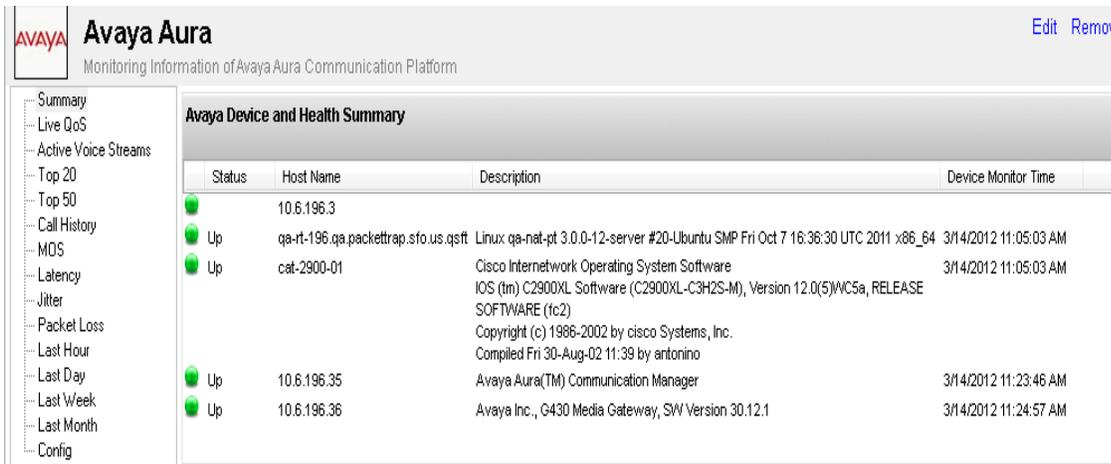


## What's New in PacketTrap MSP 6.2?

### Avaya Monitoring Support

As a network professional with increased responsibility and continually evolving technology, you are most likely challenged of how to effectively monitor VoIP systems. You want to ensure that you have adequate visibility into how your IT infrastructure and VoIP systems are working together and to do this, you may be using various different point tools to manage and monitor them. Most VoIP implementations often suffer from dropped calls, poor voice quality, and other issues so how do you create the most efficient VoIP monitoring environment, enhance user satisfaction and meet SLAs? PacketTrap MSP now provides in-depth and detailed monitoring of VoIP quality metrics like MOS, Jitter, packet-loss, delay, network utilization and comprehensive set of reports and alerts on all VoIP related voice metrics.



**Avaya Aura** Edit Remove

Monitoring Information of Avaya Aura Communication Platform

- Summary
- Live QoS
- Active Voice Streams
- Top 20
- Top 50
- Call History
- MOS
- Latency
- Jitter
- Packet Loss
- Last Hour
- Last Day
- Last Week
- Last Month
- Config

#### Avaya Device and Health Summary

Status	Host Name	Description	Device Monitor Time
Up	10.6.196.3		
Up	qa-rt-196.qa.packettrap.sfo.us.qstf	Linux qa-nat-pt 3.0.0-12-server #20-Ubuntu SMP Fri Oct 7 16:36:30 UTC 2011 x86_64	3/14/2012 11:05:03 AM
Up	cat-2900-01	Cisco Internetwork Operating System Software IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 12.0(5)WC5a, RELEASE SOFTWARE (fc2) Copyright (c) 1986-2002 by cisco Systems, Inc. Compiled Fri 30-Aug-02 11:39 by antonino	3/14/2012 11:05:03 AM
Up	10.6.196.35	Avaya Aura(TM) Communication Manager	3/14/2012 11:23:46 AM
Up	10.6.196.36	Avaya Inc., G430 Media Gateway, SW Version 30.12.1	3/14/2012 11:24:57 AM



**Avaya Aura**

Monitoring Information of Avaya Aura Communication Platform

- Summary
- Live QoS
- Active Voice Streams
- Top 20
- Top 50
- Call History
- MOS
- Latency
- Jitter
- Packet Loss
- Last Hour
- Last Day
- Last Week
- Last Month
- Config

