

## iStatus DDLD<sup>™</sup> Setup Guide

#### About iStatus Dynamic Data Leak Detection

iStatus DDLD<sup>™</sup> is used to test targets that should not be reachable to indicate potential misconfiguration or security risks to the network. When used in combination with iStatus NPM (Network Performance Monitoring), iStatus probes can run tests to verify that network security is air-tight.

For example, if you want to drop all outbound HTTP requests, you can set up one or more DDLD targets using HTTP. In this situation, DDLD then makes an HTTP-Get request which should always fail if the ACLs or firewall rules are properly blocking HTTP. In the event that the request is fulfilled, DDLD will generate a security event and send an alert email, indicating that a DDLD (data leak event) has occurred. DDLD can run these tests against LAN targets, VPN targets, Internet targets, or any combination thereof.

# This brief guide will show you how to set up DDLD targeting. Feel free to use the bookmarks to jump to your deseired section, such as DDLD Templating.

\*NOTE: DDLD is an integrated component to the NPM iStatus feature – the two features share license allocations for network targets. Thus, the following guide is very similar/mirrors the NPM setup guide. To purchase additional network target licenses, please get in touch with an Akative Sales Representative at <u>Sales@Akative.com</u>.

### **Assigning Licensing**

#### NOTE: A Group must have available licenses assigned to it before you can create targets or a template.

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

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

Make sure that NPM (in the right top corner of the License Management box) is underlined. From here you can assign licensing from your pool to each Group in iStatus, as well as connect an existing NPM/DDLD template (NPM/DDLD templating is shared as the features are cointegrated). You can view how many licenses you have purchased and applied.

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

<b>i</b> Status				
shboard > Organizations • > Licensing				
BC INC.				
Summary Licensing Templating Contacts & Notific	ations Organization Probes Billing			
icense Management For Organization: NPM @				NPM ArpWatch
This organization currently has 0 of 10 NPM licenses in use	Click here to get more.			_
This organization currently has 0 NPM licenses reserved fo Search	r this subscription (Unusable by the group).			
NAME	LICENSES	CONNE	CTED TEMPLATE	
Customer A	0	Edit Licenses None		Edit
	0 of 10 organiz groups	ation licenses allocated to		
	Showing 1 to 1 of 1	evious 1 Next >	Results per page: 10 V	



## Add DDLD Targets

1. Once you have applied your NPM/DDLD licensing, you may add DDLD targets to your Timeline View page. From your Timeline View, select the probe that you wish to monitor DDLD from by clicking into that probe (You may need to scroll down to the Probe Overview box to select your location's probe).

Search	Show Filters	
Online NPM Probe		
Probe Owner: M. Johnson		
Connections	۰۵. Categories	
🕑 Primary - 198.51.100.19 🥊	Common ICMP Targets	
Eailover - 203 0 113 254		

2. Scroll down on your probe page and in the NPM Categories Overview, click the green button that says Create an NPM Category. (Reminder: DDLD is an integration of NPM)

Uptime: 99.93%	Downtime: 0.07%	Failed Over: 0.01%	SD-WAN Active: 0%	Issues	Event Bundle	No Data
mmary NPM - ArpWatch	Pinpoint					
Primary - 198.51.100.1 Online for 6 days 15 hours	9 ✓ ConnectionValidation™	>	NPM Categories Overvie	w 0	2 out of 9 targets monitored	Create an NPM Categ
Failover - 203.0.113.25 Online for 6 days 18 hours	54 ✓ ConnectionValidation™	>	Partial Common ICMP	Targets @Organization	Templated	
work Events ArpWatch Even	ts NPM Events	Export 🗸	Delete		Angua - 9/9/9/9	
			Carlos			(

Name your category accordingly (i.e. DDLD for what type of network targets will be in that group (LAN, WAN, Cloud Applications., etc.)).

in the categories over the		a sur or a targeta manitorea	Concession,
Search		Show Filters	
Category Name	Example		
Cancel			Create
Partial Common ICMP	Targets Organization T	emplated	
		Quad9 - 9.9.9.9	
Google DNS - 8.8.8.8			



3. Now that you've successfully made an NPM Category, navigate to that category's page by using the NPM tab and clicking the DDLD targets' Category.

