ReliaTel

New Features and Enhancements

Release 6.2.0

TONE

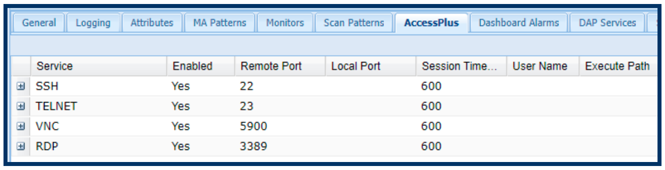
Functionality Added to Data Acquisition Points

Functionality added to Data Acquisition Points (DAPs) includes:

- Systematically checking and alarming on SSL certificate expiration dates
- Adding default access services (SSH, RDP, Telnet, VNC) to auto-created DAP entities

SSL Certificates - Expiration dates will be monitored daily. As the expiration date approaches ReliaTel will generate a status alarm: 90 days = FYI; 60 days = MIN; 30 days = MAJ; 15 days = CRI. Self-signed certificates are not included in this feature.

Default Access Services - ReliaTel automatically creates a DAP entity when a remote DAP is added to a network. This feature also adds the following access services automatically - SSH, RDP, Telnet, and VNC - for use with AccessPlus, to the entity. Other services can be added; default services are editable.

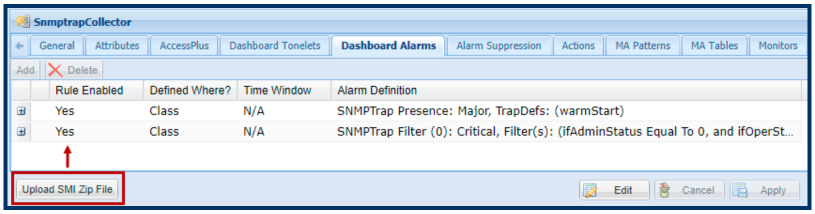


	Service	Enabled	Remote Port	Local Port	Session Time...	User Name	Execute Path
⊞	SSH	Yes	22		600		
⊞	TELNET	Yes	23		600		
⊞	VNC	Yes	5900		600		
⊞	RDP	Yes	3389		600		

Setting Up SNMP Traps for New Devices

Between product releases your organization may add a new device to your network: a device that ReliaTel doesn't yet monitor. If the new device supports SNMP this feature will enable you to monitor the device for SNMP traps until Tone Technical Support creates a supporting foundation kit.

This feature will give you the tools and processes to set up SNMP trap monitoring on your own. Using ReliaTel you'll be able to upload vendor SMI files to the database, extract SNMP traps from the MIB files, convert OIDs to readable text, set parameters for alarming, and assign alarm severities.



	Rule Enabled	Defined Where?	Time Window	Alarm Definition
⊞	Yes	Class	N/A	SNMPTrap Presence: Major, TrapDefs: (warmStart)
⊞	Yes	Class	N/A	SNMPTrap Filter (0): Critical, Filter(s): (ifAdminStatus Equal To 0, and ifOperSt...

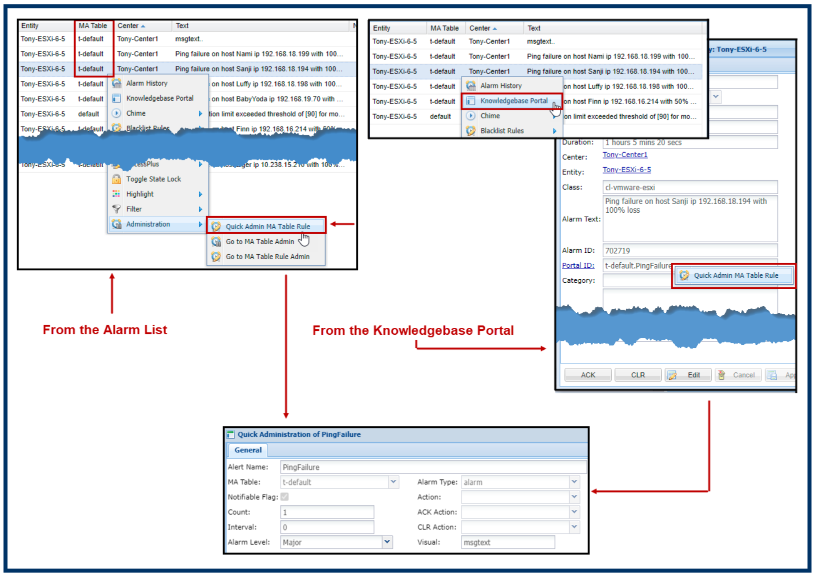
You can also use this feature to monitor old, outdated devices that support SNMP for which ReliaTel doesn't have a foundation kit. Tone Technical Support can be contacted at (714) 991-9460 +1 if you need assistance.

