Application Note

Incident Management with Vantage DX Analytics

Overview

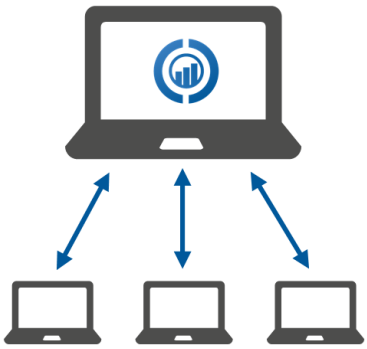
When a service interruption or outage occurs, the first priority is to restore normal operations as quickly as possible to minimize the impact of the disruption and to maintain service quality. To maintain quality and availability, it is important that problem management is proactive as well as reactive. You can address these needs by having a consolidated view of your monitoring tools and ITSM systems, and by automating incident management tasks.

This application note describes how you can use Vantage DX Analytics to:

- Automatically create incidents based on alerts.
- Automatically send notifications to the right team members, so they can start investigating the cause of the alert before it impacts end users.

Understanding the Incident Management Workflow

Vantage DX Analytics integrates with your existing monitoring tools, cloud platforms and IT Service Management (ITSM) systems to help you analyze the health of your applications and network infrastructure. Because it establishes bi-directional communication with your existing tools, Vantage DX Analytics can help you optimize the way that you manage alerts, create incidents, and notify support teams about issues.



Incident Management

VDX Analytics pulls alerts and health state information from your various monitoring tools and consolidates the information. The bi-directional communication between VDX Analytics and your other tools allows you to resolve alerts raised by these monitoring tools directly from within VDX Analytics. You can also navigate to your ITSM from within VDX Analytics to close incidents quickly.

Using one interface to monitor the health of your network and manage incidents streamlines your work processes, and automating these tasks provides additional efficiencies.

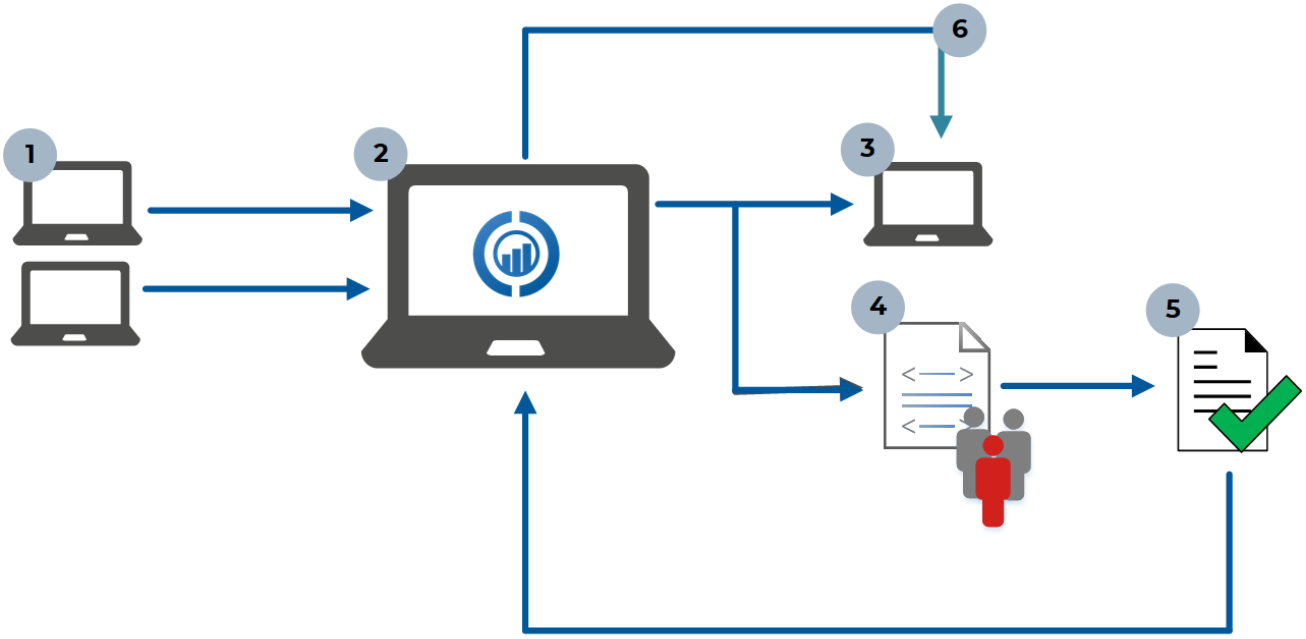
In addition, the data modelling in VDX Analytics means that when an alert is raised by any of your other monitoring tools, it is immediately clear which applications are affected by the problem. That's because in VDX Analytics, alerts are related to boards, business services, or saved searches.

