iStatus Pinpoint™ Setup Guide

About iStatus Pinpoint

iStatus Pinpoint can automatically troubleshoot a connection failure and determine the exact point of failure in minutes rather than hours or days associated with the manual process of having a technician find a problem. Because iStatus Pinpoint can identify issues in just a few minutes, the labor savings generated by Pinpoint can save Akative customers thousands of dollars per year, frequently allowing our solutions to immediately ROI. Pinpoint can prevent costly in-person intervention and enables problems to be quickly understood so that repairs can be made.

In the context of iStatus Security™, Pinpoint and NPM can be combined and can play an important role. For example, suppose cyber attackers launch a DDOS (distributed denial of service attack), taking a location offline. In that case, Pinpoint can determine the point of failure, helping distinguish the difference between a link failure or if performance is considerably affected, but the connectivity doesn't completely fail. In contrast, NPM can help provide analytics and baseline information to help IT professionals understand the root cause.

This brief guide will show you how to set up iStatus Pinpoint.

NOTE: The iStatus Pinpoint feature is dependent upon a special firewall configuration. Please reach out to support@akative.com to have an Akative technician assist you.

Assigning Licensing

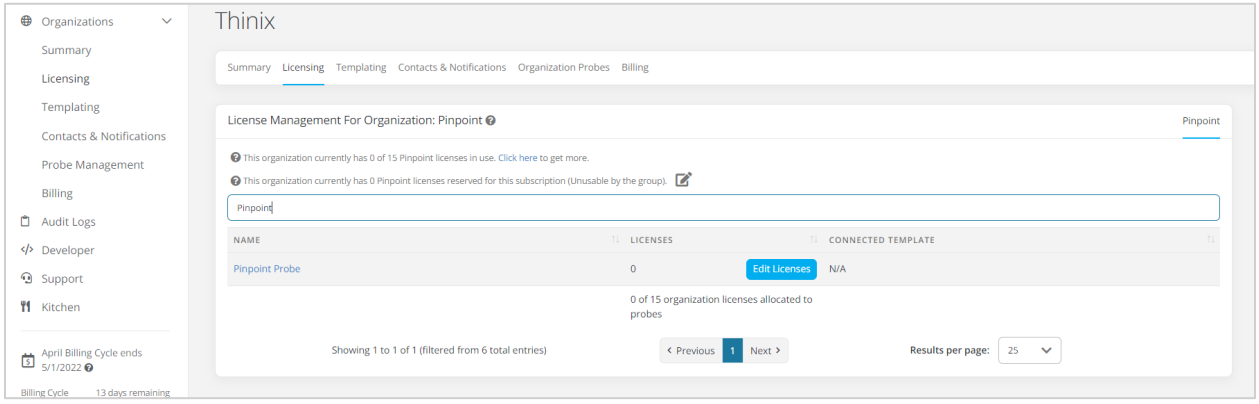
1. Select 'Organization' from the left-hand navigation menu on the iStatus Dashboard.

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

2. Select the 'Pinpoint' tab.

   Here you can assign 'Licensing' from your pool to each Probe in iStatus, as well as connect a Pinpoint template. You can view how many licenses you have purchased and applied.

In the example, ABC Inc. has 1 Group Customer A and 10 Pinpoint licenses. No licenses have been applied.