Authenticating and Authorizing ReliaTel Users Through LDAP

This feature gives administrators the option to use an external user management server, via LDAP (Light Directory Access Protocol), to authenticate (user name/password) and authorize (permissions) ReliaTel users. Administrators will no longer need to create new user accounts, manage user passwords, or assign specific permissions to ReliaTel users - those duties can now be deferred to an external system.

Accessing and Editing MA Tables and Table Rules

Alarms generated by SNMP traps are defined in MA tables and MA table rules. Prior to this release, if you wanted to make edits to an alarm, such as changing the severity level or message text, you first had to drill down through General Administration to Alarming then to the MA Tables and MA Table Rules sub-modules and finally locate the specific table. ReliaTel implementations can have hundreds of MA tables. This feature simplifies the hunt for and the editing of an MA table or rule by opening the table directly from either the Alarm List or the Knowledgebase Portal.



Entity	MA Table	Center	Text
Tony-ESXi-6-5	t-default	Tony-Center1	msgtext..
Tony-ESXi-6-5	t-default	Tony-Center1	Ping failure on host Nami ip 192.168.18.199 with 100...
Tony-ESXi-6-5	t-default	Tony-Center1	Ping failure on host Sanji ip 192.168.18.194 with 100...
Tony-ESXi-6-5	t-default		on host Luffy ip 192.168.18.198 with 100...
Tony-ESXi-6-5	t-default		on host BabyYoda ip 192.168.19.70 with ...
Tony-ESXi-6-5	default		tion limit exceeded threshold of [90] for mo...
Tony-ESXi-6-5	t-default		host Finn ip 192.168.16.214 with 50% ...

Entity	MA Table	Center	Text
Tony-ESXi-6-5	t-default	Tony-Center1	msgtext..
Tony-ESXi-6-5	t-default	Tony-Center1	Ping failure on host Nami ip 192.168.18.199 with 100...
Tony-ESXi-6-5	t-default	Tony-Center1	Ping failure on host Sanji ip 192.168.18.194 with 100...
Tony-ESXi-6-5	t-default		on host Luffy ip 192.168.18.198 with 100...
Tony-ESXi-6-5	t-default		on host Finn ip 192.168.16.214 with 50% ...
Tony-ESXi-6-5	default		on limit exceeded threshold of [90] for mo...

y: Tony-ESXi-6-5

Duration: 1 hours 5 mins 20 secs
Center: Tony-Center1
Entity: Tony-ESXi-6-5
Class: cl-vmware-esxi
Alarm Text: Ping failure on host Sanji ip 192.168.18.194 with 100% loss
Alarm ID: 702719
Portal ID: t-default.PingFailure
Category:

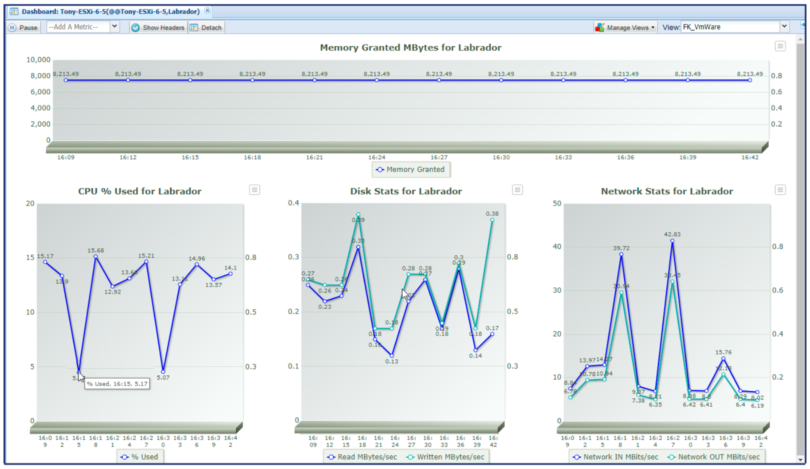
Quick Administration of PingFailure

General

Alert Name:	PingFailure		
MA Table:	t-default	Alarm Type:	alarm
Notifiable Flag:	☑	Action:	
Count:	1	ACK Action:	
Interval:	0	CLR Action:	
Alarm Level:	Major	Visual:	msgtext

Monitoring VMWare ESXi™ Servers

For organizations using VMWare ESXi™ servers this feature enables ReliaTel to now monitor the guest machines hosted on a ESXi™ server. ReliaTel will monitor these metrics - CPU utilization, logical disk usage, memory, processes, and network utilization - and display these metrics in Dashboard tonelets. ReliaTel will also generate alarms when metrics exceed specified thresholds and or when event faults occur.

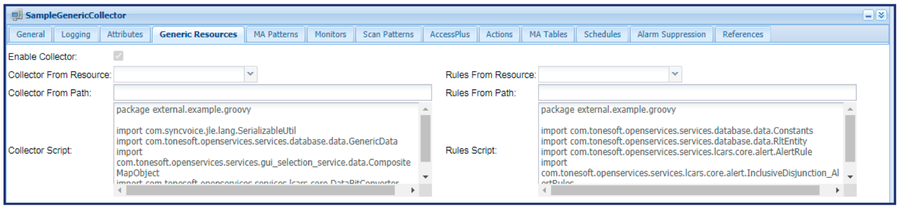


Guest machine metrics displayed in a Dashboard tonelet

Monitor a New Device Intra-Release with a Generic Entity

This feature is similar to the SNMP traps feature for new devices, also introduced in this release. Both features enable users to monitor new devices added to a network intra-release, where a foundation kit has not yet been created. This feature differs from the SNMP feature in that this feature enables the monitoring of *any* new, old, or commonly not monitored devices. This feature can function as a bridge to the next release, when Tone Technical Support has created a foundation kit to support the device.

If a device can be programmatically queried, ReliaTel will be able to monitor the device to generate fault event and metric alarms, display data in the Dashboard, and run reports in Performance Reporting. This will be accomplished by ReliaTel's Tone Technical Support staff collaborating with your organization to identify monitoring parameters and create the scripts needed to query the device. Contact Tone Technical Support at (714) 991-9460 +1 for assistance.



Enable Collector: ☑

Collector From Resource:

Collector From Path:

Collector Script:

```
package external.example.groovy

import com.syncvoice.jle.lang.SerializableUtil
import com.tonesoft.openservices.services.database.data.GenericData
import
com.tonesoft.openservices.services.gui_selection_service.data.Composite
MapObject
```

Rules From Resource:

Rules From Path:

Rules Script:

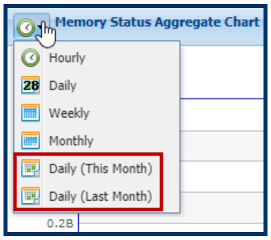
```
package external.example.groovy

import com.tonesoft.openservices.services.database.data.Constants
import com.tonesoft.openservices.services.database.data.RltEntity
import com.tonesoft.openservices.services.lcars.core.alert.AlertRule
import
com.tonesoft.openservices.services.lcars.core.alert.InclusiveDisjunction_Al
```

Sample scripting for a new device

Enhancements

Add *This Month* and *Last Month* to Dashboard Metric Tone-lets

Tonelets with calendar options have two additional selections - 'This Month' and 'Last Month'.