NPM Probe	>						
te: Scale bars are ≈1 day apart	02/04	02/05	02/06	02/07	02/08	02/09	02/10
gs Event Count Location (IP Address)							
	Displayed statistics are based on	this probe. Applying filters	or selecting specific ti	melines will change these values. To sh	now statistics for all visible til	melines <u>click here.</u>	
Optime: 99.93%	Downtime: 0.07%	Failed Ove	r: 0.01%	SD-WAN Active: 0%	Issues	Event Bundle	No Data
Summary NPM <del>-</del> ArpWatch	Pinpoint						
Common ICMP 1	argets						
Primary - 198.51.100.1	ConnectionValidation**		>	NPM Categories Overvie	ew O	2 out of 9 targets monitored	Create an NPM Catego
Online for 6 days 15 hours			,				

4. From this page, locate the Network Targets Overview box (you may need to scroll down). In this box, click the green 'Create a Network Target' button and add some LAN, WAN, Cloud Applications, or Protocols that you'd like to monitor for data leaks.

Search T Show	v Filters
Compare Network Target Performance	
Congested Google DNS - 8.8.8.8 👖 @ Organiza	ation Templated
IP Address: 8.8.8.8	
Protocol: Ping (ICMP)	
Average Latency: 257 ms (Last 10 Minutes)	
Last Status Code: 20: OK (Success) 🚱	
Delete	II Pause Edit
Delete Online Quad9 - 9.9.9.9	II Pause Edit
Online Quad9 - 9.9.9.9    @ Organization Tempi	II Pause Edit
Delete Online Quad9 - 9.9.9.9    @ Organization Templ IP Address: 9.9.9.9 Protocol: Ping (ICMP)	II Pause Edit
Delete Online Quad9 - 9.9.9.9     Organization Templ IP Address: 9.9.9.9 Protocol: Ping (ICMP) Average Latency: 14 ms (Last 10 Minutes)	II Pause Edit
Delete Online Quad9 - 9.9.9.9     Organization Tempi IP Address: 9.9.9.9 Protocol: Ping (ICMP) Average Latency: 14 ms (Last 10 Minutes) Last Status Code: 20: OK (Success) ?	II Pause Edit
Delete Online Quad9 - 9.9.9.9  Organization Templ Protocol: Ping (ICMP) Average Latency: 14 ms (Last 10 Minutes) Last Status Code: 20: OK (Success)	II Pause Edit



5. Fill out the fields with the target information and click the Create button. Note: make sure to select 'Dynamic Data Leak Detection' for the Target Type.

Network Targets Overview 🚱	2 out of 20 targets monitored Create a Network Target
You are creating this target outside of NPM Templating. Using NPM Templat and manage the same target among multiple probes, and opens up features NPM Templating to create this and other targets. You can find the NPM Tem	ing to create your targets allows us to automatically create such as timeline filtering by Target. Please consider using plating component on your Group's page.
We store all data for up to 90 days. After 90 days, detailed data is compresse The threshold of sending alerts and the recipients of alerts can be adjusted (	ed into 10-minute averages for NPM targets.
threshold to only receive alerts for issues that have been happening for 15 n You have 4 license(s) left out of 4. Creating a target will use a license. Click he	ninutes or turn them off entirely for this category. ere to upgrade your plan and monitor more network targets.
Network Target Name *	
Station 1	
Monitoring Probe	
Location 1	
Category	
Work Station Monitoring	
Protocol * What should I select?	
Ping (ICMP)	~
Hostname or IP Address *	
192.168.11.10	
This entry will be saved as an IP Address.	
* - Indicates a required field.	
Cancel	Create

6. Once targets are created, they will appear on the timeline under their NPM/DDLD Category. DDLD graphs for each target will also be created and will appear below the timeline. Note: it takes a few minutes before data appears on the timeline and DDLD graphs. Once data starts appearing you'll be able to observe data leaks that can indicate things like misconfigurations and network security vulnerabilities/risks.





## **Creating a Template**

2. 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.

Once created, click on create, select edit down below to change settings, and set up your DDLD Targeting. There are several settings here to set up deployment of the DDLD Template you have

created. The 🕜 explains each setting.