#### Call History

Last Hour

Start Time	Duration	Caller Phone	Callee Phone	MOS	Jitter	Latency	Packet Loss
3/14/2012 11:36:00 AM	0:01:00	1003	1001	4.99	0 ms	2 ms	0.0000000%
3/14/2012 11:35:00 AM	0:01:30	1003	1002	4.99	0 ms	1 ms	0.0000000%
3/14/2012 11:33:00 AM	0:01:42	1001	1003	4.98	0 ms	2 ms	0.0000000%
3/14/2012 11:31:00 AM	0:02:18	1001	1002	4.86	0 ms	1483 ms	0.0000000%
3/14/2012 11:26:00 AM	0:01:18	1002	1001	4.99	0 ms	0 ms	0.0000000%
3/14/2012 11:24:00 AM	0:00:48	1002	1003	4.59	1581 ms	0 ms	0.0000000%

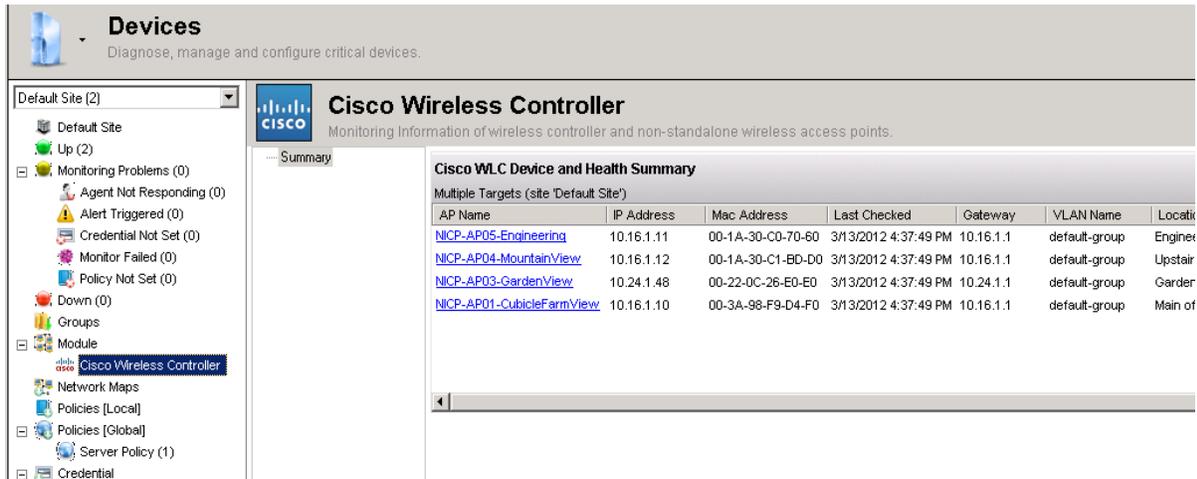
#### Call History

Last Day

Start Time	Duration	Caller Phone	Callee Phone	MOS	Jitter	Latency	Packet Loss
3/14/2012 11:36:00 AM	0:01:00	1003	1001	4.99	0 ms	2 ms	0.0000000%
3/14/2012 11:35:00 AM	0:01:30	1003	1002	4.99	0 ms	1 ms	0.0000000%
3/14/2012 11:33:00 AM	0:01:42	1001	1003	4.98	0 ms	2 ms	0.0000000%
3/14/2012 11:31:00 AM	0:02:18	1001	1002	4.86	0 ms	1483 ms	0.0000000%
3/14/2012 11:26:00 AM	0:01:18	1002	1001	4.99	0 ms	0 ms	0.0000000%
3/14/2012 11:24:00 AM	0:00:48	1002	1003	4.59	1581 ms	0 ms	0.0000000%

## Cisco Wireless Controller Monitoring

Devices like Cisco wireless controllers are being used more and more to manage all the wireless access points, instead of managing individual access points. PacketTrap MSP now has the capability to provide the deep monitoring stats that you are used to at the access point level through a central wireless controller. Out of box monitoring includes: health status, access points managed, their performance, and who is connected to what device.



