iStatus ChangeDetection™ Setup Guide

About iStatus ChangeDetection for DNS Changes & Gateway Changes

iStatus ChangeDetection establishes a baseline and automatically documents critical network attributes such as the DNS servers in use, the MAC address of the default gateway, and the IP addresses of servers and other network devices.

Detect critical changes in your default gateway – All the devices on a network segment send data to the default gateway, which forwards that traffic to other servers or the Internet. When hackers gain access to secure networks, they frequently launch a MIM (Man-in-the-Middle) attack where the hacker masquerades as the default gateway. iStatus ChangeDetection thwarts these attacks by detecting changes to your default gateway that can indicate an attack or possible misconfiguration.

Detect critical security changes in DNS – Changes in DNS servers can be an indication of DNS hijacking, which hackers use to redirect unsuspecting users to servers that act as normal servers, but instead are designed to harvest credentials. iStatus ChangeDetection also detects DNS changes that can help alert to possible attacks or misconfigurations.

This brief guide will show you how to set up your ChangeDetection feature and where to go to see detected events. NOTE: ChangeDetection is a co-integrated component of the ArpWatch feature.

Navigate to Your Group Page

1. There are many different ways you can find the Group you would like to activate DNS Change detection for. In the search box, you can search for the Group you would like to activate DNS change detection for.

   OR

   On the main Dashboard page, we will also list the Groups you are a member of. You can also use the 'View All Groups' link on the navigation bar to view all of the groups you are a member of

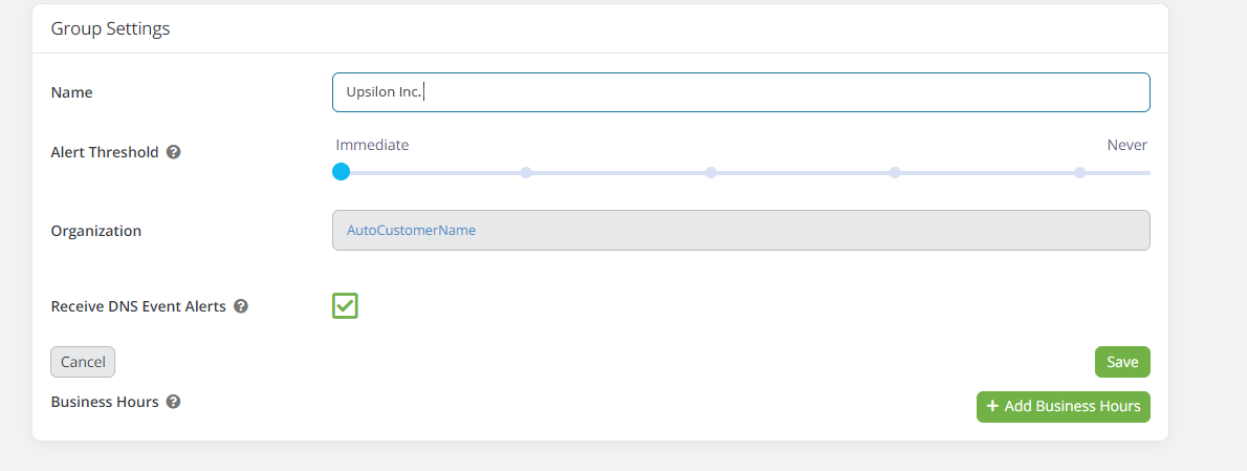
2. Once you navigate to the Group page, there should be a component called 'Group Settings.'