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

board > Organizations → > Templating BC INC. mmary Licensing Templating Contacts & Notifications Organization Probes Billing emplate Management for ABC INC. @	
mmary Licensing Templating Contacts & Notifications Organization Probes Billing	
mmary Licensing Templating Contacts & Notifications Organization Probes Billing	
emplate Management for ABC INC. @	
	Organization & View Group Templating
rrent Template: Default 🖋 ABC Standard Template	~
)elete	Create a new Template
efault NPM Configuration 😧	(NPM) 1.
is Organization has used 0 out of 10 NPM licenses. 🚱 ere are currently <b>0</b> NPM templated items in this Configuration out of a total of <b>10</b> 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 🔞	
Jse 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
ancel	Save



## **Setting up DDLD Targets**

3. To set up your targets, Click 'Create a new DDLD Template'.

Then select 'Create a new Category.'

In the example, ABC Inc. has created two Categories, one Internal Target, and one External Target

Summary Licensing Templating Contact	& Notifications Organization Pro	obes Billing	
Femplate Management for ABC INC. @			Organization 🔗 View Group Templating
Current Template:	Default 🖋 🛛 ABC :	Standard Template	~
Delete			Create a new Template
Default NPM Configuration <b>2</b>			NPM 🕹
his Organization has used 0 out of 10 NPM licer	ses. 😧		
his Organization has used 0 out of 10 NPM licer here are currently 0 NPM templated items in th Changes made here will affect and update Configuration will be given these target cha	ses. <b>©</b> s <i>Configuration out of a total of <b>10</b> N all of the iStatus<sup>®</sup> Probes that are u Inges.</i>	IPM templated items using this template on save. This means that any probe	that uses this template on any
this Organization has used 0 out of 10 NPM licer there are currently 0 NPM templated items in the Changes made here will affect and update Configuration will be given these target cha Femplate Name:	ses. <b>@</b> s Configuration out of a total of <b>10</b> N all of the iStatus <sup>®</sup> Probes that are u inges.	IPM templated items using this template on save. This means that any probe	that uses this template on any
this Organization has used 0 out of 10 NPM licer there are currently 0 NPM templated items in thi Changes made here will affect and update Configuration will be given these target cha Template Name:	ses. <b>@</b> s Configuration out of a total of <b>10</b> N all of the iStatus <sup>®</sup> Probes that are u inges. NPM Default Targets	iPM temploted items using this template on save. This means that any probe	that uses this template on any
This Organization has used 0 out of 10 NPM licer There are currently 0 NPM templated items in this Changes made here will affect and update Configuration will be given these target changes Template Name: Internal Target I I Create a new Network Target Create a new Network Target	ses.    seconfiguration out of a total of 10 N all of the iStatus <sup>®</sup> Probes that are u inges.  NPM Default Targets	IPM templated items using this template on save. This means that any probe	that uses this template on any
This Organization has used 0 out of 10 NPM licer There are currently 0 NPM templated items in thi Changes made here will affect and update Configuration will be given these target cha Template Name: Internal Target $\checkmark$ 1 Create a new Network Target Create a new Network Target Create a new Network Target	ses. <b>@</b> s Configuration out of a total of <b>10</b> N all of the iStatus <sup>®</sup> Probes that are u inges. NPM Default Targets	IPM templated items using this template on save. This means that any probe	that uses this template on any
This Organization has used 0 out of 10 NPM licer There are currently 0 NPM templated items in the Changes made here will affect and update Configuration will be given these target cha Template Name: Internal Target  Internal Target Create a new Network Target Create a new Network Category Create a new Network Category	ses.    seconfiguration out of a total of 10 N all of the iStatus <sup>®</sup> Probes that are u inges.  NPM Default Targets	IPM templated items using this template on save. This means that any probe	that uses this template on any
This Organization has used 0 out of 10 NPM licer There are currently 0 NPM templated items in thi Changes made here will affect and update Configuration will be given these target cha Template Name: ★ Internal Target	ses. s Configuration out of a total of 10 N all of the iStatus <sup>®</sup> Probes that are u inges. NPM Default Targets	iPM templated items using this template on save. This means that any probe	that uses this template on any

Once the 'Category' is created, you can define the DDLD target by selecting 'Create a new Network Target;' you can define the target by Ping(ICMP) or HTTP(HEAD).



