August 17, 2023

Application Note

Manage Incidents and Alerts

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 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—which is part of the Vantage DX solution—to proactively manage incidents by:

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

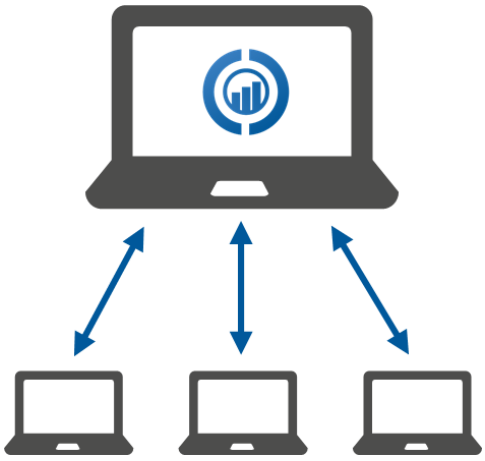
If you are new to Vantage DX, you may find it helpful to read *Understanding Vantage DX* for an overview of the solution and its modules. See the **Resources** section at the end of this document for more information.

Understanding the Incident Management Workflow

VDX 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, VDX Analytics can help you optimize the way that you manage alerts, create incidents, and notify support teams about issues.

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.

Manage Incidents and Alerts



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. In VDX Analytics, alerts are related to boards, business services, or saved searches.

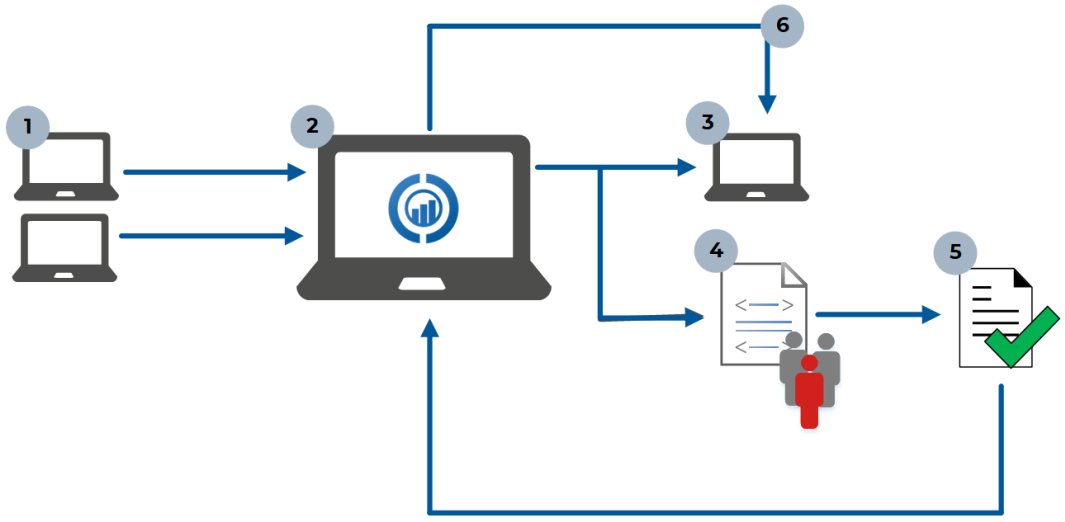
- **Boards** are a way of organizing groups of objects from one or more monitoring systems. You can create boards and nest them within boards. This allows you to model your IT environment in the way that best fits your needs. For example, you can create boards for locations, applications, or business 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.

Workflow

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

Manage Incidents and Alerts

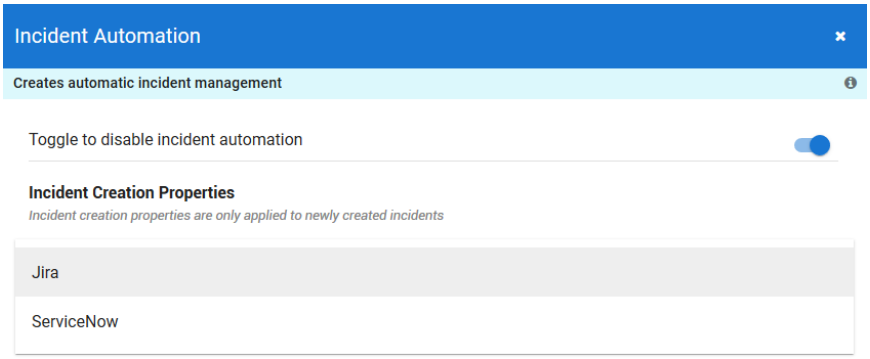


1	The source monitoring systems raise alerts.
2	VDX Analytics consolidates all the alerts from the various source monitoring systems.
3	VDX Analytics creates an incident in your ITSM based on these alerts.
4	VDX Analytics automatically sends a notification to the team that is responsible for supporting 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.