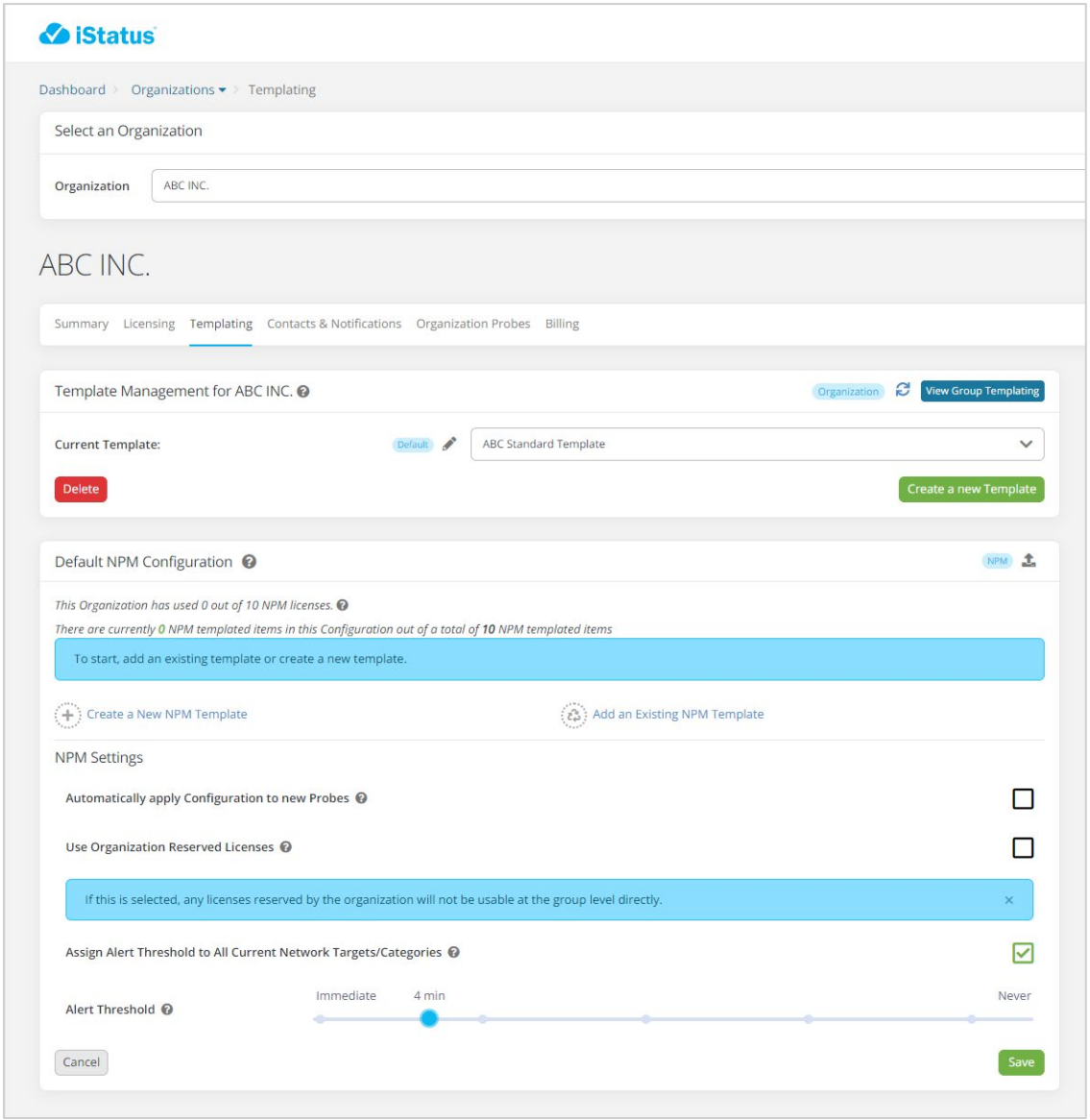
Creating a Template

3. 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.

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

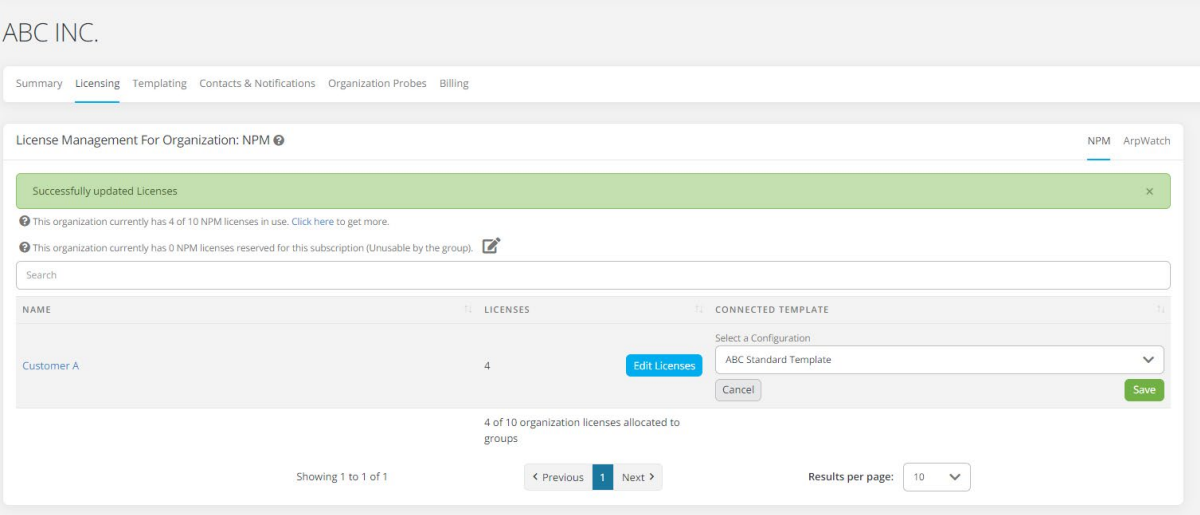
4. Once you've created your template, click on 'Create,' then select 'Edit' down below to change settings and begin setting up your Pinpoint Targeting. There are several 'Settings' here to set up deployment of the Pinpoint Template you have created. The provides an explanation of each setting.