#### In the example, ABC Inc. Has set a target using Ping(ICMP) for a local Access Point

		Template Management for Auto Group I	Name 🔞	Group View Organization Templating
Dashboard		Select a Group:	Auto Group Name	~
Insight Manager	1			
Register a Probe		Current Template:	Default Default Template For Group: Keith	's Group
Organizations	~	Delete		Go To Group
Summany	Ť			
Licensing		Default NPM Configuration For Group: K	eith's Group 🔞	(NPM) 🟦
Templating		This Group has used 9 out of 1500 NPM licenses.	9	
Contacto & Notificatio		There are currently 3 NPM templated items in this	Configuration out of a total of <b>20</b> NPM templated items	
Probe Management	115	Changes made here will affect and update a on any Configuration will be given these tar	II of the iStatus <sup>®</sup> Probes that are using this template on s get changes.	save. This means that any probe that uses this template
Billing		Tomplate Name:	Lippamed Template	
Audit Logs		remplate Name:	Unnamed remplate	
		-& New Templated Category		
Developer		New Templated Category     New Local PC - 192.168.1.2 - 192.168.1.3     Prehably a mabile device 103.168.1.3	2 (PING) (Default)	
Developer Support Kitchen		New Templated Category     New Local PC - 192.168.1.2 - 192.168.1.3     Probably a mobile device - 192.168.1.3     We store all data for up to 90 days. After     The threshold of sending alerts and the i     to only receive alerts for issues that have	2 PWG (Default) 192,168.1.3 PMG (Default) 90 days, detailed data is compressed into 10-minute ave ecipients of alerts can be adjusted on the Category page been happenping for 15 minutes or turn them off entirely	erages for NPM targets. 2. For example, you can change the alert threshold for this category.
Developer Support Kitchen April Billing Cycle ends 5/1/2022 <b>@</b> 16 days remai	ining	<ul> <li>New Templated Category</li> <li>New Local PC - 192.168.1.2 - 192.168.1.3</li> <li>Probably a mobile device - 192.168.1.3</li> <li>We store all data for up to 90 days. After The threshold of sending alerts and the to only receive alerts for issues that have Upon clicking create and saving your tem Click here to upgrade your plan and mor</li> <li>Network Target Name *</li> </ul>	2 PWG <b>Default</b> 192.168.1.3 PWG <b>Default</b> 90 days, detailed data is compressed into 10-minute ave ecipients of alerts can be adjusted on the Category page 4 been happening for 15 minutes or turn them off entirel aplate, a target will be created and a license will be used itor more network targets.	rrages for NPM targets. 2. For example, you can change the alert threshold y for this category. for each target that is created under each probe
Developer Support Kitchen April Billing Cycle ends 5/1/2022 • 16 days remai	ning	<ul> <li>New Templated Category         <ul> <li>New Local PC - 192.168.1.2 - 192.168.1.3</li> <li>Probably a mobile device - 192.168.1.3</li> </ul> </li> <li>We store all data for up to 90 days. After         <ul> <li>The threshold of sending alerts and the to only receive alerts for issues that have</li> <li>Upon clicking create and saving your ten Click here to upgrade your plan and mor</li> </ul> </li> <li>Network Target Name *         <ul> <li>Protocol * What should I select?</li> </ul> </li> </ul>	2 (PVG) (Default) 192.168.1.3 (PVG) (Default) 90 days, detailed data is compressed into 10-minute ave ecipients of alerts can be adjusted on the Category page is been happening for 15 minutes or turn them off entirel uplate, a target will be created and a license will be used itor more network targets.	erages for NPM targets. 2. For example, you can change the alert threshold y for this category. for each target that is created under each probe
Developer Support Kitchen April Billing Cycle ends 5/1/2022 • 16 days remain Organization Tour Request Support	ining	<ul> <li>New Templated Category         <ul> <li>New Local PC - 192.168.1.2 - 192.168.1.3</li> <li>Probably a mobile device - 192.168.1.3</li> </ul> </li> <li>We store all data for up to 90 days. After         The threshold of sending alerts and the         to only receive alerts for issues that have         Upon clicking create and saving your ten         Click here to upgrade your plan and more         Network Target Name *         <ul> <li>Protocol * What should I select?</li> <li>Target Type * What should I select?</li> </ul> </li> </ul>	2 PING Default 192.168.1.3 PING Default 90 days, detailed data is compressed into 10-minute ave ecipients of alerts can be adjusted on the Category page been happening for 15 minutes or turn them off entirel uplate, a target will be created and a license will be used itor more network targets.	erages for NPM targets. Eror example, you can change the alert threshold y for this category. for each target that is created under each probe
Developer Support Kitchen April Billing Cycle ends 5/1/2022 ng Cycle 16 days remail Organization Tour Request Support f a 2022 Akativation	ining	New Templated Category  New Local PC - 192,168.1.2 - 192,168.1.3 Probably a mobile device - 192,168.1.3 We store all data for up to 90 days. After The threshold of sending alerts and the to only receive alerts for issues that have Upon clicking create and saving your ten Click here to upgrade your plan and model. Network Target Name * Protocol * What should I select? Target Type * What should I select?	2 PMG <b>Extant</b> 192.168.1.3 PMG <b>Extant</b> 90 days, detailed data is compressed into 10-minute ave ecipients of alerts can be adjusted on the Category page 1 been happening for 15 minutes or turn them off entirel aplate, a target will be created and a license will be used to itor more network targets.	erages for NPM targets. 2. For example, you can change the alert threshold y for this category. for each target that is created under each probe
Developer Support Kitchen April Billing Cycle ends 5/1/2022 16 days remain Organization Tour Request Support f © 2022 Akative <sup>27</sup> All Rights Reserved. r U.S. Patent Information, status.com/IP, Patents Pendid	see	New Templated Category  New Local PC - 192,168,1.2 - 192,168,1.3 Probably a mobile device - 192,168,1.3 We store all data for up to 90 days. After The threshold of sending alerts and the to only receive alerts for issues that have Upon clicking create and saving your tenclick here to upgrade your plan and moto click here to upgrade your plan and moto click here to upgrade your plan and moto the term of term of the term of t	2 PDG Control (Control (Contro) (Control (Contro) (Control (Contro) (Contro	erages for NPM targets.  2. For example, you can change the alert threshold y for this category. for each target that is created under each probe

