MARTELLO

Savision is a subsidiary
of Martello Technologies

VANTAGE DX ANALYTICS

USER GUIDE — CLOUD DEPLOYMENTS

RELEASE 3.21

DOCUMENT DATE: MAY 12, 2025

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Martello Technologies Corporation. The information is subject to change without notice and should not be construed in any way as a commitment by Martello Technologies or any of its affiliates or subsidiaries. Martello Technologies and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Martello Technologies.

Trademarks

MarWatch™, Savision, Martello Technologies, GSX, and the Martello Technologies logo are trademarks of Martello Technologies Corporation.

Windows and Microsoft are trademarks of Microsoft Corporation.

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.

User Guide — Cloud Deployments
Release 3.21 - May 12, 2025

Contents

CHAPTER 8

CHAPTER 9

CHAPTER 10

Introduction

Document Purpose and Intended Audience

This document provides information about how to use Vantage DX Analytics to analyze and manage data from your existing monitoring tools, cloud platforms and ITSM systems.

This guide is intended for use by administrators and operators.

Revision History

Document Date	Description
May 12, 2025	Vantage DX AnalyticsUser Guide — Cloud Deployments Release 3.21

About Vantage DX Analytics

Vantage DX Analytics is a powerful IT analytics solution that consolidates information from your existing monitoring tools, cloud platforms and ITSM systems into a single system. It pulls alerts and health state information from your various monitoring systems and unifies them in one interface. You can model the data in boards and business services to reflect the needs of your organization. Consolidating the information from various monitoring tools allows you to see the overall health status of a system quickly. For example, you can use VDX Analytics to view the status of computers monitored by SCOM, network objects monitored by SolarWinds, and Linux computers monitored by Nagios—all in one place. VDX Analytics also integrates with Vantage DX Monitoring to provide proactive monitoring of your Microsoft 365 services. VDX Analytics uses an Elasticsearch database that allows you to search and analyze data quickly.

VDX Analytics also integrates with your ITSM system. When it pulls information from your monitoring systems, it also retrieves any alerts raised by that system. Because the integrations are bi-directional, you can use VDX Analytics to create an incident based on several alerts and then close those alerts once the incident has been resolved.

VDX Analytics provides tools that you can use to model your monitoring data in the way that best suits your business. It also automatically creates dashboards that you can use immediately, without the need to model your data.

The following sections provide an overview of these features:

- "Boards" on page 8
- "Business Services" on page 9
- "Dashboards" on page 9

Boards

VDX Analytics boards are a way to group components from one or more monitoring systems or cloud platforms. Boards are flexible and allow you to model your IT environment in the way that best fits your needs. For example, if you have multiple sites or multiple data centers, you can a create a board for each location. You can

also create boards for business units, or for different types of users. You can create a single board or you can create sub-boards within a higher-level board.

Whether your boards reflect your corporate structure or are organized in some other way, a best practice is to create boards that reflect the most important aspects of your organization, so that the disruptions or failures that would be most critical to your business are easy to monitor. The more critical a component is, the more important it is that you can see and fix it easily.

Business Services

Business services are services that you deliver to your internal and external customers. Business services can be tools such as email services and collaboration platforms, or business functions such as accounts receivable.

Business services are a way of mapping the devices and applications that work together to support specific business functions. 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. For each business service that you define, you can map components to the following ITIL perspectives:

- End User
- Application
- Infrastructure
- Supplier services; these are other business services that impact other business services. For example, if you create an "Authentication" business service to monitor all of the resources that are needed to authenticate users in your organization, it can be a supplier service to other business services that depend on authentication resources to work properly.

Dashboards

Dashboards allow you to monitor call quality data, without the need to model it using boards or business services.

There are two types of dashboards:

- **Data Analysis Dashboards**—The dashboards under the Data Analysis menu provide access to information that you need for troubleshooting call quality issues. They help you correlate data from a range of sources.
- **Proactive Monitoring Dashboards**—The dashboards under the Proactive Monitoring menu provide access to information about synthetic transactions so that you can proactively monitor metrics that are predictors of call quality.

For information about the dashboards, see *Performance Data in Vantage DX*. The guide is available from the Martello Help Center by clicking the following link:

https://helpcenter.martellotech.com/s/documentation/vantage-dxcloud

About the Interface

The VDX Analytics main menu allows you to view default dashboards, as well as manage boards, business services, and administrative settings.

The following sections describe each of the menu options and the functionality they provide:

- "Data Analysis" on page 10
- "Proactive Monitoring" on page 13
- "Explore" on page 1
- "Settings" on page 25
- "Help" on page 28

> **Note:**
> The menu options that display depend on your license package. This document may describe menus that are not available in your deployment.

Data Analysis

Use the Data Analysis menu to access the dashboards that VDX Analytics creates automatically. The dashboards contain call quality data from the following sources:

- Microsoft Teams Call Quality Dashboard (CQD)
- Vantage DX Monitoring
- AudioCodes Session Border Controllers (SBCs)
- Zoom (if licensed)

Access to the dashboards is role-based. By default, only administrators can view the dashboards. Users in other roles can view the dashboards only if an administrator has assigned access to them. The Data Analysis sub-menu lists the dashboards that the user has permission to access. If a user does not have permission to access any dashboards, the Data Analysis menu is not visible to that user.

For information about the dashboards, see *Performance Data in Vantage DX*. The guide is available from the Martello Help Center at the following link:

https://helpcenter.martellotech.com/s/documentation/vantage-dxcloud

In addition to the dashboards, the Data Analysis menu provides access to boards and business services, which allow you to model data in the way that best suits your needs. For information, see the following sections:

- "Boards" on page 11
- "Business Services" on page 12

Boards

Use the Boards page to configure, monitor, and share boards. You can also create sub-boards, and view board details. The Boards page includes a Filters panel that you can use to organize how the boards are displayed, and to find specific boards.

Click the arrow on the left side to show options to organize and configure the page view, and to find specific boards:

- **Display Top**—Choose to show a maximum of 20, 50, or 100 boards on the page.
- **Visualize By**—Choose how you want the boards to display information.
- **Sort By**—Choose whether to sort the boards by the board states or the board names.
- **Display Board States**—Filter the boards based on the state of the board.
- **Health Rollup Types**—Filter the boards based on the type of health rollup configured for the board.
- **Exclude Child Boards**—This option is selected by default. When this is selected, only top-level boards display. Boards that roll up their health state to a higher-level board are not shown.
- **Display boards with**—Filter the boards based on whether incident automation or notifications are enabled for the board.

Click the icon in the header of each board to access the following menu items:

- **Actions**
  - Share—Make the board available to users in a specific role.
  - PIN—Pin the board to a another board, as a sub-board.
  - Delete—Delete the board.
- **Edit**
  - Details—Change the board name or health rollup type.
  - Manual State—Manually change the current state of the board.
  - Notifications—Configure a notification that is triggered when a board is shared, when its state changes, or when there is a new alert or new incident.
- **Maintenance Mode**—Schedule maintenance, or put the board in maintenance mode immediately.
- **Incident Automation**—If you have integrated an ITSM system with VDX Analytics, you can automate the creation of incidents.

Click the Add icon in the bottom right corner of the page to create a new board.

Click on any board header to open the board and to view board details, including:

- **Members**—Displays all member objects currently pinned to the board. Member objects can include components such as computer, groups, or services, as well as sub-boards.
- **Explorer**—Displays a topology diagram that allows you to view board objects and to explore related objects.
- **Alerts or Incidents**—Displays a list of all active alerts or incidents related to the board.
- **Rules**—Displays all rules that have been configured to dynamically add objects to this board.
- **Exclusions**—Displays the objects within the configured rules that will be excluded from the rules; these specific objects will not be dynamically added to the board.

Click the Actions icon in the bottom right corner of each tab to access the valid actions for that tab.

Business Services

Use the Business Services page to organize and monitor critical business services. You can also generate SLA availability reports, and access details about the business service perspectives and member objects.

The page also displays the number of active events and incidents related to the business service, and the overall SLA percentage of availability for each business service, based on the service level objectives (SLO) you have configured for each business service.

Click on the business service name to view information about the overall business service including:

- **SLA**—Displays a summary of SLA availability information for the business service, and a breakdown of the health state of each perspective.
- **Members**—Displays all member objects of the business service, organized by perspective. You can click each perspective to drill down to view the objects within each perspective.
- **Alerts or Incidents**—Displays a list of all active alerts or incidents related to the business service.

Alternatively, click any of the perspective columns to view information about that particular perspective for the business service, including:

- **Members**—Displays all member objects for the selected perspective of the business service. Member objects can include components such as computer, groups, or services. You can click each object to view the object details.
- **Alerts or Incidents**—Displays a list of all active alerts or incidents related to the business service.
- **Rules**—Displays all rules that have been configured to dynamically add objects to this business service.