**Devices**  
Diagnose, manage and configure critical devices.

**Cisco Wireless Controller**  
Monitoring Information of wireless controller and non-standalone wireless access points.

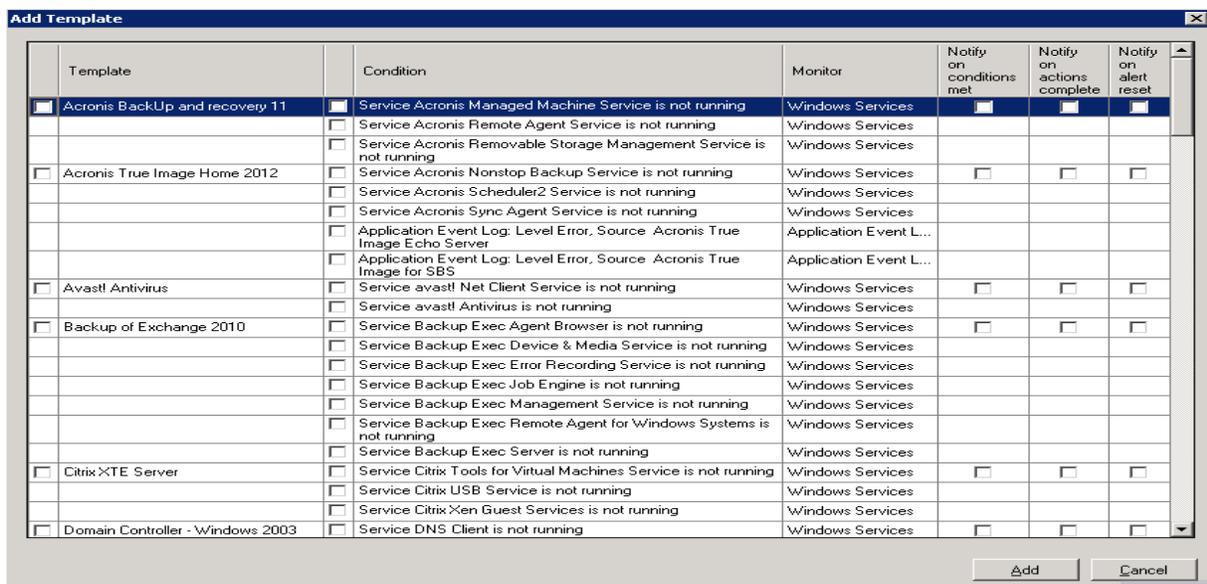
Summary

**Cisco WLC Device and Health Summary**  
Multiple Targets (site 'Default Site')

AP Name	IP Address	Mac Address	Last Checked	Gateway	VLAN Name	Location
<a href="#">NICP-AP05-Engineering</a>	10.16.1.11	00-1A-30-C0-70-60	3/13/2012 4:37:49 PM	10.16.1.1	default-group	Engineer
<a href="#">NICP-AP04-MountainView</a>	10.16.1.12	00-1A-30-C1-BD-D0	3/13/2012 4:37:49 PM	10.16.1.1	default-group	Upstair
<a href="#">NICP-AP03-GardenView</a>	10.24.1.48	00-22-0C-26-E0-E0	3/13/2012 4:37:49 PM	10.24.1.1	default-group	Gardner
<a href="#">NICP-AP01-CubicleFarmView</a>	10.16.1.10	00-3A-98-F9-D4-F0	3/13/2012 4:37:49 PM	10.16.1.1	default-group	Main of

## Out of Box Application Monitoring Templates

Ease of use and out of box configuration is a critical foundation piece for PacketTrap MSP. This exciting new feature automatically groups monitors, alerts, and actions to completely monitor and manage applications. The one-click setup dramatically simplifies configuration time and allows you to spend your time on other projects. You can use a monitoring template across global policies, site policies, or on a particular device.