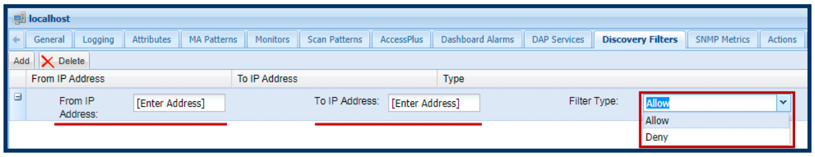


Include IP Node Correlation in RTCP and Cisco Reports

IP node correlation is included in ReliaTel's network Flow analysis. Flow was introduced in a previous release and displayed graphically in the Visual 360 module. This release adds IP node correlation to Flow RTCP and Cisco reports.

Apply Blacklist and Whitelist IP Ranges to the Device Discovery Feature

This is an enhancement to the Device Discovery feature which was introduced in release 6.1.0. Use this enhancement to select the IP addresses you want to include (whitelist) and the IP addresses you want to exclude (blacklist) from device discovery.

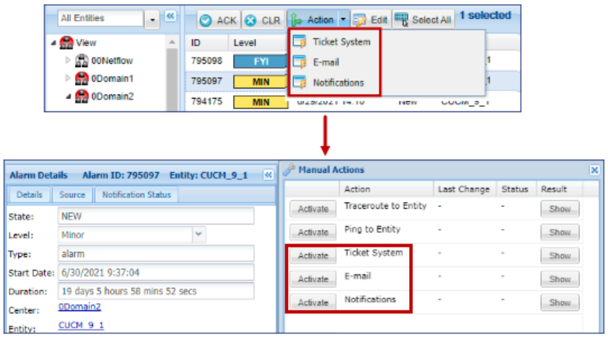


From IP Address	To IP Address	Type

From IP Address: [Enter Address] To IP Address: [Enter Address] Filter Type: Allow

Alarm List Actions Feature Added to the Knowledgebase

This enhancement automatically includes, in the Manual Actions portlet of the Knowledgebase Portal, all actions added to the Actions feature in the Alarm List.



ID	Level
795098	FYI
795097	MIN
794175	MIN

Alarm Details Alarm ID: 795097 Entity: CUCM_9_1

State: NEW
Level: Minor
Type: alarm
Start Date: 6/30/2021 9:37:04
Duration: 19 days 5 hours 58 mins 52 secs
Center: 0Domain2
Entity: CUCM_9_1

Manual Actions

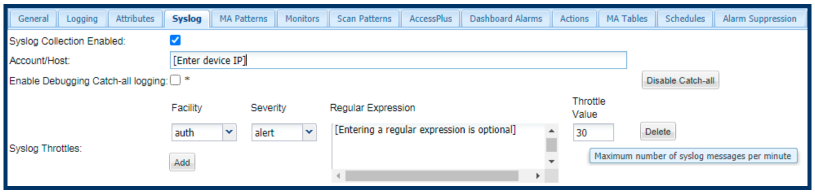
	Action	Last Change	Status	Result
Activate	Traceroute to Entity	-	-	Show
Activate	Ping to Entity	-	-	Show
Activate	Ticket System	-	-	Show
Activate	E-mail	-	-	Show
Activate	Notifications	-	-	Show

Actions added in the Alarm List

Actions automatically added to the Manual Actions portlet

Increase the Level of Detail in Managing Syslog Messages

Use this addition to the syslog interface to manage syslog messages at an enhanced level of detail. With this tool you will be able to manage individual facilities by severity and message count (throttling). You will also be able to switch to 'catch-all' mode for collecting syslog messages and to select specific facilities for which you don't want to receive messages.