- **Exclusions**—Displays the objects within the configured rules that will be excluded from the rules; these specific objects will not be dynamically added to the business service.

Click the icon at the end of each business service row to access the following menu items:

- Configure
  - **Service Details**—View or update configuration details for the business service.
  - **Service Level Objectives**—View or update the SLA goal, and the time period and business hours to use in SLA calculations.
  - **Supplier Services**—View or update the supplier services that relate to the selected business service.
  - **Incident Automation**—If you have integrated an ITSM system with VDX Analytics, you can automate the creation of incidents.
  - **Notifications**—Configure a notification that is triggered when a business service is shared, when its state changes, or when there is a new alert or new incident.
  - **Manual State**—Manually change the current state of the business service.
- **Maintenance Mode**—Schedule maintenance, or put the business service in maintenance mode immediately.
- **Share**—Make the business service available to users in a specific role.
- **Remove**—Delete the business service.

> **Tip:**
> You can change the display for the business service data. Click the icon in a column header and select options to sort data, to hide or show columns, or to reset to the default display. Click and drag column headers to rearrange the columns.

Proactive Monitoring

This menu provides access to information about synthetic transactions so that you can proactively monitor metrics that are predictors of call quality. The dashboards contain call quality data from Vantage DX Monitoring.

Access to the dashboards is role-based. By default, only administrators can view the dashboards. Users in other roles can view the dashboards only if an administrator has assigned access to them. The sub-menu lists the dashboards that the user has permission to access. If a user does not have permission to access any dashboards, the Analyze menu is not visible to that user.

For information about the dashboards, see *Performance Data in Vantage DX*. The guide is available from the Martello Help Center at the following link:

https://helpcenter.martellotech.com/s/documentation/vantage-dxcloud

Explore

When you click on the Explore menu, the Explore page displays and provides access to tabs that allow you to view and search health information, as well as the raw properties that VDX Analytics collects from the source systems. The following tabs are available:

- "Computers" on page 15
- "Alerts" on page 18
- "Incidents" on page 19
- "Groups and Services" on page 19
- "Components" on page 22
- "Saved Searches" on page 24

In addition, the Explore page provides a Search bar that allows you to search the details or raw properties of each object, alert, and incident.

Under the Explore menu, sub-menus display that provide access to pre-defined searches. These searches allow you to quickly find data that Vantage DX Analytics has retrieved from the Microsoft Teams CQD integration. The following searches are available:

- Users with poor calls within 24 hours*****
- Users with poorly rated calls within 7 days*****
- Users with Wi-Fi signal strength issues within 7 days*****
- User Devices
- Teams Alerts
- Teams Meetings
- Meeting Rooms
- Offices
- Locations with poor calls within 1 month*****
- Offline IP phones

In addition to these CQD searches, an additional pre-defined search is available on the Saved Searches tab, named "Users with SIP Response 408 within 7 days.*****" This search finds users who experienced 20% or more calls that failed due to PSTN issues. In order to use this search successfully, you must edit the search criteria to specify the address of your PSTN trunk. A placeholder address is provided that you can edit when you load the search into the Search bar.

> **Tip:**
> The ***** indicates searches that you can use to configure notifications. Notifications that are based on searches are

triggered when the search criteria is met. For information about how to configure these notifications, see "Manage Notifications and Incidents" in the *Vantage DX Deployment Guide*. The guide is available in the Martello Help Center at:

https://helpcenter.martellotech.com/s/documentation/vantage-dxcloud

Note:
We recommend that you configure a consolidation rule before you use the Meeting Rooms search. For more information, see the "Integrate Data from your Microsoft Tenant" chapter in the guide *Performance Data in Vantage DX*. It is available on the Martello website at https://martellotech.com/documentation/vantage-dx/#documentation.

Computers

The Computers tab provides information about the properties of the computers that are monitored by your systems. Each monitoring system or ITSM that VDX Analytics connects with uses its own terminology. For consistency, VDX Analytics normalizes the monitored objects into data types. On the Computers tab, the data types are:

- Computer
- Virtual machine

You can filter the computers and virtual machines using the following options:

- **Types**—Filter based on the type of object: computers or virtual machines.
- **Integration Types**—Filter based on the type of integration, such as Operations Manager or PRTG. This option lists all the supported integration types, not only the ones that you have configured.
- **Integrations**—Filter based on the names of the integrations that you have configured.
- **Hide Correlated Components**—This option is selected by default. When it is selected, the page displays the consolidated components but does not show the components that are correlated with them. Deselect this option to show all components.
- **Consolidation Rules**—Filter the list based on consolidation rules that apply to this type of component.
- **State**—Filter based on the health status of the object.

When you select a single computer or virtual machine, the properties panel displays. It shows information about the number of open alerts and incidents, as well as the Mean Time to Resolution (MTTR). It also provides information about

uptime and state changes, and it indicates the component type and the source monitoring system. For consolidated components, the component type is indicated by the consolidation icon, and the source system is listed as Consolidation.

The following functions are available from the properties panel of a computer or virtual machine:

Button	Function	Description
	More Details	This button opens a page with the details about the selected computer. The page contains the following tabs: • **Properties**—View the raw properties from the original monitoring system. • **Explorer**—View a topology diagram that shows components and relationships. For more information about using the Explorer, see "Use the Components Explorer" on page 63 • **Alerts**—View alerts related to the selected computer or virtual machine. • **Incidents**—View incidents related to the selected computer or virtual machine. • **Boards**—View boards that the computer or virtual machine is a member of. • **Services**—View services that the computer or virtual machine is a member of. • **Correlated Components**—This tab displays for consolidated components only. Use it to view a list of the components that are contained in the consolidated component. You can select a component to view its properties, such as the object type and the source system that is monitoring it.
	Source	This button opens a new browser tab and navigates to the selected object in the console of the integrated source system.

Button	Function	Description
	Action	This button provides access to the following options:
	Incident Automation	This button opens a dialog box that allows you to configure incident automation for the selected consolidated component. This feature is available for consolidated components only, and you must have integrated an ITSM system with VDX Analytics to use this feature.
	Pin	This button pins the object to a new or existing board.
	Service	This button pins the object to a service.

If you want to perform an action for multiple objects on this tab, you can use the Ctrl and Shift keys to select them. For example, you can pin multiple objects to a board or service. When you select multiple objects, the following functions are available.

Button	Function	Description
	Action	This button provides access to the following options:
	Pin	This button pins the object to a new or existing board.
	Service	This button pins the object to a service.

 Note: Not every monitoring system has the concept of computers. Some monitoring systems identify objects as devices, which may be computers. VDX Analytics shows objects that may be considered computers or virtual machines on this tab; however, if a computer does not display on this tab, it may be due to the way that the original monitoring system has identified it. If you are unable to find a computer on this tab, you can find it in the Components tab, which contains all objects.

Alerts

The Alerts tab displays all of the alerts from the different monitoring systems. The most recent alerts are shown at the top of the tab by default, but you can change the sort order.

You can filter alerts using the following options:

- **Integration Types**—Filter based on the type of integration, such as Operations Manager or PRTG. This option lists all the supported integration types, not only the ones that you have configured.
- **Integrations**—Filter based on the names of the integrations that you have configured.
- **Severity**—Filter based on the severity of the alert.
- **Active**—Show active alerts only.
- **Incidents**—Choose whether to display alerts with incidents or without incidents.
- **Time**—Filter based on the length of time since the alert was raised or updated.

You can use the Ctrl and Shift keys to select multiple alerts on this tab. When you select a single alert, the properties panel displays.

The following functions are available on the properties panel:

Button	Function	Description
	Editable Fields	This toggle displays for SCOM and MPA integrations. Use it to view editable fields in SCOM.
	Related Components	This button opens a new page that lists details about components in VDX Analytics that are related to this alert.
	Source	This button opens a new browser tab and navigates to the selected object in the console of the integrated source system.
	Resolve	Resolve the alert in the source system.
	Link an Incident	Link the alert to an existing incident.
	Acknowledge an Alert	Acknowledge an alert in the source system.
	Create an Incident	Link the alert to a new incident.

Incidents

The Incidents tab displays incidents that VDX Analytics has retrieved from your integrated systems.

You can filter incidents using the following options:

- **Integration Types**—Filter based on the type of integration, such as ServiceNow or Ivanti. This option lists all the supported integration types, not only the ones that you have configured.
- **Integrations**—Filter based on the names of the integrations that you have configured.
- **Active**—Show active incidents only.
- **Vantage DX Analytics**—Show only those incidents created by VDX Analytics.
- **Time**—Filter based on the length of time since the alert was raised or updated.

When you select a single incident, the properties panel displays.

The following functions are available from the properties panel:

Button	Function	Description
	More Details	Use the button to view the incident page with raw properties and related alerts.
	Related Components	This button opens a new page that lists details about components in VDX Analytics that are related to this incident.
	Source	This button opens a new browser tab and navigates to the selected object in the console of the integrated source system.

