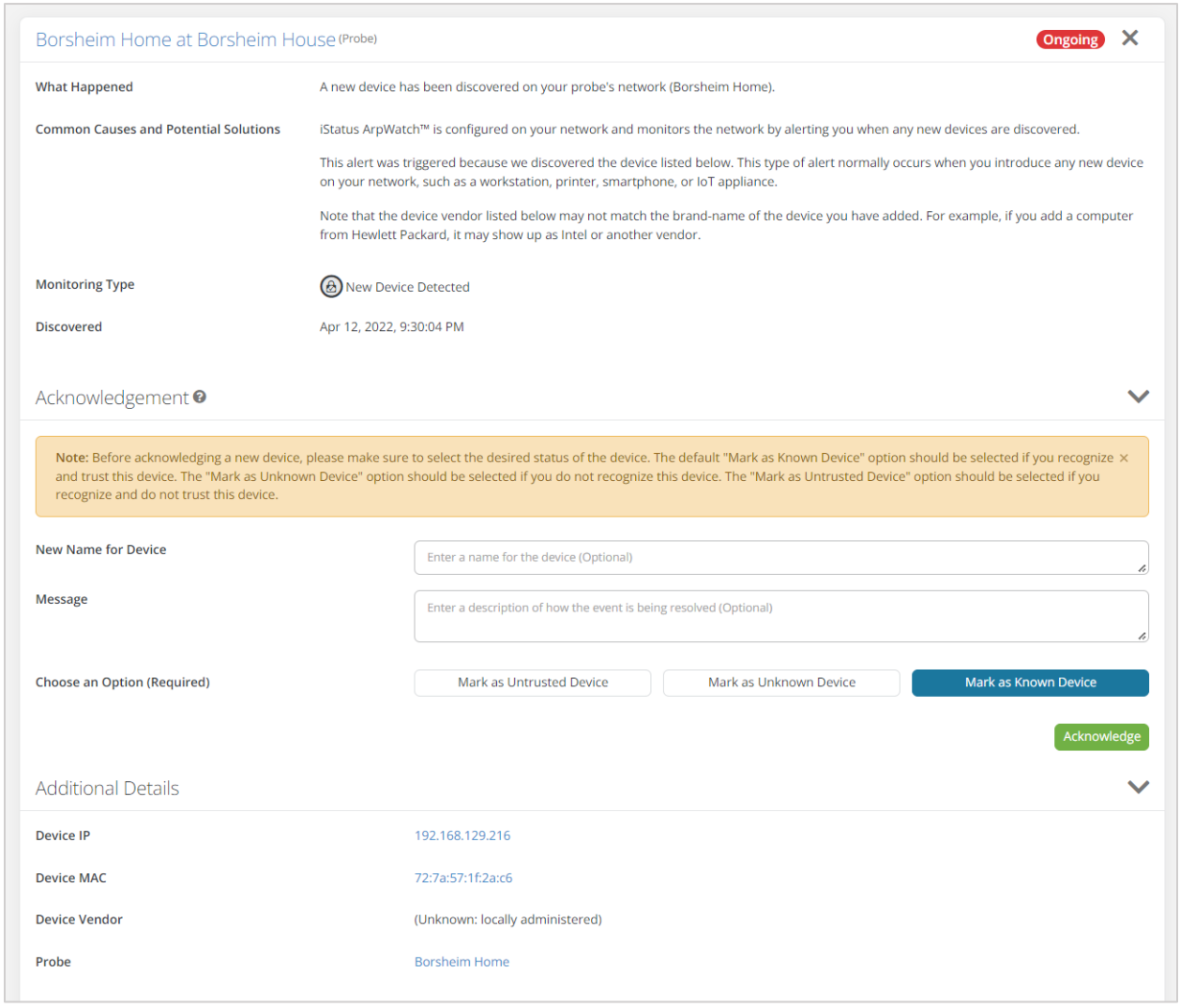


Marking ArpWatch Devices as Known, Untrusted, Etc. (Optional)

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.

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.



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