Syslog Collection Enabled: ☑
Account/Host: [Enter device IP]
Enable Debugging Catch-all logging: ☐ *

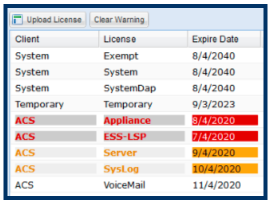
Syslog Throttles:

Facility	Severity	Regular Expression	Throttle Value
auth	alert	[Entering a regular expression is optional]	30

Add GUI Enhancements to Licensing to View License Statuses

Release 6.1.0 introduced the License Management feature. This release expands on the usability of that feature in the following ways:

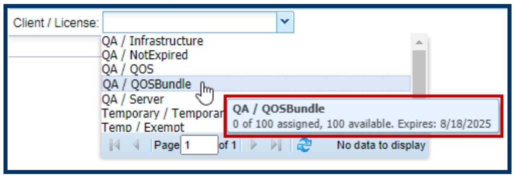
- Color-coded visual cues to let you know that a license has expired or is about (90 days) to expire.



Upload License | Clear Warning

Client	License	Expire Date
System	Exempt	8/4/2040
System	System	8/4/2040
System	SystemDap	8/4/2040
Temporary	Temporary	9/3/2023
ACS	Appliance	🟥 8/4/2020
ACS	ESS-LSP	🟥 7/4/2020
ACS	Server	🟧 9/4/2020
ACS	SysLog	🟧 10/4/2020
ACS	VoiceMail	11/4/2020

- When creating a new entity or collector, license statistics can be displayed before assigning a license.

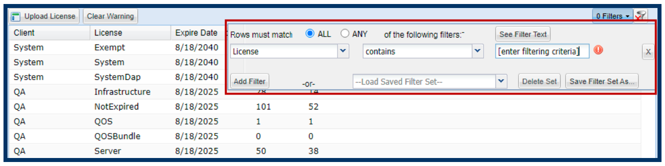


Client / License:

QA / Infrastructure
QA / NotExpired
QA / QOS
QA / QOSBundle
QA / Server
Temporary / Temporar
Temp / Exempt

QA / QOSBundle
0 of 100 assigned, 100 available. Expires: 8/18/2025

- In License administration the filter tool is now available to filter on licenses included in your implementation.



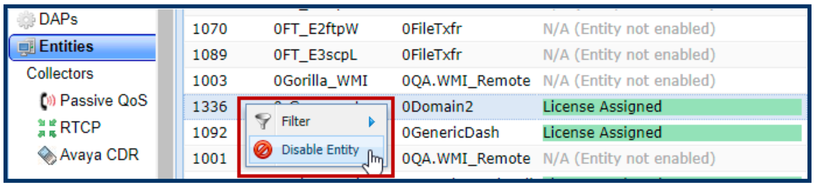
Rows must match ● ALL ○ ANY of the following filters:

License | contains | [enter filtering criteria]

Client	License	Expire Date		
System	Exempt	8/18/2040		
System	System	8/18/2040		
System	SystemDap	8/18/2040		
QA	Infrastructure	8/18/2025		
QA	NotExpired	8/18/2025	101	52
QA	QOS	8/18/2025	1	1
QA	QOSBundle	8/18/2025	0	0
QA	Server	8/18/2025	50	38

Disable Entities and Collectors in Administration With a Single Click

A previous release enabled administrators to disable entities and collectors, with a single click, in the Navigation tree of the Alarm List. In this release administrators can do the same directly from the Entity and Collector sub-modules in Administration.



1070	0FT_E2ftpW	0FileTxfr	N/A (Entity not enabled)
1089	0FT_E3scpL	0FileTxfr	N/A (Entity not enabled)
1003	0Gorilla_WMI	0QA.WMI_Remote	N/A (Entity not enabled)
1336		0Domain2	License Assigned
1092		0GenericDash	License Assigned
1001		0QA.WMI_Remote	N/A (Entity not enabled)