Groups and Services

The Groups & Services tab displays all groups and services from your monitoring systems. This tab allows you to view the group health as well as the health of the objects within the group.

You can filter groups and services using the following options:

- **Types**—Filter based on the type of object: groups or services.
- **Integration Types**—Filter based on the type of integration, such as Operations Manager or PRTG. This option lists all the supported integration types, not only the ones that you have configured.
- **Integrations**—Filter based on the names of the integrations that you have configured.
- **Hide Correlated Components**—This option is selected by default. When it is selected, the page displays the consolidated components but does not show

the components that are correlated with them. Deselect this option to show all components.

- **Consolidation Rules**—Filter the list based on consolidation rules that apply to this type of component.
- **State**—Filter based on the health status of the object.

You can use the Ctrl and Shift keys to select multiple objects on this tab. When you select a single group or service, the properties panel displays.

The following functions are available when you select an object:

Button	Function	Description
	More Details	This button opens the Component page. The page contains the following tabs: • **Properties**—View the raw properties from the original monitoring system. • **Members**—View members of the group or service. You can click the name of the member to view more information about that object. • **Explorer**—View a topology diagram that shows components and relationships. You can use the diagram to explore the group or service to see the hierarchy of objects. For more information about using the Explorer, see "Use the Groups and Services Explorer" on page 62. • **Alerts**—View alerts related to the selected group or service. • **Incidents**—View incidents related to the selected group or service. • **Boards**—View boards that the group or service is a member of. • **Services**—View services that the group or service is a member of. • **Correlated Components**—This tab displays for consolidated components only. Use it to view a list of the groups and services that are included in the consolidated component. You can select a component to view its properties, such as the object type and the source system that is monitoring it.
	Action	This button provides access to the following options:
	Import a Live Maps Service	Import a Live Maps service from Microsoft System Center Operations Manager (SCOM).

21

Button	Function	Description
+	Create a Synced Board	A synched board displays the members of the group as they are configured in the source system. When members are added or removed in the source system, those changes are reflected on the board in VDX Analytics. The health state of the board is the same as the health state of the original group in the source system.
📌	Pin	This button pins the object to a new or existing board.
⚠	Service	This button pins the object to a service.
🪄	Incident Automation	This button opens a dialog box that allows you to configure incident automation for the selected consolidated component. This feature is available for consolidated components only, and you must have integrated an ITSM system with VDX Analytics to use this feature.

Components

The Components tab displays all monitored components.

You can filter the components using the following options:

- **Types**—Filter based on the type of object. Each monitoring system uses its own terminology. For consistency, VDX Analytics normalizes the monitored components into types, such as computers, websites, databases, and more. You can filter the components on this tab based on any of the available types.
- **Integration Types**—Filter based on the type of integration, such as Operations Manager or PRTG. This option lists all the supported integration types, not only the ones that you have configured.
- **Integrations**—Filter based on the names of the integrations that you have configured.
- **Hide Correlated Components**—This option is selected by default. When it is selected, the page displays the consolidated components but does not show the components that are correlated with them. Deselect this option to show all components.
- **Consolidation Rules**—Filter the list based on consolidation rules that apply to this type of component.
- **State**—Filter based on the health status of the component.

You can use the Ctrl and Shift keys to select multiple components on this tab. When you select a single component, the properties panel displays.

The following functions are available when you select a component:

Button	Function	Description
	More Details	This button opens a page with details about the component. It contains the following tabs: • **Properties**—View the raw properties from the original monitoring system. • **Alerts**—View alerts related to the selected component. • **Explorer**—View a topology diagram that shows components and relationships. You can use the diagram to explore the group or service to see the hierarchy of objects. For more information about using the Explorer, see "Use the Components Explorer" on page 63. • **Incidents**—View incidents related to the selected component. • **Boards**—View boards that the component is a member of. • **Services**—View services that the component is a member of. • **Correlated Components**—This tab displays for consolidated components only. Use it to view a list of the components that are contained in the consolidated component. You can select a component to view its properties, such as the object type and the source system that is monitoring it.
	Action	This button provides access to the following options:

Button	Function	Description
	Incident Automation	This button opens a dialog box that allows you to configure incident automation for the selected computer. You must have integrated an ITSM system with VDX Analytics to use this feature.
	Pin	This button pins the object to a new or existing board.
	Service	This button pins the object to a service.

Search Bar

The Search bar allows you to search the details or raw properties of each object, alert, and incident in Elasticsearch. When you use the Search bar, it returns results for each of the tabs on the page. As long as the search term remains in the Search bar, the tabs continue to display information based on that search term.

Unless you use a wild card, the search looks for the exact words that you enter. For example, searching SQL will not return SQLSVR01. For information about using search strings, see "Search Operators" on page 41.

On the right side of the Search bar, there are three options:

- **Save**—Save a search.
- **Load**—Load a saved search.
- **X**—Clear the search.

Saved Searches

The Saved Searches tab allows you to customize searches and save your preferences. You can set filters for the search and select the tab where you want the results to display.

The Saved Searches tab includes several pre-defined searches:

- Contains 'SQL'
- Critical Alerts in Last 24h
- Critical Computers
- Critical Databases
- Critical Websites
- Exceptions and Errors
- Incidents Created in Last 24h

The saved search displays the number of objects, alerts, incidents or components that match your search criteria. You can click the information on the saved search to go directly to the data tab for that item.

Settings

The Settings option on the main menu is available to VDX Analytics administrators only.

The Settings page contains the following tabs:

Customer Management

If you are using Vantage DX to provide managed services for your customers, your deployment displays a Customer Management tab. This tab allows you to create customer profiles and assign integrations to them.

For information about how to configure customer profiles, see "Manage User Access" in the *Vantage DX Deployment Guide for Service Providers*.

System Integrations

If you are using Vantage DX to provide managed services for your customers, your deployment displays a System Integrations tab. You can use this tab to configure the integrations that your organization will use to deliver services, such as integrations for email notifications or Teams notifications, or an integration with an ITSM system such as ServiceNow. Integrations that are associated with a specific customer are configured on the Customer Management tab.

Integrations

VDX Analytics can connect to several different monitoring and ITSM systems. You can connect to one or more of these systems on the Integrations tab. The integrations are categorized according to whether they are data systems or action systems.

Authorization

Use this tab to configure the following options:

- **Roles**—Roles are used to specify the type of data that users in each role can access.
- **Scope Components By Boards and Services**—When a user accesses a board or service, the board or service may contain components from an integration that the user does not have permission to access. Administrators can configure whether users can view details about all components on a board, regardless of the source, or administrators can choose to limit the user to viewing data from specific integrations.
- **Saved Searches Visibility**—Administrators can control who can see and use saved searches. Use the toggle on this page to choose one of the following options:
    - Admin only
    - Everyone

Agents

There is always one active agent, which is called the local agent. For complex implementations of VDX Analytics, you may require multiple remote agents to overcome network boundaries. For example, if you want to use a monitoring system installed on-premises and VDX Analytics is running in Amazon Web Services, you can use the remote agent to communicate with VDX Analytics in the cloud without any open inbound ports on-premises.

Use the Agents tab to download additional agents.

General Settings

- **Downtime**—Administrators can define which states are considered as downtime for the board SLA calculations.
- **Dashboarding Feature**—Administrators can set the refresh interval for the call quality dashboards, which are available under the Analyze menu. The default value is 60 minutes.
- **Notifications and Incident Automation**—Administrators can customize the time interval at whichVantage DX Analytics sends notifications. If you are using incident automation, the setting also determines the interval at which Vantage DX Analytics creates incidents. The default interval is 5 minutes, which is also the minimum that you can configure. The maximum interval is 30 minutes.
- **Consent Messages**—Administrators can create messages that display in a banner at the bottom of the page. Users must accept the message to remove the banner. Administrators can multiple messages and can configure them to display for specific user roles.
- **Product Analytics**—Administrators can enable or disable Product Analytics. When this option is enabled, we collect metrics that help us understand how you use the interface. We use this information to improve future versions of the product.
- **Explorer Feature**—Administrators can enable or disable the Boards Explorer and the Components Explorer tabs. The tabs are enabled by default We

recommend that you disable them for large environments where the Explorer diagrams contain more than 300 objects.

Application Health

The Application Health tab allows you to configure notifications when warnings or errors are raised for an integration or for the VDX Analytics application.

Licensing

Use this tab to view and update licenses.

Storage

Use this tab to control the number of days that VDX Analytics retains data from its integrated source systems. By default, VDX Analytics retains data for 90 days; this value is the maximum.

You can also use this tab to see the amount of data stored for each integration.

Consolidation Rules

Consolidation rules allow you to link together components that have common properties. This feature is helpful if you have components that are monitored by multiple integrations. VDX Analytics can consolidate the components based on rules that you configure. It then displays them as a single component.