Select 'Receive DNS Event Alerts'

3. In the 'Settings' component, hit the 'Edit' button. If you do not see this button, contact the iStatus Support Team.

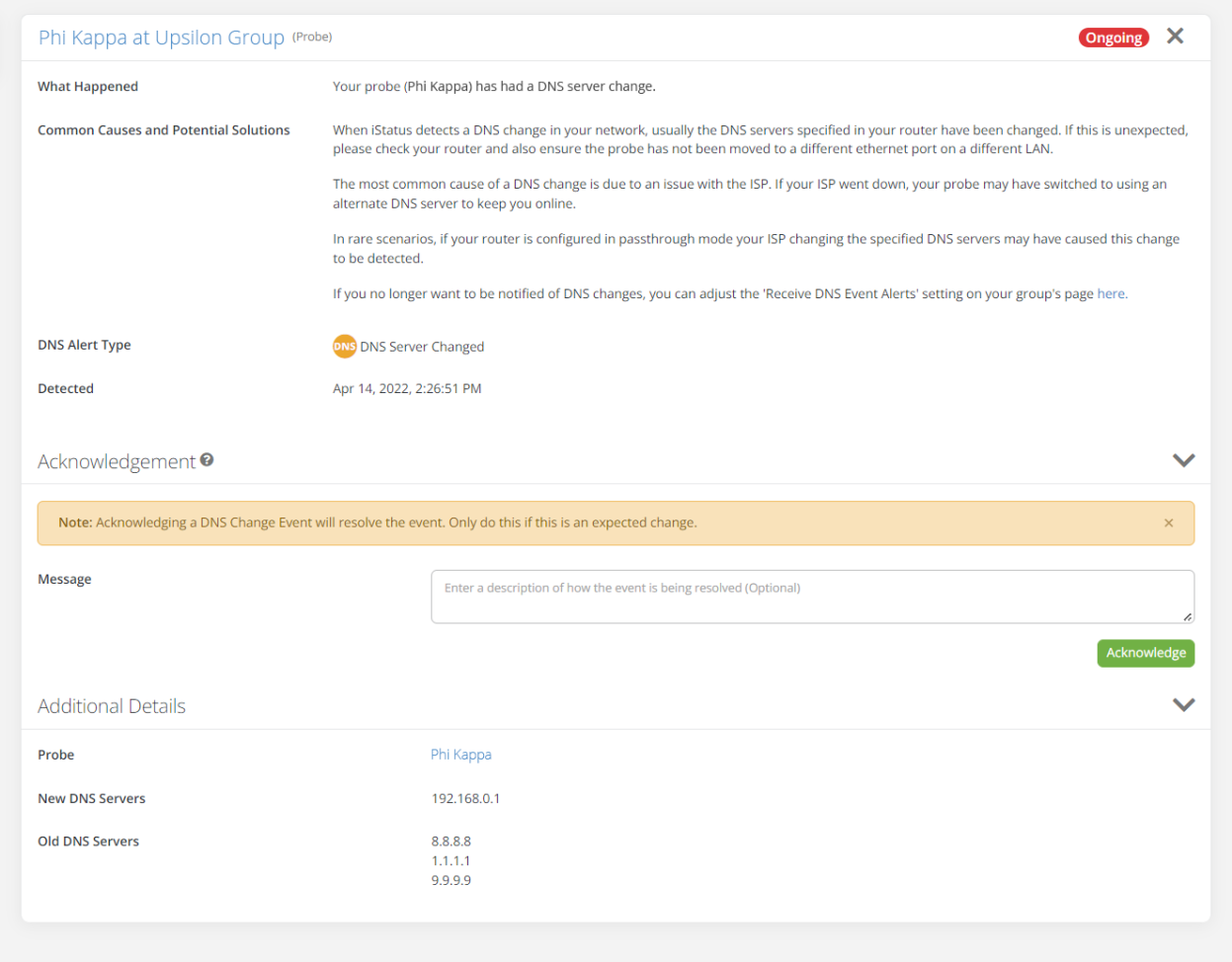
The  Provides an explanation of each setting.

4. Check 'Receive DNS Event Alerts' – this will allow iStatus to start tracking DNS changes on this selected Group's network(s).



Hit 'Save.'

That's it! You're set to receive alerts whenever a probe detects a DNS change in your locations in this Group.



A DNS change event will look like this – you can acknowledge and resolve the event by hitting acknowledge (and providing an optional message)