- **Boards** are a way of organizing groups of objects from one or more monitoring systems. You can create boards and nest them within boards. This allows you to model your IT environment in the way that best fits your needs. For example, you can create boards for locations, applications, or business units, and then divide these boards into sub-boards.
- **Business services** provide a way of mapping the devices and applications that work together to support specific business services. When you map devices and applications to a business service, you can monitor your organization's IT resources in the context of the business workflow where those resources are used.
- **Saved searches** are customized searches that allow you to see the number of objects, alerts, incidents or components that match the criteria you specify.

This organization of data in VDX Analytics allows you to quickly determine which applications or services may be affected by the issue, so that you can begin your problem management process more quickly and prioritize issues more easily.

Incident Management Process

The following diagram provides an overview of the incident management workflow that you can configure in VDX Analytics:



1. The source monitoring systems raise alerts.
2. VDX Analytics consolidates all the alerts from the various source monitoring systems.
3. VDX Analytics creates an incident in your ITSM based on these alerts.
4. VDX Analytics automatically sends a notification to the team that is responsible for supporting the affected applications or services. The notification is sent using your choice of method.
5. The support team resolves the problem that caused the alert.
6. You can navigate directly to the ITSM from within VDX Analytics to close the incident. VDX Analytics automatically closes the alerts in the source systems when it detects that the issue no longer exists, or that the incident is closed in the ITSM.

Automatically Create Incidents

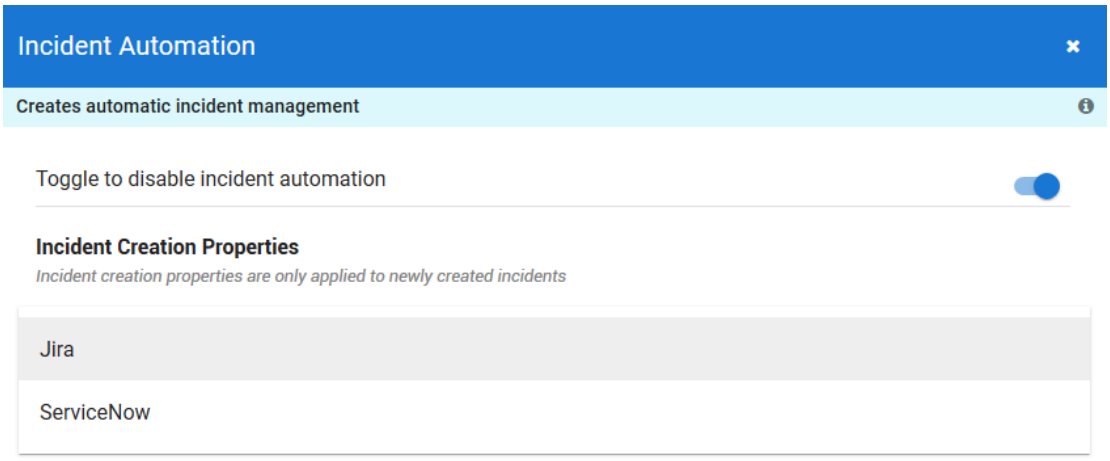
If you have integrated an ITSM system with VDX Analytics, you can automate the creation of incidents. When you enable this feature, VDX Analytics creates an incident when an alert is raised for a board, a business service, or a saved search. Any subsequent alerts for that board, business service, or saved search are attached to the incident, so that all alerts are consolidated in one incident in your ITSM.