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.



5. 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.

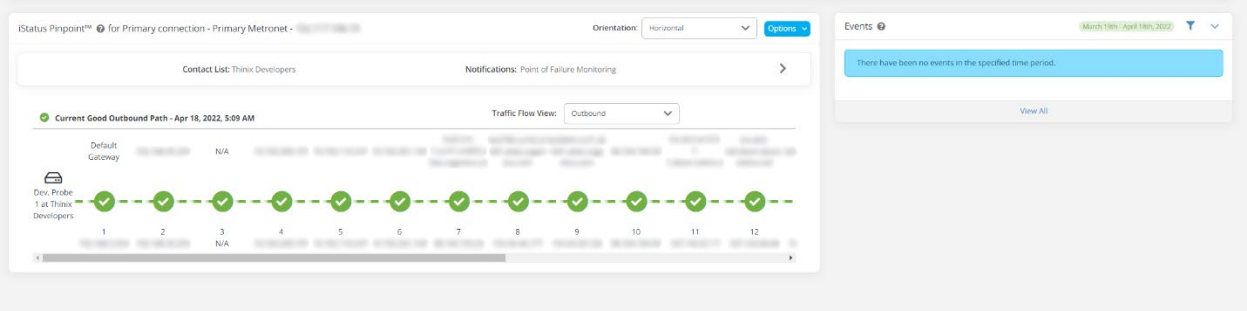
Navigate to the Probe page

Once your probe has a Pinpoint license, it should automatically activate and start watching your network (if you have an active RocketFailover connection for the probe). If you do not have a valid RocketFailover connection, Pinpoint will be automatically disabled until you get one. A primary connection is also required.

NOTE: It's recommended that you have a fully registered and fully set up probe with active connections before activating Pinpoint, but you may configure it before having the required connections set up if desired.

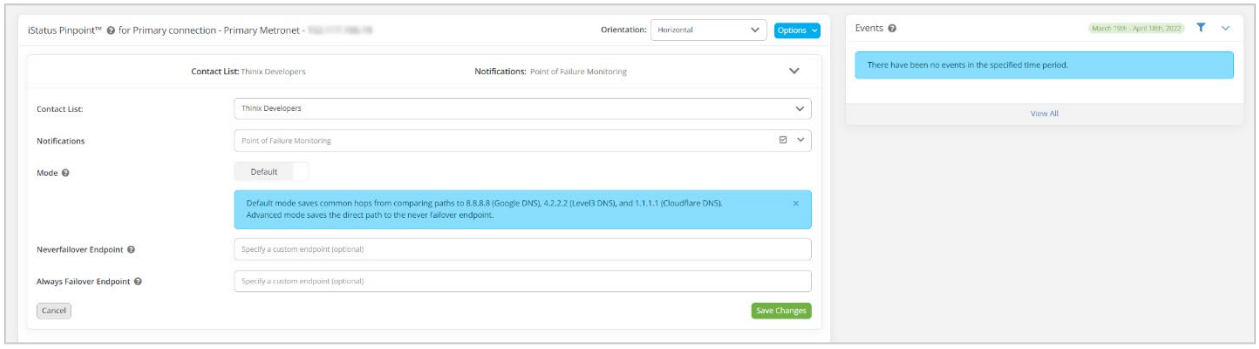
Pinpoint also requires a custom firewall configuration or a 'NeverFailover' path to be set up on the firewall to work correctly. To set this up, refer to the NeverFailover setup guide.

6. You can go to the Pinpoint page by navigating to the probe page and then clicking on the 'Pinpoint' tab – this can be done via the search box (Searching for the Probe's Probe ID, the owned location, etc.), the Organization Overview on the main dashboard page, or by going to the probe via the 'View All Groups' page located on the navigation bar
7. In the Pinpoint component, you can view your current 'good' path, and if you go into failover, your probe will attempt to detect the point of failure on the path and show it to you in this component as the current (Bad) path.