For example, if you have a computer that is monitored by SCOM, it may also be inventoried in the ServiceNow CMDB and have security-log data that is monitored by Splunk. VDX Analytics models all of this data in a single object that you can monitor and manage.

The consolidated component displays as a separate component in VDX Analytics. The interface lists Consolidation as the source system for these components because they are created by VDX Analytics rather than retrieved from another monitoring system. The following icon is used throughout the interface to indicate a consolidated component:

The Consolidation Rules page is available when you log in as an administrator. It allows you to add rules that determine how components are consolidated. A table displays the all of the rules, and contains the following information:

- **Component Type**—When you create a consolidation rule, you assign the component type. When components are monitored by multiple source systems, they may be categorized as different types of components by each source system. When you consolidate the components in VDX Analytics, you can choose how you want to categorize the new consolidated component. The following options are available:

- Object
- Group
- Service
- Computer
- Database
- Website
- Virtual Machine

The column displays the consolidation rules that are configured for each type of component.

- **Consolidated Components**—This column shows the number of consolidated components that VDX Analytics has created for each component type.
- **Correlated Components**—This column shows the number of components that are associated with consolidated components.
- **Noise Reduction**—This column shows the reduction in the number of components to manage, as a result of consolidating them into a single component. The noise reduction is measured as a percentage.

Help

The Help page provides version information and contains the following tabs:

- **Resources**—This tab provides links to the Technical Documentation, the Knowledge Base, and the Online User Group.
- **Support**—This tab provides a link to open a support ticket and provides information about how to contact technical support.
- **About**—This tab provides a high-level description of VDX Analytics.

Configuring Integrations

Use the information in this section to complete the following tasks:

Task	Description
"Add a License Key" on page 29	Activate your license.
"Add an Integration" on page 30	Integrate your monitoring systems with VDX Analytics.
"Test an Integration" on page 30	Ensure that monitoring systems are communicating successfully with VDX Analytics.
"Download a Remote Agent" on page 30	Optional. VDX Analytics has a default remote agent; however, complex integrations may require additional remote agents.
"Import Live Maps Services" on page 31	Optional. If you use Savision Live Maps, you can import the business services you have created into VDX Analytics. You can also import pre-defined services from Live Maps.

Add a License Key

After you purchase a license, the support team sends you an email with the license key attached in a text file. Use this procedure to activate the license.

1. From the main menu, select **Settings**.
2. Click the **Licensing** tab.
3. Click the **Add License** button.
4. Paste your license key in the dialog box and click **Activate**.

Add an Integration

You must be a VDX Analytics administrator to perform this procedure. When you configure an integration, you must provide credentials that VDX Analytics can use to access the source system. These user permissions determine the access that VDX Analytics has to the source system. If the user in the source system does not have sufficient permissions, some data may not be visible in VDX Analytics and some functionality—such as the ability to close an alert—may not work.

Before you Begin

Ensure that you have information about how to access the monitoring system. The information required varies depending on the monitoring system. For example, you may need user names and passwords, tenant IDs or client IDs, or URLs where the monitoring system is installed. For a complete list of the information needed, see the *VDX Analytics Integration Guide.*

1. From the main menu, select **Settings**.
   The Integrations tab displays the currently installed integrations.
2. Click the **Add** button at the bottom of the page.
3. Select a monitoring system from the dialog box.
4. Enter the information required for the monitoring system.
5. Click **Save**.

Test an Integration

You must be an administrator to perform this procedure.

1. From the main menu, select **Settings**.
   The Integrations tab displays the currently installed integrations.
2. Select an integration and click the **Test Integration** button.
   A banner displays at the top of the screen to indicate the status.

Download a Remote Agent

A remote agent is needed when it is not possible to connect to the source system from the VDX Analytics web server due to network boundaries. For example, you may need a remote agent because of firewall restrictions or, if you use VDX Analytics in a standalone on-premises deployment, you may authenticate users against a remote Active Directory.

You must be an administrator to perform this procedure.

1. From the main menu, select **Settings**.
2. Click the **Agents** tab.
3. Click the **Download Agent** button.
   A dialog box displays.
4. Click **Save** to download the AgentInstaller.zip file.
5. Unzip the file on the Windows server where you want to install the remote agent and execute the command file.

The command file installs the remote agent using the correct VDX Analytics web server settings and registers with VDX Analytics automatically.

Import Live Maps Services

1. From the main menu, click **Explore**.
2. Select the **Groups & Services** tab.
3. Select a service from a SCOM deployment that has Live Maps installed. The service should have the following raw property: Is Live Maps Service Imported.
4. Click the **Action** button.
5. Click the **Import Live Maps Service** icon.
6. Select the service you want to import and click **OK**.

Dashboards

Use the information in this section to understand the dashboards that are available in VDX Analytics and how you can use them.

Topic	Description
About Dashboards	
"Dashboards for Data Analysis" on page 32	This section describes the dashboards that you can use to analyze data about your Teams or Zoom calls.
"Dashboards for Proactive Monitoring" on page 34	This section describes the dashboards that display data about synthetic transactions, which helps you identify issues proactively.
Working with Dashboards	
"Dashboard Controls" on page 34	This section describes the settings and controls that are available when you work with dashboards.
"Network Diagnostics Diagrams" on page 35	This section describes the data that is available on the network diagnostics diagrams.
"Adding Calls to the Dashboards" on page 37	You can retrieve data about calls that occurred outside of the data collection window if you have a Call ID from the Microsoft CQD.

Dashboards for Data Analysis

The **Data Analysis** menu provides access to dashboards that help you correlate call quality data from a range of sources.VDX Analytics automatically creates these dashboards using data it retrieves from the following sources:

- Microsoft Teams Call Quality Dashboard (CQD)
- Microsoft 365 services

- Vantage DX Monitoring
- AudioCodes Session Border Controllers (SBCs)
- Zoom (if licensed)

If you do not have all of the integrations configured, the dashboard will display "no results found" in some widgets.

Teams Dashboards

The Teams dashboards provide comprehensive information about the call quality that your users are experiencing. You can use them to understand:

- The locations where problems are impacting users.
- The specific users who are experiencing problems with voice quality.
- The percentage of calls that are good, poor, or failed; this information is displayed for the total number of peer-to-peer calls, as well as conference calls and PSTN calls.
- The network issues that impact call quality, such as round-trip time (RTT), packet loss, jitter, and frame rate.
- Connectivity data, such as the connection type, the ISP, and the connected device.
- Teams Meeting room data, including the health state of devices associated with meeting rooms.

The following dashboards are available under the **Data Analysis** menu:

- Teams Overview
- Teams Users
- Teams Locations
- Teams Meeting Rooms
- Teams Phone Licenses Dashboard (available in Enterprise and Professional license packages)

You can also navigate to the following additional dashboards:

- Teams Calls—Navigate to this dashboard from the Users Dashboard by clicking on a Call ID and selecting **Go to Calls Dashboard**.
- Teams Meeting Room Devices—Navigate to this dashboard from the Meeting Rooms Dashboard by clicking on a meeting room and selecting **Go to Meeting Room Devices Dashboard**.

Zoom Dashboards

The Zoom dashboards provide information about the quality of meetings and webinars. You can use them to understand:

- The meetings that experienced the worst call quality.
- The specific users who are experiencing call quality issues.
- Network conditions that caused poor meetings.

The following Zoom dashboards are available under the **Data Analysis** menu:

- Zoom Meeting Overview

- Zoom Participants

You can also navigate to the following additional dashboard:

- Zoom Meeting Details—Navigate to this dashboard from the Zoom Overview dashboard or the Zoom Participants dashboard by clicking on a meeting ID and selecting **Go to Meeting Details**.

For more detailed information about the dashboards, see *Performance Data in Vantage DX*. The guide is available by clicking the following link:

https://documentation.martellotech.com/Solution_
web/MSPerformanceData/index.htm

Dashboards for Proactive Monitoring

The **Proactive Monitoring** menu provides access to a Teams dashboard that contains test results from Vantage DX Monitoring robots. The dashboard helps you proactively monitor metrics that are predictors of call quality.

For more detailed information about proactive monitoring, see *Performance Data in Vantage DX*. The guide is available by clicking the following link:

https://documentation.martellotech.com/Solution_
web/MSPerformanceData/index.htm
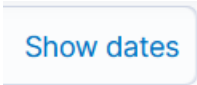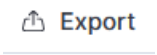
Dashboard Controls

By default, the dashboards refresh every 60 minutes. Administrators can change the refresh interval using the option available on the **Settings > General Settings** page.