**Add Template**

Template	Condition	Monitor	Notify on conditions met	Notify on actions complete	Notify on alert reset
<input checked="" type="checkbox"/> Acronis BackUp and recovery 11	<input checked="" type="checkbox"/> Service Acronis Managed Machine Service is not running	Windows Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> Service Acronis Remote Agent Service is not running	Windows Services			
	<input type="checkbox"/> Service Acronis Removable Storage Management Service is not running	Windows Services			
<input type="checkbox"/> Acronis True Image Home 2012	<input type="checkbox"/> Service Acronis Nonstop Backup Service is not running	Windows Services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/> Service Acronis Scheduler2 Service is not running	Windows Services			
	<input type="checkbox"/> Service Acronis Sync Agent Service is not running	Windows Services			
	<input type="checkbox"/> Application Event Log: Level Error, Source: Acronis True Image Echo Server	Application Event L...			
	<input type="checkbox"/> Application Event Log: Level Error, Source: Acronis True Image for SBS	Application Event L...			
<input type="checkbox"/> Avast! Antivirus	<input type="checkbox"/> Service avast! Net Client Service is not running	Windows Services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/> Service avast! Antivirus is not running	Windows Services			
<input type="checkbox"/> Backup of Exchange 2010	<input type="checkbox"/> Service Backup Exec Agent Browser is not running	Windows Services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/> Service Backup Exec Device & Media Service is not running	Windows Services			
	<input type="checkbox"/> Service Backup Exec Error Recording Service is not running	Windows Services			
	<input type="checkbox"/> Service Backup Exec Job Engine is not running	Windows Services			
	<input type="checkbox"/> Service Backup Exec Management Service is not running	Windows Services			
	<input type="checkbox"/> Service Backup Exec Remote Agent for Windows Systems is not running	Windows Services			
	<input type="checkbox"/> Service Backup Exec Server is not running	Windows Services			
<input type="checkbox"/> Citrix XTE Server	<input type="checkbox"/> Service Citrix Tools for Virtual Machines Service is not running	Windows Services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/> Service Citrix USB Service is not running	Windows Services			
	<input type="checkbox"/> Service Citrix Xen Guest Services is not running	Windows Services			
<input type="checkbox"/> Domain Controller - Windows 2003	<input type="checkbox"/> Service DNS Client is not running	Windows Services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add Cancel

## One Click Help and Tutorial Videos

IT infrastructure management can be difficult and complex. Our goal is to provide you with resources at your fingertips so that you are able to find answers to your questions and not spend a lot of time looking for where to find the answer. We've taken a leap forward in 6.2 with a newly launched knowledgebase that is directly linked from features and configuration screens. With a single-click you can peruse topics in the new PacketTrap MSP Knowledgebase. In addition, you can find feature-specific help from anywhere in the product.

Welcome to the PacketTrap MSP Knowledgebase!

### PacketTrap MSP Knowledgebase

Need help? Click a resource below to learn more about PacketTrap MSP.

  
 Antivirus

  
 Configuration

  
 Dashboards

  
 Getting Started

  
 Integration Partners

  
 Managing Devices

  
 Monitors & Alerts

  
 Network Maps

  
 PacketTrap PSA

  
 Remote Access

  
 Reports

  
 Traffic Analysis

  
 VoIP

Do not show this dialog again. Close

### Server Policy

Smart policy used for monitoring all typical linux, unix and window servers.