Changing Pinpoint Settings

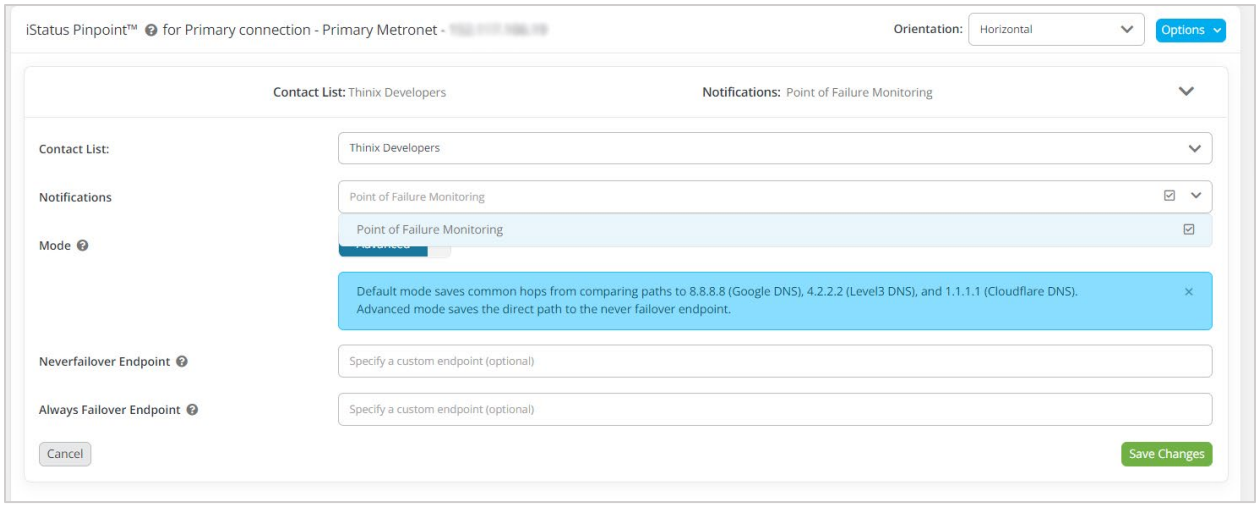
8. By default, Pinpoint is activated in the 'Default' mode (This compares your path to the internet to three common DNS targets and uses the common hops as your good outbound path to the internet).
   NOTE: There are fields where you can specify your NeverFailover target and AlwaysFailover endpoint. You should use these fields only if you are an advanced user and know that you need these custom fields specified.



The ? Provides an explanation of each setting.

9. By clicking 'Advanced,' your Pinpoint will now use the direct path to the NeverFailover endpoint instead of using common DNS targets for common hops

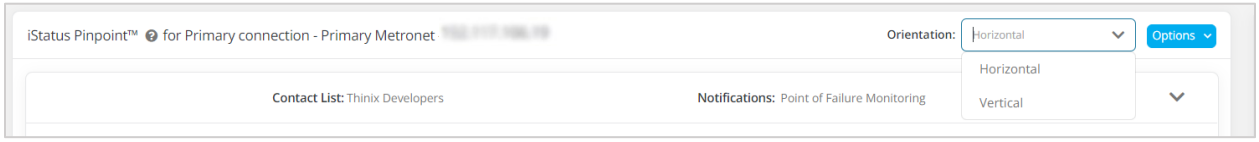
10. You can adjust which types of events to monitor on your network by changing the 'Notifications' options in the monitoring types drop-down. Any notification types selected here will be pushed out to users in the given contact list



11. Hit 'Save Changes,' and you're good to go!

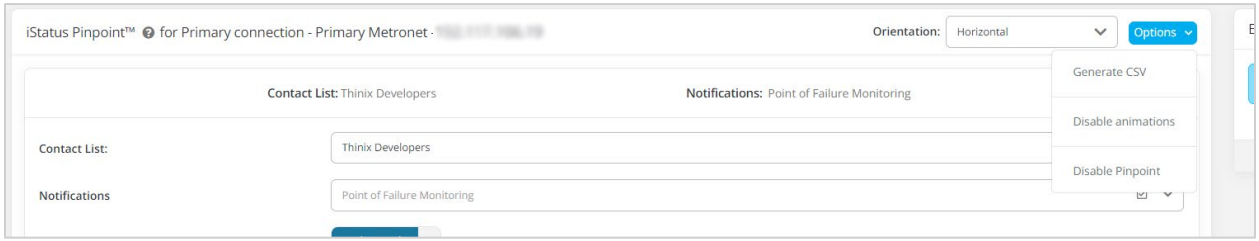
Additional Pinpoint Options

You can adjust the default orientation of the pinpoint component here:



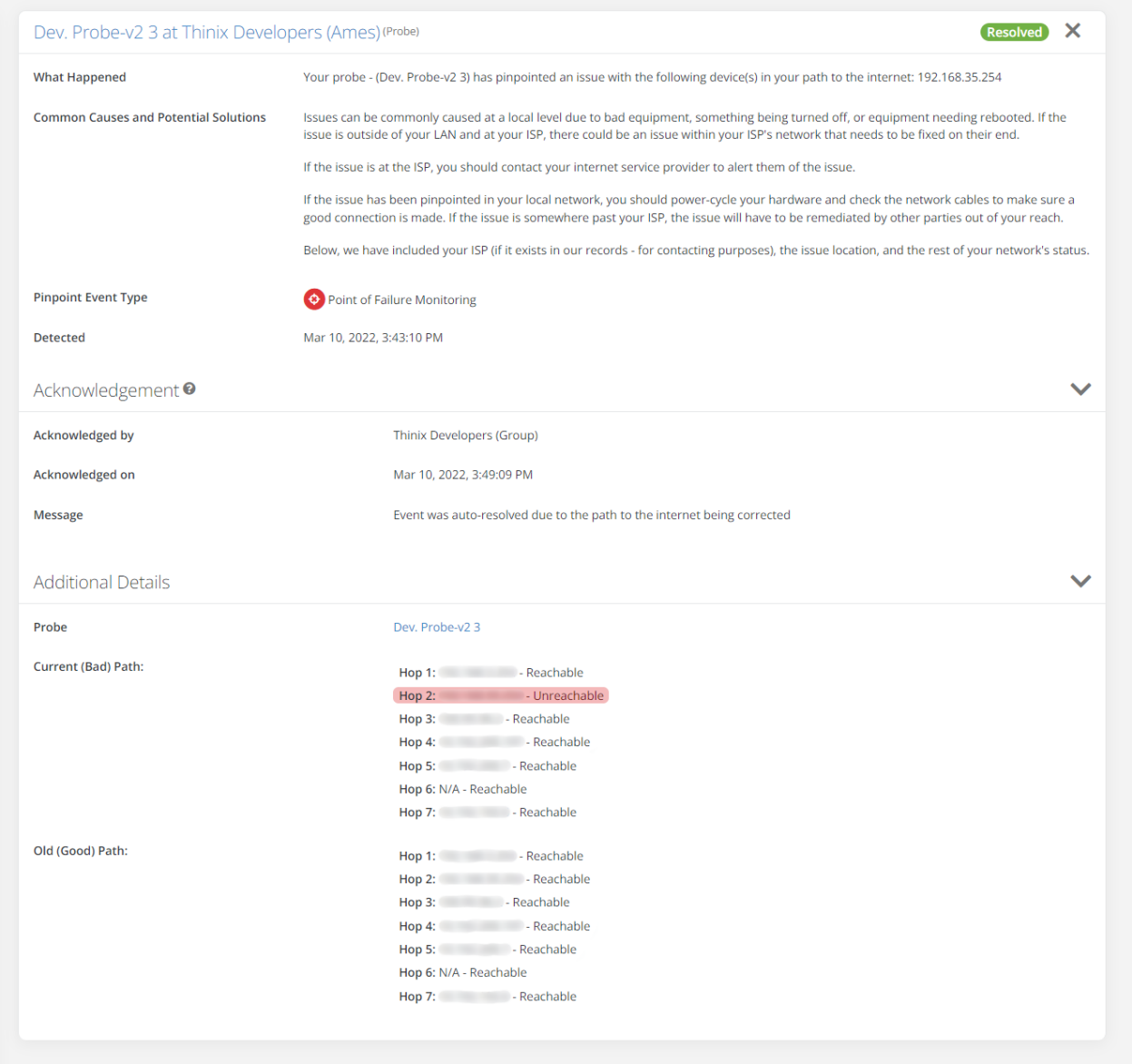
By default, the orientation is set to horizontal; however, a vertical orientation may be better on smaller devices such as smartphones.

Using the 'Options' drop-down, you can export a CSV of the current path(s), disable animations if they are causing your device to slow down, or disable Pinpoint altogether (you can re-enable it again once it's disabled)



That's it!

You're all set up. When Pinpoint is working correctly, you will receive events like the one below (when we detect a failure on your path to the internet)



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