By default, VDX Analytics resolves all related alerts when the incident is closed.

VDX Analytics currently integrates with the following ITSMs:

- BMC Remedy
- Cherwell
- Ivanti
- JIRA
- Provance
- ServiceNow
- TopDesk

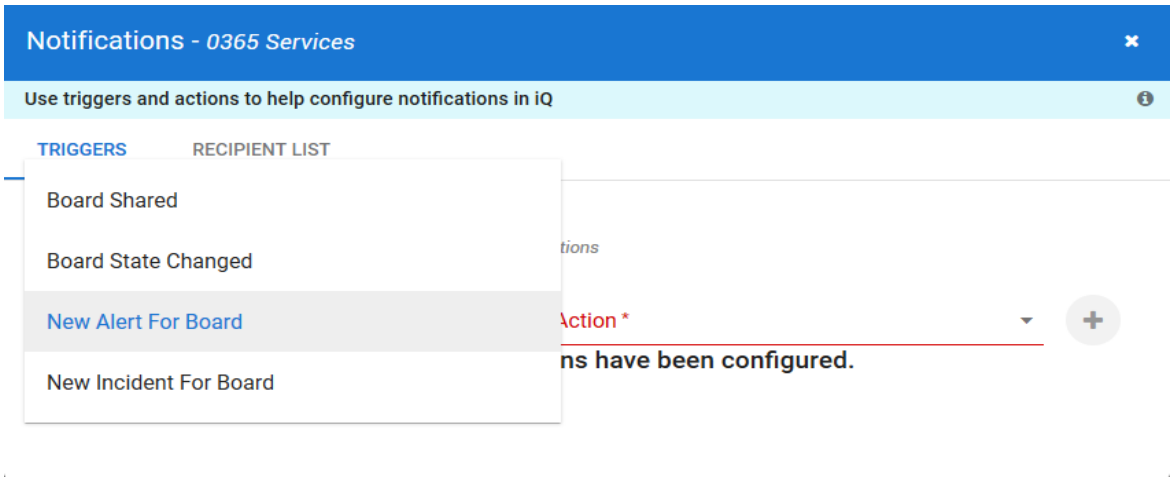
You can use the Incident Automation dialog box, shown in the image below, to configure the properties for incident that VDX Analytics creates in your ITSM.