Once you have created your targets 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).	Ľ		
Search			
NAME	LICENSES	CONNECTED TEMPLATE	
Customer A	4 Edit Licenses	Select a Configuration ABC Standard Template Cancel	► Save
	4 of 10 organization licenses allocated to groups		
Showing 1 to 1 of 1	<pre> Previous 1 Next &gt;</pre>	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.

#### **Defining a Probe DDLD Target**

4. If you have a Template that allows for Groups to define their own targets or no template assigned to a Group and have an extra DDLD targeting license for the Group, then a target can be defined on the Probe.

Click on the 'Dashboard' and either search for or select.

In The example, ABC Inc. Has a probe at location 1 for Customer A.



Once at the probe, you can 'Create a new Category' for DDLD targets under 'Create an NPM Category.' (Reminder again, NPM/DDLD functionality is shared as the features are co-integrated).



In the example ABC Incs, Customer A is defining a new category of Work Stations; because we applied the Template at the Organization level, two targets have already been defined.

NPM Categories Overview 🚱		2 out of 20 targets monitored	Create an NPM Category
Search			
Category Name	Work Station Monitoring		
Cancel			Create
Unmonitored External Target			
Network Targets			
Google - https://www.google.com/			
Delete			NPM Diagnostics
Unmonitored Internal Target			
Network Targets			
🔕 Access Point 1 - 192.168.10.101			
Delete			NPM Diagnostics

- 5. Once the 'Category' is created, select the Category to set up the target.
- 6. Then create a 'Network Target' of your choosing.



#### In the example, Customer A set up Targeting for Station 1.

Network Targets Overview 🚱	7 out of 10 targets monitored Create a Network Target
You are creating this target outside of NPM Templating. Using NPM Templating to create your targets allows us to automatically create and manage the same target among multiple probes, and opens up features such as timeline filtering by Target. Please consider using NPM Templating to create this and other targets. You can find the NPM Templating component on your Group's page.	
We store all data for up to 90 days. After 90 days, detailed data is compres	ssed into 10-minute averages for NPM targets.
The threshold of sending alerts and the recipients of alerts can be adjusted change the alert threshold to only receive alerts for issues that have been for this category.	d on the Category page. For example, you can happening for 15 minutes or turn them off entirely
You have 913 license(s) left out of 1000. Creating a target will use a license more network targets.	e. Click here to upgrade your plan and monitor
Network Target Name *	
Station 1	
Monitoring Probe	
Dev. Probe 3	
Category	
3252532	
Protocol * What should I select?	
Ping (ICMP)	~
Hostname or IP Address *	
192.168.11.10	
This entry will be saved as an IP Address.	
Target Type * What should I select?	
Dynamic Data Leak Detection	~
* - Indicates a required field.	
Cancel	Create

DDLD Targets at the Probe level can be set up by anyone who has Manager access to the Group that has that probe.