Enabled: True ▾

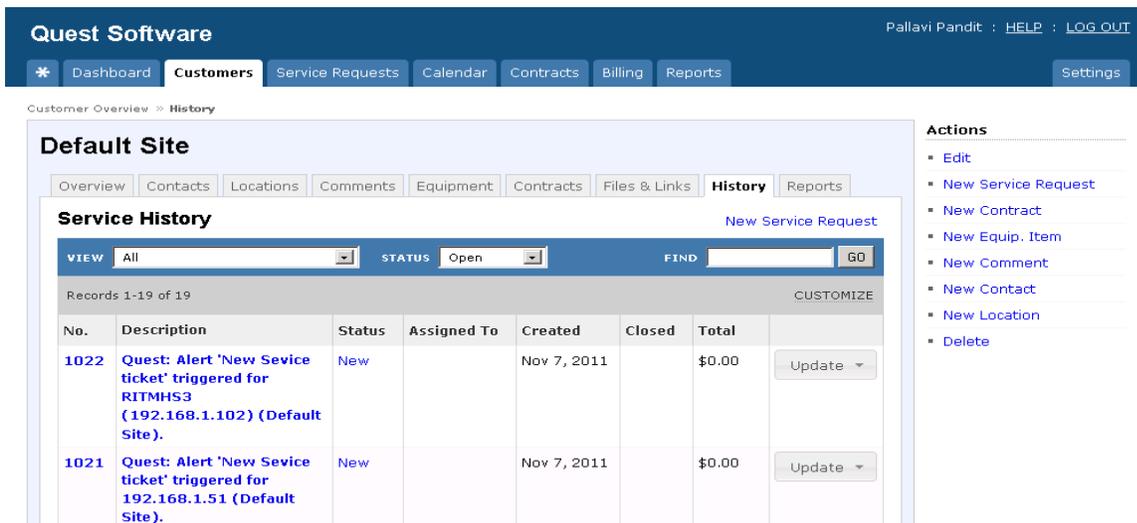
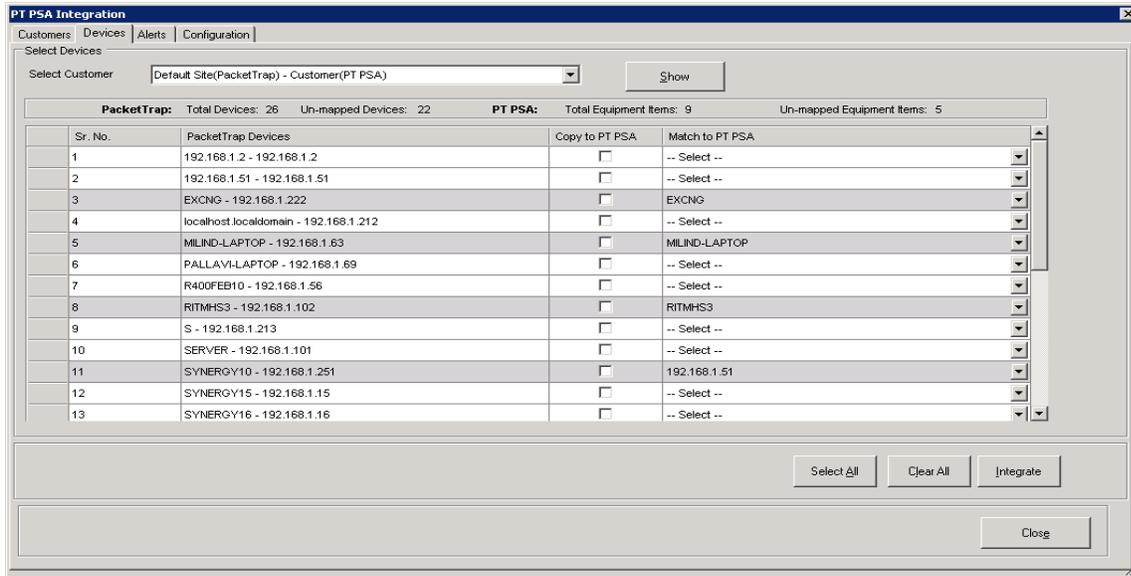
Device Members | Monitors | Custom Monitors | **Alerts** | Scheduled Actions | Blackout Schedule

+ Add alert
📄 Edit alert
✖ Remove alert
🔄 Restore default
+ Add Template
?

Enabled	From policy	Name
<input checked="" type="checkbox"/>		Agent Polling Smart Alert
<input checked="" type="checkbox"/>		Logical Disk Free Percent Smart Alert
<input checked="" type="checkbox"/>		Memory Smart Alert
<input checked="" type="checkbox"/>		Network Interface Traffic Percent Smart Alert
<input checked="" type="checkbox"/>		Ping Latency Smart Alert
<input checked="" type="checkbox"/>		Ping PacketLoss Smart Alert
<input checked="" type="checkbox"/>		Processor Smart Alert