For best viewing, we recommend that you use the following settings:

- Screen Resolution: 1920 x 1080 or higher
- Scale: 150% (Windows setting)
- Browser zoom: 100%

The following controls are available on the dashboards:

Icon	Function	Description
Show dates	Time filter options	The dashboards can display data from the past 90 days. There are two options for selecting a time filter: • Quick select—Click the calendar icon to select pre-defined time periods. • Show dates—Click this option to enter specific time periods. After you change the time filter, click the **Update** button to apply the changes. The times shown in the dashboard are based on the timezone in your browser settings.
⊜ − + Add filter	Show and clear filters	This field populates automatically when you select a filter in a widget. You do not need to add a filter in this field. If you select a filter in a widget, you can clear the filter by clicking the **X** in this field.
Ottawa, CA	Text displayed in blue	Text displayed in blue indicates that filter options are available. You can hover over the text and click the **Plus** (+) icon to see the filter options.
☰	Legend	Click this icon to view a legend that describes the colors used on graphs.
⬆ Export	Export	Click this icon to download tabular data as a raw or formatted (CSV) file.

Network Diagnostics Diagrams

The Users Dashboard and the Locations Dashboard both contain a Recent Network Diagnostics table, which lists the results of the most recent network diagnostics tests. It provides information about the number of passed tests and the number of failed tests, up to a maximum of 400 tests.

In addition to the information in the table, Vantage DX provides diagrams to help you understand the test results. There are two ways you can view the diagrams directly from the table:

- Hover over a site in the Site Name column and click the **Plus (+)** icon, then select **View Test Results**. The dashboard displays the Network Testing Summary page. It provides a bar graph that indicates whether the network diagnostics tests passed or failed. You can click on a result to view a network path diagram for a specific test.
- In the Latest Failure Result column, click the **View Results** link to open the Network Path diagram for the latest failed test.

The Network Path diagram shows the network paths from each site to the Microsoft Teams endpoint or to a custom endpoint. These diagrams identify each hop in the network path and use color-coding to indicate the health status of each hop. The hop statuses are:

- **Grey**—Hop is not responding to network testing. This may occur when a server refuses to recognize ICMP requests or de-prioritizes them so that the server response time exceeds the threshold.
- **Green**—Good hop. The network test results do not exceed the established thresholds.
- **Red**—Hop at which poor test results may have started. The threshold was exceeded for at least one of the following tests:
  - Packet loss (10%)
  - Round-trip time (500 milliseconds)
  - Jitter (30 milliseconds)

  The hops thereafter may have poor test results, but may appear with a green status because they are not considered to be the problem hops.

The following image shows an example of a network path between a remote user and the Teams service.

Figure 1: Network Path Diagram: Remote User Example
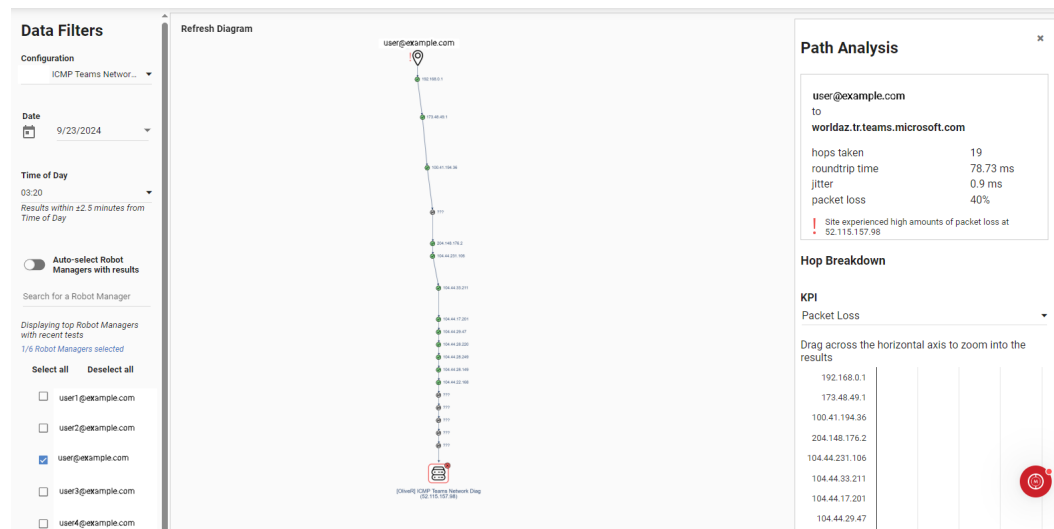
On the Network Path page, you can use the Data Filters panel on the left side to filter and group the elements on the diagram. The options include:

- **Configuration**—By default, the Network Path page is pre-filtered to show information about the site you selected on the Users Dashboard or the Locations Dashboard. You can use the drop-down to view other network diagnostics configurations.
- **Date**—Display results for a selected date. The default is the current date.
- **Time of day**—Display results for a selected time, in 5-minute increments.
- **Auto-select Robot Managers with results**—Toggle this option to On to display only those Robot Managers that have network path test results.
- **Show network owners**—Toggle this option to On to highlight each network owner in the diagram in a different color.

The Path Analysis panel to the right of the diagram provides the following detailed information about each network path that appears in the diagram:

- **Name of the path**—The name of the site to the URL of the endpoint. For example "MySite to worldaz.tr.teams.microsoft.com".
- **Hops taken**—Number of intermediate devices that a packet passes through from the source site to the endpoint.
- **Round-trip time**—The time in milliseconds that it takes a data packet to travel from point A to B and return. This is the value for the entire path.
- **Jitter**—Jitter indicates the size of the buffer that is needed to store packets before they are reconstructed in the correct order. Jitter can cause delays in calls and is an indicator of congestion of the network. This is the value for the entire path.
- **Packet loss**—Percentage of packets that are lost in a given period of time. Packet loss directly affects audio quality. This is the value for the entire path.
- **! messages**—Warning messages that inform you about detected performance issues. Issues that can be related to a specific hop include information about the hop where the path started to experience an issue.
- **Hop Breakdown**—Use the KPI selector to see how each hop in the path contributed to the total value of each of the metrics: round-trip time, jitter, and packet loss.

Adding Calls to the Dashboards

Vantage DX provides you with the option to retrieve data about calls that occurred outside of the data collection window, which is defined in the integration settings in the **Data Retrieval Period (days)** field.

Use the following procedure if you have a Call ID from the Microsoft Call Quality Dashboard (CQD) and would like to view data about that call on the Vantage DX dashboards. You must be an administrator to perform this procedure.

1. From the main menu, select **Settings**.
   The Integrations tab displays the currently installed integrations.
2. Locate the Microsoft Teams CQD integration and click on the **</>** (code) icon.

3. Enter the Call ID of the call you wish to retrieve. To enter multiple Call IDs, separate each ID by a comma.

4. Click **OK**.

> **Note:**
> If you add a Call ID for a call that already exists in the dashboard, you will see duplicate data for the call.

Organizing Data

Use the information in this section to complete the following tasks:

Task	Description
"Perform a Search" on page 40	Search for objects, alerts, or incidents, and save your searches.
"Consolidate Components" on page 46	Consolidate components so that they display as a single object when you view them in VDX Analytics.
"Create a Board" on page 48	Create boards when you want to group data from one or more monitoring systems.
"Create Sub-Boards" on page 49	Optional. Create sub-boards when you want to add child boards to a parent board.
"Create a Synced Board" on page 49	Optional. Create a board that is synced with the source system. The members of the board and the health state are determined by the source system and are not configurable in VDX Analytics.
"Create a Business Service" on page 49	Optional. Create business services when you want to monitor critical services, such as email or order entry, according to the following categories: end user, application, infrastructure, or supplier services.
"Pin Objects to a Board or Business Service" on page 51	Add components to an existing board or business service.
"Configure Rules" on page 52	Optional. Use rules to dynamically add objects to a board or business service.

Task	Description
"Configure Exclusions" on page 53	Optional. Use exclusions in conjunction with rules to refine the scope of objects that are dynamically added to a board or business service.

Perform a Search

The **Explore** menu provides several search functions:

- **Predefined searches**—Sub-menus display that provide access to pre-defined searches. These searches allow you to quickly find data that VDX Analytics has retrieved from the Microsoft Teams CQD integration.
- **Search bar**—The Search bar allows you to search the details or raw properties of each component, alert, and incident.
  - When you enter a search term, VDX Analytics returns results on all tabs, not only on the currently selected tab. If you have any filters enabled on the tabs, the search results are filtered as well. As long as the search term remains in the Search bar, the tabs continue to display information based on that search term.
  - VDX Analytics highlights areas that match the search in yellow. If a search result is returned but no data is highlighted in the main window, that typically indicates that the searched item was found in the details or raw properties. You can view the raw data by selecting the component and clicking the **More Details** button.
- **Saved searches**—The Saved Searches tab allows you to customize searches and save your preferences. You can set filters for the search and select the tab where you want the results to display.

Use the following procedure to search for data.

Before you Begin

- Click **X** to clear any existing searches.

1. From the main menu, click **Explore**.
2. Choose one of the following options:
   - Select a pre-defined search from the sub-menu.
   - Enter a search term in the **Search** bar and press **Enter** to begin the search. See the Related Topics section at the end of this procedure to learn more about the search operators that you can use.
   - To use a saved search, click **Load** in the search bar and select a **Saved Search** from the list, or click the saved searches tab (indicated by a star icon) to see a list of available saved searches.
3. Optional. Filter the search results using the options in the **Filters** pane.