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



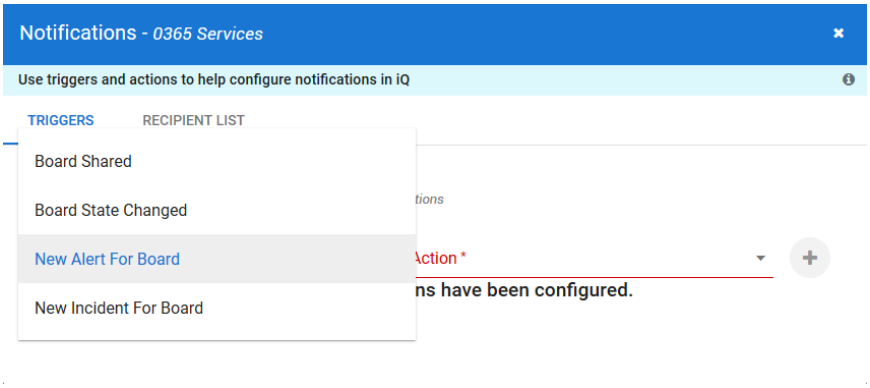
By default, VDX Analytics resolves all related alerts when the incident is closed.

VDX Analytics currently integrates with the following ITSMs:

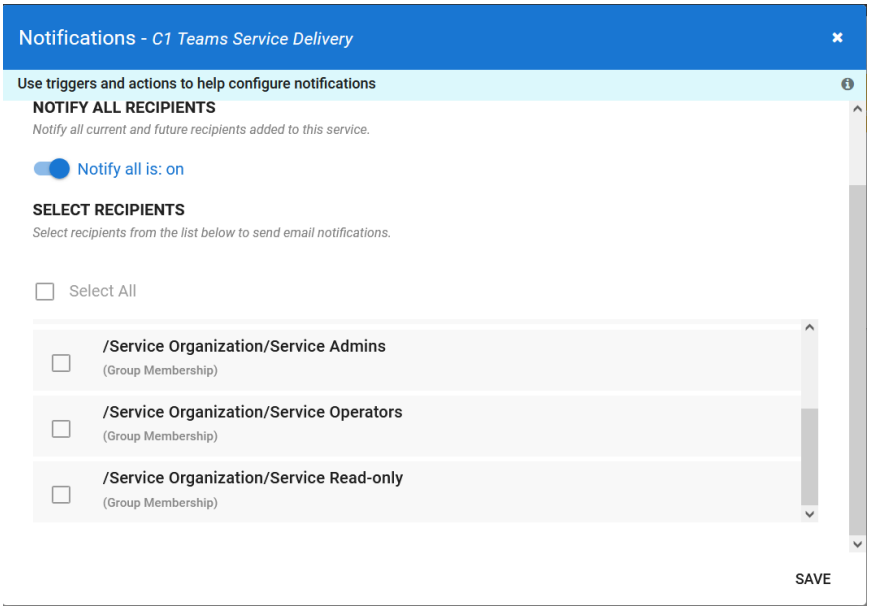
- BMC Remedy
- Cherwell
- Ivanti
- JIRA
- ServiceNow
- TopDesk

Automatically Send Notifications

VDX Analytics allows you to send notifications about alerts and incidents to users in a specific role. 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, as shown in the image below.



After you select the trigger for the notification, you can select the role that should receive the notification:



You can then select the notification method that you want to use. There are three ways to send automatic notifications:

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

You must add an integration for email notifications, MS Teams notifications, or for PowerShell before you can use the notifications feature.

Email Notifications

For each role, you must specify the email address that you want Vantage DX Analytics to use for notifications. You can assign one email address for each role.

Microsoft Teams Notifications

For each teams channel that you want to message, you must configure separate Teams notification integrations.

PowerShell Notifications

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.
- Sends a notification to Moogsoft.
- Creates a record in the Event Log when a notification is sent.

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 more information, see the following documents:

- For an overview of the Vantage DX solution and its capabilities, see the *Understanding Vantage DX* Application Note.
- For a full list of supported integrations, see the *Vantage DX Analytics Integration Guide*.
- For information about how to configure the features described in this application note, refer to the *Vantage DX Deployment Guide*.
- See the following Application Notes for information and examples about key features in VDX Analytics:
  - *Manage Data Using Boards*
  - *Manage Data Using Business Services*

Manage Incidents and Alerts

All documentation is available on the Martello website at:

https://martellotech.com/documentation/vantage-dx/

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

- Send notifications to Slack
- Send notifications to an event log
- Send notifications to Moogsoft

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 Nice, 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