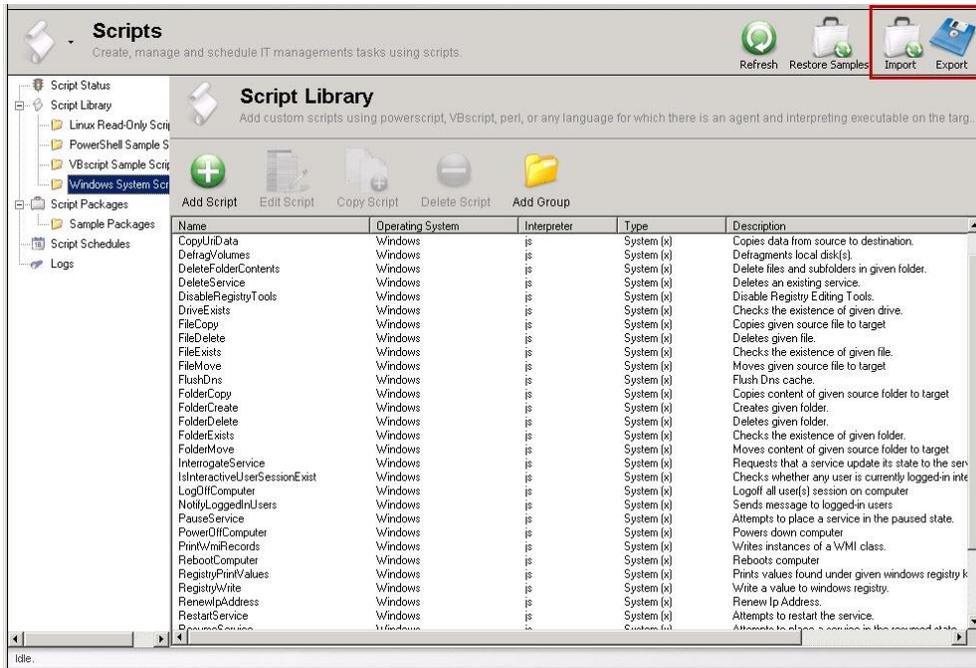
## PacketTrap PSA Integration

Whether you are using spreadsheets and sticky notes or clunky software, PacketTrap PSA will transform your service management into an efficient—dare we say enjoyable—process. Manager Service Providers will now benefit from significant time savings and see a dramatic increase in profitability. The PacketTrap MSP 6.2 release has seamless integration into PacketTrap PSA, creating a single workflow and solution to meet your business needs.



## Script Import / Export Feature

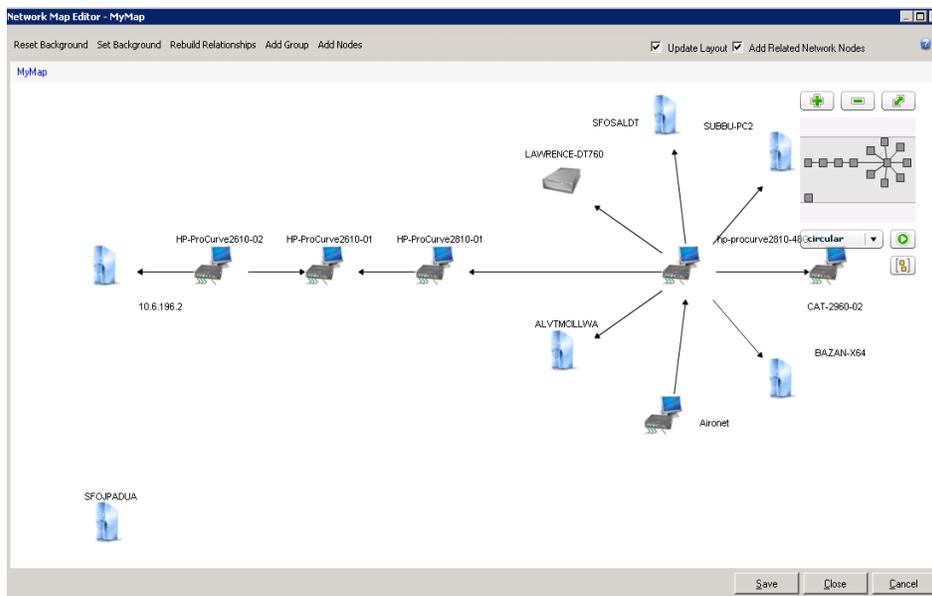
You can now import and export a large number of scripts to/from PacketTrap MSP. Scripts that you select to import or export must be formatted in XML.