4. If you selected a filter and want to create a new saved search based on your selection, click **Save** in the search bar and complete the following steps:

   - In the Save Current Search dialog box, enter a meaningful name for the search.
   - Ensure **that Save Current Filters** is selected.
   - Click **Save** or click **Save & Add Rule** if you want to pin this search to a board.

Related Topics

-

Search Operators

You can use any of the following terms to include or exclude results from your search:

- AND
- NOT
- OR
- TO

VDX Analytics performs a text search. Some characters are reserved. You cannot search for the following characters unless they are in quotes as part of a search:

```
+ - = && || > < ! ( ) { } [ ] ^ " ~ * ? : \ /
```

Searches are not case-sensitive, unless you are searching on field name. For example, you may want to search on alerts where the Priority field is set to High. In the case of field names, you must use the proper case and formatting to target a field. You can verify the proper name and case of a field by hovering your mouse over the field name. If the field name has a space in it, such as "IP Address," you must enter an escape character (\) in the search to represent the space.

Because the field names are related to the source system, you need to specify the integration type in your search. The format is:

```
source.<integration>. <field name>: <search term>
```

For example, to search for SCOM alerts with a Priority of High, use the following search string: `source.scom.Priority:HIGH`

The following table lists the names to use when you specify an integration in your search.

Table 1: Integration Names

Integration	Search Term

Amazon Web Services	aws
	
	Syntax:
	
	`source.aws.<property>:<value>`
	
	Example:
	
	`source.aws.RegionDisplayName:"US West"`

AppDynamics	AppDynamics
	
	Syntax:
	
	`source.AppDynamics.<property>:<value>`
	
	Example:
	
	`source.AppDynamics.entryPointType:ASP_DOTNET`

AudioCodes	AudioCodesSBC
	
	Syntax:
	
	`source.AudioCodesSBC.<property>:<value>`
	
	Example:
	
	`source.AudioCodesSBC.IPAddress:172.16.29.100`

Cherwell	cherwell
	
	Syntax:
	
	`source.cherwell.<property>:<value>`
	
	Example:
	
	`source.cherwell.next\ Status:Retired`

Microsoft Azure	azure
	
	Syntax:
	
	`source.azure.<property>:<value>`
	
	Example:
	
	`source.azure.state:stopped`

Integration	Search Term

Microsoft Call Quality Dashboard	Office365CQD
	
	Syntax:
	
	`source.Office365CQD.<property>:<value>`
	
	Example:
	
	`source.Office365CQD.GroupType:city`

Microsoft Azure Insights	azureMonitor
	
	Syntax:
	
	`source.azureMonitor.<property>:<value>`
	
	Example:
	
	`source.azureMonitor.Name:"High CPU"`

Microsoft Office 365	Office365
	
	Syntax:
	
	`source.Office365.<property>:<value>`
	
	Example:
	
	`source.Office365.FeatureName:Access`

Microsoft System Center Operations Manager (SCOM)	scom
	
	Syntax:
	
	`source.scom.<property>:<value>`
	
	Example:
	
	`source.scom.Display\ Name:test`

Mitel Performance Analytics	MPA
	
	Syntax:
	
	`source.MPA.<property>:<value>`
	
	Example:
	
	`source.MPA.severity:Critical`

Nagios Core and Xi	nagios
	
	Syntax:
	
	`source.nagios.<property>:<value>`
	
	Example:
	
	`source.nagios.display_name:HTTP`

Integration	Search Term

PRTG Network Monitor	prtg
	
	Syntax:
	
	`source.prtg.<property>:<value>`
	
	Example:
	
	`source.prtg.Host:*.savision.int`

ServiceNow	serviceNow
	
	Syntax:
	
	`source.serviceNow.<property>:<value>`
	
	Example:
	
	`source.serviceNow.number:INC0010021`

SolarWinds	solarWinds
	
	Syntax:
	
	`source.solarWinds.<property>:<value>`
	
	Example:
	`source.solarWinds.ipAddress:192.168.1.100`

Splunk	Splunk
	
	Syntax:
	
	`source.Splunk.<property>:<value>`
	
	Example:
	
	`source.Splunk.Name:"First Alert"`

Vantage DX Diagnostics	NPV
	
	Syntax:
	
	`source.NPV.<property>:<value>`
	
	Example:
	
	`source.NPV.name:Ottawa`

Integration	Search Term

Vantage DX Monitoring	Gizmo
	
	Syntax:
	
	`source.Gizmo.<property>:<value>`
	
	Example:
	
	`source.Gizmo.appAlias:Mailbox`

VMware vCenter	vMwarevCenter
	
	Syntax:
	
	`source.vMwarevCenter.<property>:<value>`
	
	Example:
	
	`source.vMwarevCenter.hostId:"host-24"`

WhatsUp Gold	whatsupgold
	
	Syntax:
	
	`source.whatsupgold.<property>:<value>`
	
	Example:
	
	`source.whatsupgold.DeviceId:28`

Zabbix	zabbix
	
	Syntax:
	
	`source.zabbix.<property>:<value>`
	
	Example:
	
	`source.zabbix.host:VMhost01`

Examples

The following table provides examples of how to use search terms:

Search Term	Results	Notes
sql	ms-sql SQL-svr01	Shows only those results where sql is a word by itself. For example, this search does not find: sqlsvr01 or Devsql
sql	ms-sql sqlsrv01	The asterisk (*) searches for results where the letters sql or SQL exist in any raw property field.

Search Term	Results	Notes
dc?3	dc03 dc13 DCX3	The question mark (?) is a single character wild card.
[192.168.1.101 TO 192.168.1.120]	Any IP address in the specified range.	This syntax is a way to find a range of components.
[dc02 TO dc10]	Any object within the specified range, such as DC05, DC06.	You can search on ranges that are not numerical.
iq AND "Hard Disk"	Returns any results that contain both search terms.	If both terms are not found, then the search will not return any results.
iq OR "Hard Disk"	Returns results that contain either term.	—
iq AND ("Hard Disk" OR NTFS)	Returns results that have IQ and either Hard Disk or NTFS	You can use parentheses ( ) to group certain parts of you query together.

Consolidate Components

Use this procedure to configure consolidation rules. Consolidation rules are a way to link together components that have common properties. This feature is helpful if you have components that are monitored by multiple source systems. VDX Analytics can consolidate the components based on the rules you configure, and then display them as a single component.

When you consolidate components, VDX Analytics creates a new component that represents all of the components it contains. Because the consolidated component is created within VDX Analytics, the interface lists Consolidation as the source system for the component. You assign a component type to the new consolidated component.

VDX Analytics can search object properties provided by the source systems and identify components to consolidate based on an exact match, a partial match, or on whole words. You need to specify the type of match to use when you configure a consolidation rule.

- **Exact match**—Use an exact match when the properties of the objects have the same values in the source system. For example, if both of the source systems have an IP Address field that stores one IPv4 address, the fields will have an exact match.

- **Partial match**—Use a partial match when the source systems store information differently. For example, if one source system has an IP Address field that stores one IPv4 address, but another source system has an IP Address field that stores both an IPv4 and an IPv6 address, the fields will have a partial match.
- **Whole word match**—Use a whole word match when a partial match returns too many results. For example, a rule based on matching a property such as "Computer 1" will include results such as Computer-1, Computer-10, and Computer-11. In cases where a partial match does not provide the correct results, use a whole word match.

1. From the main menu, select **Settings** and click the **Consolidation Rules** tab.
2. Click the expansion icon next to the type of component that you want to make.
3. Click **Add Rule**.
4. To define the rule, enter the following information:

Field	Description
Rule Name	Enter a name for the rule
Description	Enter a description of the rule.
Field Mappings	
Integration Type	Select the source system from the drop-down list.
Field Name	Select the field in the source system to base the consolidation on.
Match Type	When VDX Analytics searches the specified field, it can match components based on an exact match, partial match, or whole words. Select the type of matching to use.

5. Optional. Click **Add A Property** to add another rule.
6. If you create multiple rules, click the arrows next to the integration type to assign a higher or lower priority to the field mapping.
   When VDX Analytics consolidates components, it begins with the first mapping in the list. Any components that are consolidated as a result of the first mapping are not considered when VDX Analytics applies the next mapping in the list.
7. Click **Save**.
8. Click the **Action** button and then click the **Start Consolidation** icon.
9. Click **Ok**.

Create a Board

Boards are a way of organizing groups of objects from one or more monitoring systems. Use the following procedures to create a new board.

There are two ways to create boards. Choose one of the following options:

- and then search for objects and pin them at a later time.
- Search for an object and .