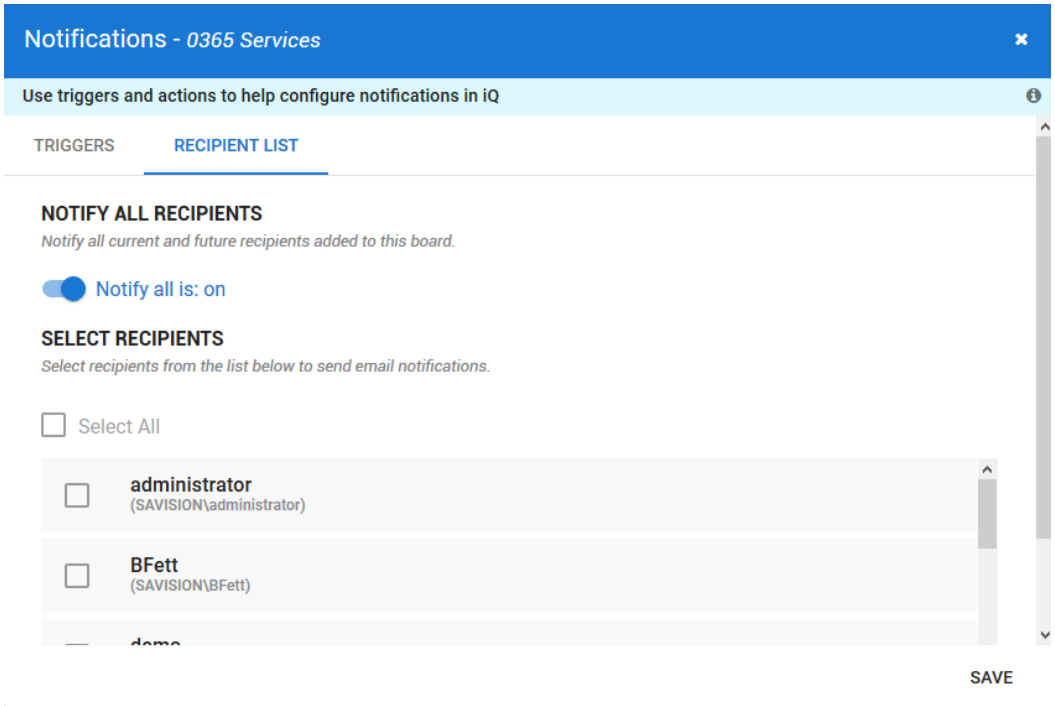
Automatically Send Notifications

An alert management process that notifies all members of the team about an alert or incident is inefficient. VDX Analytics allows you to send notifications about alerts and incidents to the specific team that is responsible for supporting the affected applications or services.

You can configure notifications to be sent automatically when there is a new alert or new incident. You can also configure a notification that is triggered when a board or business service is shared, or when its state changes.



After you select the trigger for the notification, you can select the recipients who should be notified:



Incident Management

There are two ways to send automatic notifications:

- You can send notifications to email recipients.
- You can send notifications to a PowerShell script.

The option to send notifications to a PowerShell script gives you the flexibility to configure a range of actions in response to the notification. For example, you can send notifications to a PowerShell script that:

- Generates an SMS message.
- Sends a notification to a Slack channel.
- Sends a notification to Microsoft Teams.

If you choose to send notifications to a PowerShell script, VDX Analytics sends the following data:

- [String] $notificationtrigger
- [String] $destinationemails
- [String] $destinationphone
- [String] $destinationaccount
- [String] $userrole
- [Int32] $userroleid
- [String] $affecteditemkey
- [String] $affecteditemname
- [String] $affecteditemtype
- [String] $message
- [String] $title
- [String] $severity
- [DateTime] $timestamp
- [String] $details
- [String] $url

Close Alerts

VDX Analytics resolves related alerts in the source monitoring system when it detects that the incident is closed in the ITSM. VDX Analytics performs this task for incidents that are created automatically, as well as for incidents that you create manually.

Resources

For sample PowerShell scripts that you can use to send notifications to Slack or Teams, see the following Knowledge Base articles:

https://support.martellotech.com/knowledgeBase/9844929

and

https://support.martellotech.com/knowledgeBase/10021981

For information about how to configure the features described in this Application Note, refer to the *Vantage DX Analytics User Guide*.

For information about modelling your data, including examples, see the following Application Notes:

- For information about using business services, refer to *Vantage DX Analytics Business Services*.
- For information about using boards, refer to *Manage Complex Data in Vantage DX Analytics*.

All documents are available on the Martello website at:

https://martellotech.com/documentation/analytics/

About Martello Technologies

Martello Technologies Group Inc. (TSXV: MTLO) is a technology company that provides digital experience monitoring (DEM) solutions. The company develops products and solutions that provide monitoring and analytics on the performance of real-time applications on networks, while giving IT teams and service providers control and visibility of their entire IT infrastructure. Martello's products include unified communications performance analytics software and IT analytics software.

Martello Technologies Group is a public company headquartered in Ottawa, Canada with offices in Montreal, Amsterdam, Paris, Dallas and New York. For more information, please contact us:

NORTH AMERICA: +1-613-271-5989
EUROPE: +31-20-2170-790
INTERNET: WWW.MARTELLOTECH.COM
EMAIL: INFO@MARTELLOTECH.COM

MARTELLO | ***Savision*** is a subsidiary of Martello Technologies