## Network Map Additions

Visual representation of the IT infrastructure is a quick and easy way to identify the root cause of many problems. This release of PacketTrap MSP has two new improvements for Network Maps:

1. Ability to show or not show connected devices for the devices already on the map. For example, you can now choose to not show a core switch that is connected to a device.
2. Update the map layout when devices are added or removed. You can drag and drop devices to specific areas on the map and they will not change unless you select this new option.



## **ConnectWise, TigerPaw, AutoTask Integration Enhancements**

There is a series of new improvements to the integration with popular PSA solutions. We understand how important it is to have a tightly integrated solution with our MSP industry partners.

### **Connectwise**

- Close Tickets on Return to Normal.
  - This feature provides PacketTrap MSP with the ability to stop a callback from ConnectWise. Currently, if the URL is properly configured in ConnectWise, then a PacketTrap alert is reset from ConnectWise if the conditions are matched. Through the use of a flag, PacketTrap avoids the resetting of alerts from ConnectWise. This flag has been added to the ConnectWise configuration.
- Add Acknowledgement
  - When a ticket is generated in ConnectWise, it is always acknowledged in PacketTrap. Through the use of a flag, the user has an option to specify whether or not the acknowledgement should be added when the ticket is added in ConnectWise. This flag has been added to the ConnectWise configuration
- PacketTrap MSP has been enhanced with the following configuration details:
  - Setup name - This is the name provided by the user while setting up the Management IT configuration. If the Setup Name is specified, then only the devices with the specified setup is integrated.
  - Solution name - This is the name provided by the user while setting up the Management IT configuration. If the Solution Name is specified, then only the devices with the specified solution is integrated.
  - Monitor alert board 1 - This routes all tickets to the designated service board if a monitor's alert action has been set up to send tickets to 'ConnectWise Ticket'. This is designed for internal monitors.
  - Monitor alert board 2 - The Monitor Alert Board 2 is the same as Monitor Alert Board 1 except that the monitor alert action needs to be set to 'ConnectWise Ticket 2'.
- Automatic Synchronization of the Clients after a Specified Time Interval.
  - In PacketTrap MSP, clients/companies are synchronized manually. An enhancement has been made through the use of a flag to synchronize the copied PacketTrap companies in ConnectWise after a specified time interval.
- See the mapped devices.
- Filter the Management IT setups for a selected company.

### **TigerPaw**

- Automatic Synchronization of the Clients after Specified Time Interval
  - In PacketTrap, clients/companies are synchronized manually. An enhancement has been made through the use of a flag to synchronize the PacketTrap companies in Tigerpaw after a specified time interval.
- The addition of callback functionality in Tigerpaw makes it simple for the user to reset alerts in PacketTrap from Tigerpaw for synchronized accounts at a specified time interval.
- Asset Polling / Asset Synchronization is the functionality by which the polled assets of the Tigerpaw application are synchronized with PacketTrap devices at a specified time interval.

## **AutoTask**

- Additional Configuration Settings
  - Device Integration
    - Serial Number
    - Location
    - VendorID
  - Ticket Integration
    - Ticket Source - Select the value to be assigned for the origin of tickets (e.g. Email or Website).
    - Due Date - Type the value (in hours) for when the tickets will be due. The ticket due date will be set as the original ticket creation time plus the number of hours that are configured by the user.
- Close Tickets on Return to Normal.
  - This feature provides PacketTrap with the ability to stop a callback from Autotask. Currently, if the URL is properly configured in Autotask, a PacketTrap alert is reset from Autotask if the conditions are matched. Through the use of a flag, PacketTrap avoids the resetting of alerts from Autotask. This flag has been added in the Autotask configuration.
- Add Acknowledgement
  - When a ticket is generated in Autotask, it is always acknowledged in PacketTrap. Through the use of a flag, the user has an option to specify whether or not the
  - acknowledgement should be added when the ticket is added in Autotask. This flag has been added in the Autotask configuration.
- Ability to Configure Computer User Defined Fields and Network Device User Defined Fields. Data for all user defined fields in Autotask can be passed at the time of device/account integration.
- Ability to Map Computer/Device Name to Reference Number. If selected, the computer/device name will be switched to the reference number.

For additional information regarding PacketTrap solutions, go to [www.packettrap.com](http://www.packettrap.com) or contact [sales@packettrap.com](mailto:sales@packettrap.com)