> **Tip:**
> When you create a board, VDX Analytics creates a URL for it. The URL is based on how you are connected to VDX Analytics at the time that you create the board. For example, if you connect to VDX Analytics through localhost, the URL is based on the localhost address. We recommend that when you create a new board, you access VDX Analytics in the same way that all users typically access the application. This practice ensures that the URL of the board is accessible to other users when it is shared. For example, if you configure automatic notifications, the board URL is included in the message sent to recipients.

Create a New Board

1. On the main menu, select **Data Analysis > Boards**.
2. Click the **Add** icon at the bottom right corner.
3. Enter a name for the board.
4. Choose the way that you want the health status reported for the board:
   - Worst-case
   - Best-case
   - Percentage-based
     If you chose percentage-based, enter a percentage.
5. Click **OK**.

Create a Board from Search Results

1. On the main menu and click **Explore**.
2. Select a saved search or search for an object and select it on the related tab.
3. Click the **Action** button and then click the **Pin** button.
4. In the dialog box, click **Create a Board**.
5. Enter a name for the board.
6. Choose the way that you want the health status reported for the board:

- Worst-case
- Best-case
- Percentage-based
  If you chose percentage-based, enter a percentage.

7. Click **Pin it**.

Create Sub-Boards

1. On the main menu, select **Data Analysis > Boards**.
2. Find the board that you want to assign as sub-board and click the icon in the top corner.
3. Click **Actions** and select **Pin**.
4. Select a board from the list. If needed, use the **Filter** field to search for a board.

Create a Synced Board

Create a board that is synced with the source system. The members of the board and the health state are determined by the source system and are not configurable in VDX Analytics. If members are added or deleted in the source system, or if the health state changes in the source system, the board in VDX Analytics automatically updates.

1. On the main menu, click **Explore**.
2. Select a saved search or search for an object and select it on the **Groups & Services** tab.
3. Click the **Action** button and then click the button to create a synced board. A dialog box prompts you to confirm that you want to create a board from the selected group.
4. Click **OK**.
5. Optional. To view the source system, click .

> **Tip:** To create multiple synced boards at once, use the Ctrl or Shift keys when you select groups or services. VDX Analytics creates one synced board for each group or service that you selected.

Create a Business Service

Business services are a way of organizing data about critical business services from one or more monitoring systems. Business services allow you to view information about critical business services, such as email or order entry, according to the following categories: end user, application, infrastructure, or supplier services.

Use the following procedures to create a new business service.

There are two ways to create business services. Choose one of the following options:

- and then search for objects and pin them at a later time.
- Search for an object and .

> **Tip:**
> When you create a business service, VDX Analytics creates a URL for it. The URL is based on how you are connected to VDX Analytics at the time that you create the business service. For example, if you connect to VDX Analytics through localhost, the URL is based on the localhost address. We recommend that when you create a new board, you access VDX Analytics in the same way that all users typically access the application. This practice ensures that the URL of the business service is accessible to other users when it is shared. For example, if you configure automatic notifications, the business service URL is included in the message sent to recipients.

Create a New Business Service

1. On the main menu, select **Data Analysis > Business Services**.
2. Click **Create**.
3. Enter a name and description for the business service.
4. Choose the perspectives that you want to use to calculate the health status for the business service:
   - End user
   - Application
   - Infrastructure

   If you choose multiple perspectives, the status is based on the perspective with the worst health.
5. Choose the way that you want the health status reported for each of the selected perspectives:
   - Worst-case
   - Best-case
   - Percentage-based
     If you chose percentage-based, enter a percentage.
6. Click **Create**.

Create a Business Service from Search Results

1. On the main menu and click **Explore**.

2. Select a saved search or search for an object and select it on the related tab.

3. Click the **Action** button and then click the **Pin to Service** button.

4. In the dialog box, select the **Create a Service** tab.

5. Select a perspective for the object: End User, Application, or Infrastructure.

6. Enter a name and description for the business service.

7. Choose the perspectives that you want to use to calculate the health status for the business service:

   - End user
   - Application
   - Infrastructure

   If you choose multiple perspectives, the status is based on the perspective with the worst health.

8. Choose the way that you want the health status reported for each of the selected perspectives:

   - Worst-case
   - Best-case
   - Percentage-based
     If you chose percentage-based, enter a percentage.

9. Click **Create**.

> **Tip:** You can edit the name, description, and health roll-up setting for a business service from the **Business Services** page. Click the icon at the end of the entry for the business service and select **Details**.

Pin Objects to a Board or Business Service

Use this procedure to add objects to an existing board or business service.

1. On the main menu and click **Explore**.

2. Search for an object. When the results display, select one of the following tabs: **Computers**, **Groups & Services**, or **Components**.

3. Select an object in the list. If needed, filter the list using the options on the left side of the page.

4. Click the **Action** button and choose one of the following options:

   - To pin the object to a board, click the **Pin** button and select a board from the list.
   - To pin the object to a business service, click the **Service** button and select a business service from the list. Choose a perspective and click **Pin It**.

> **Tip:**
> You can add a supplier service to a business service without performing a search. Choose one of the following options:
>
> - On the main menu, select **Data Analysis > Business Services**. Click the icon at the end of the entry for the business service and select **Supplier Services**. In the dialog box, select the supplier services that relate to the selected business service.
> - From the **Business Services** page, open the business service and click the **Action** button. Click **Edit Supplier Services** and select the supplier services that relate to the selected business service.

Configure Rules

Use this procedure to dynamically add objects to a board or business service using rules. You can use any saved search as a rule.

There are two ways to create a rule. Choose one of the following options:

Create a New Rule

1. On the main menu, click **Data Analysis > Explore**.
2. Enter a search term in the **Search bar** and press Enter to begin the search.
3. Filter the search results if necessary.
4. Click **Save** and enter the following information in the dialog box:
   - Name your search.
   - Select the target tab for the object: Computers, Groups & Services, or Components.
5. Click **Save & Add Rule**.
6. Choose one of the following options:
   - To apply this rule to a board, select **Add Rule to Board** and select a board from the list.
   - To apply this rule to a business service, select **Add Rule to Service** and select a service from the list, then choose a perspective.
7. Click **Pin It**.
   A status message indicates that the rule has been added. Click the link to navigate to the board or service.

Create a Rule from an Existing Saved Search

> **Note:** Saved searches that contain alerts or incidents cannot be used as rules.

1. On the main menu, click **Explore**.
2. Select the **Saved Searches** tab and select a saved search.
3. Click the icon in the top corner of the search and select one of the following options:
   - Click **Add Rule to Service** and select a service from the list. Choose a perspective and click **Pin It**.
   - Click **Add Rule to Board** and select a board from the list.

   A status message indicates that the rule has been added. Click the link to navigate to the board or service.

Configure Exclusions

You can configure exclusions after you add a rule to a board or business service. Exclusions are a way of refining rules.

1. Review the board or the perspective in a business service where you added a rule. If the search results included an object that you do not want, click the icon in the upper corner of the object and click **Remove**.
2. Click **OK** to confirm the removal.
   The object is moved to the Exclusions tab.
3. Optional. If you want to reinstate the object, click the **Exclusions** tab.
4. Click the **Action** button and click **Remove Exclusion**.
5. Click **OK** to confirm the change.

Configuring Views

Use the information in this section to complete the following tasks:

Task	Description
"Configure the Boards View" on page 54	Select how you want to view boards.
"View Boards or Business Services in NOC Mode" on page 55	Display boards or business services in a NOC view, where the status colour fills the entire board.
"Configure Table Layouts" on page 55	Change the order of the columns on pages that display data in tabular format.
"Disable the Explorer Feature" on page 56	The Explorer feature is enabled by default. In large environments, retrieving the objects for the diagram may impact performance, and you may prefer to disable this feature.

Configure the Boards View

You can show a maximum of 20, 50, or 100 boards on the Boards page; you can reduce the page load time by decreasing the number of boards to show. You can configure how you want those boards to display information, and how the boards are sorted on the page. Use this procedure to select how many boards to show, and how to display and sort those boards.

1. On the main menu, select **Data Analysis > Boards**.
2. Click the arrow on the left side of the screen to display the **Filters** panel.
3. Click the **Display Top** drop-down and choose to show a maximum of 20, 50, or 100 boards on the page.
   The page header displays the current number of boards shown out of the total number of available boards.
4. Click the **Visualize By** drop-down and select how you want the boards to display information:

- **Pie chart**—Displays the health status of individual objects within the board, shown in pie chart form.
- **Heat map**—In non-NOC mode, displays tiles of colour that indicate the health status of individual objects within the board, as well as the overall health status of the board. In NOC mode, the background colour indicates the health status of the board as a whole.
- **Alerts**—Displays the total number of alerts for all the objects, plus the Mean Time To Resolution (MTTR).
- **Incidents**—Displays the total number of incidents related to the components plus the MTTR.
- **Uptime**—Displays the uptime percentage of the board, calculated over the last 7 days.

5. Click the **Sort By** drop-down and choose whether to sort the boards by the board states or the board names.

Related Topics

To find and filter boards on the Boards page, see .

View Boards or Business Services in NOC Mode

By default, each board or business service shows the health roll-up of the board, as well as the health of the underlying objects. Use this procedure when you prefer a NOC view, where the status color fills the entire board.

1. From the Data Analysis menu, select one of the following options:
   - **Boards**
   - **Business Services**
2. Use the toggle on the upper right side of the page to select one of the following options:
   - **NOC mode**—The color that indicates the overall health status displays as the background of the board or business service.
   - **Non-NOC mode**—Non-NOC mode shows the overall health status of the board, as well as the health state of the individual components pinned to the board. This view displays up to 100 individual objects. If the board has more than 100 objects pinned to it, VDX Analytics displays 100 tiles that represent the health states as a percentage. For example, if 30% of the objects are in a critical state, the view shows 30 tiles as critical.

Configure Table Layouts

Use this procedure to change the order of the columns on pages where the data is displayed in table form. The method differs, depending on the type of table display:

- Some tables have column headers that allow you to click and drag to reposition (for example, the Business Services page).

- Some table pages have a button that allows you to edit the order of table columns (for example, the Computers, Alerts, Incidents, Groups & Services, and Components tabs, which are available on the Explore page).

1. Select the page or tab for which you want to configure display options.
2. Choose one of the following options, based on the type of table page:
    - Click and drag the column headers to reposition the table columns.
    - Click the **Edit your table settings** button, click the arrows to reposition the table columns, and click **Save**.

Disable the Explorer Feature

The Explorer feature is a topology diagram that shows components and their relationships. The feature is available on two tabs in the interface:

- **Boards page**—When you select a board from the **Boards** page, a new page displays, which includes the **Explorer** tab. When you click the tab, VDX Analytics displays a topology diagram that allows you to view board objects and their related objects.
- **Components page**—When you select a component and click the **More Details** icon, a new page displays, which includes the **Explorer** tab. When you click the tab, VDX Analytics displays a topology diagram that allows you to view components and relationships and see the hierarchy of objects.

The Explorer feature is enabled by default. In large environments, retrieving the objects for the diagram may impact performance, and you may prefer to disable this feature. Use the following procedure to disable the feature.

You must be an administrator to perform this procedure.

1. On the main menu, select **Settings > General Settings**.
2. In the **Explorer Feature** section, deselect one or both of the following options:
    - Board Explorer
    - Components Explorer

Managing Boards and Business Services

Use the information in this section to complete the following tasks:

Task	Description
"Change the State of a Board or Business Service" on page 58	Manually change the state of a board.
"Place a Board or Business Service in Maintenance Mode" on page 58	Place a board or business service in maintenance mode when you want to temporarily suppress state changes, notifications and incident automation steps.
"Share a Board or Business Service" on page 60	Give a specified group of users access to a board or business service.
"Locate Critical Issues" on page 60	Find critical issues on boards or groups and services.
"Filter Boards" on page 61	Filter the view to easily find boards on the Boards page.
"Use the Board Explorer" on page 61	View a topology diagram that allows you to view components and explore related components.
"Use the Groups and Services Explorer" on page 62	View a topology diagram that allows you to view groups and services and their related components.
"Use the Components Explorer" on page 63	View a topology diagram that allows you to view components and their relationships.

Change the State of a Board or Business Service

You can manually change the state of a board or business service.

1. From the Data Analysis menu, select one of the following options:
   - **Boards**
   - **Business Services**
2. Open a board or a business service, and click the **Members** tab.
3. Click the **Action** button and then click the **Manual State** button.
   A dialog box displays.
4. Select a state from the drop-down list and click **Update**.

> **Tip:** Alternatively, you can perform this task without opening the board or the business service. From the Boards page, click the icon in the top corner of the board, or from the Business Services page, click the icon at the end of the entry for the business service. Select the appropriate menus and options.

Place a Board or Business Service in Maintenance Mode

Place a board or business service in maintenance mode when you want to temporarily suppress state changes, notifications and incident automation steps.

Choose one of the following options:

-
-

Place a Board or Business Service in Maintenance Mode Immediately

1. From the Data Analysis menu, select one of the following options:
   - **Boards**
   - **Business Services**
2. Open a board or a business service, and click the **Members** tab.
3. Click the **Action** button and then click the **Start Maintenance Now** button.
   A banner indicates that the board was placed in maintenance mode.

> **Tip:** Alternatively, you can perform this task without opening the board or the business service. From the Boards page, click the icon in the top corner of the board, or from the Business Services

> page, click the icon at the end of the entry for the business service. Select the appropriate menus and options.

Schedule Maintenance Mode for a Board or Business Service

1. From the Data Analysis menu, select one of the following options:
    - **Boards**
    - **Business Services**
2. Open a board or a business service, and click the **Members** tab.
3. Click the **Action** button and then click the **Schedule Maintenance Mode** button.
   A dialog box displays.
4. To schedule a maintenance period, enter the following information:

Field	Description
Recurrence Interval	Choose one of the following: • Once • Daily • Weekly • Monthly
Duration	
Start Time	Enter a start time
End Time	Choose one of the following options: • Set a duration (in minutes) for the maintenance period. • Enter a specific time for the maintenance period to end.
Schedule Start and Expiration	
Timezone	Select a timezone from the drop-down list.
Effective Date	Select a start date for the maintenance period.
Expiry Date	Select an end date for the maintenance period. For Daily, Weekly, or Monthly schedules only.

5. Click **Save**.

Tip: Alternatively, you can perform this task without opening the board or the business service. From the Boards page, click the icon in the top corner of the board, or from the Business Services page, click the icon at the end of the entry for the business service. Select the appropriate menus and options.

Tip: You can disable a scheduled maintenance period by using the toggle at the top of the Maintenance Mode dialog box.

Share a Board or Business Service

Use this procedure when you want to give a specified group of users access to a board or business service.

1. From the Data Analysis menu, select one of the following options:
   - **Boards**
   - **Business Services**
2. Open a board or a business service, and click the **Members** tab.
3. Click the **Action** button and then click the **Share** icon.
   A dialog box displays a list of roles.
4. Select a role (a group of users) to share the board with.
5. Click **Save**.

Tip: Alternatively, you can perform this task without opening the board or the business service. From the Boards page, click the icon in the top corner of the board, or from the Business Services page, click the icon at the end of the entry for the business service. Select the appropriate menus and options.

Locate Critical Issues

You can use the Explorer to locate critical issues in your network.

1. Choose one of the following options:
   - On the main menu, select **Data Analysis > Boards**. Open a board and click the **Explorer** tab.
   - On the main menu, click **Explore**. Click **Groups & Services** and select a group or service. Click the **More Details** icon and then select the **Explorer** tab.

- On the main menu, click **Explore**. Click **Components** and select an object. Click the **More Details** icon and then select the **Explorer** tab.
2. Click the **Action** button and click the **Critical Issue Locator** icon.
  The diagram expands, if needed, to show critical issues. Click on the item to display detailed information.

Filter Boards

You can show a maximum of 20, 50, or 100 boards on the Boards page; you can reduce the page load time by decreasing the number of boards to show. Use this procedure to filter the boards.

1. On the main menu, select **Data Analysis > Boards**.
2. Click the arrow on the left side to display the **Filters** panel.
3. Click the **Display Top** drop-down and choose to show a maximum of 20, 50, or 100 boards on the page.
  The page header displays the current number of boards shown out of the total number of available boards.
4. Optional. Click the **Visualize By** drop-down and select the how you want the boards to display information.
5. Optional. Click the **Sort By** drop-down and select how you want the boards sorted on the page.
6. Optional. To display a specific set of boards, enter a search term into the **Search** bar and press **Enter**. You can use the filtering options to further filter the search results.
7. Select the filtering options:
    - **Display Board States**—Filter the boards based on the state of the board. Select one or more states.
    - **Health Rollup Types**—Filter the boards based on the type of health rollup configured for the board. Select one or more rollup types.
    - **Exclude Child Boards**—This option is selected by default. When this is selected, only top-level boards display. Boards that roll up their health state to a higher-level board are not shown.
    - **Display boards with**—Filter the boards based on whether incident automation or notifications are enabled for the board.

Use the Board Explorer

1. From the main menu, select **Data Analysis > Boards**.
2. Open a board and click the **Explorer** tab.
3. Perform any of the following tasks:

Button	Function/Task	Description
—	Change the layout	Drag nodes/items to change how they are displayed.
—	View object information	Hover over the item to see its name. Click on the item/object to open a details pane.
🚀	Action	This button provides access to the following options:
💾	Save	Save all changes that you made to the layout of the topology diagram.
⛁	Get All Nodes	Expand nested boards and display the nodes in a tree diagram.
⤢	Center	Center the diagram on the page.
↺	Revert Network	Revert the diagram to its default display.
●	Critical Issue Locator	Show critical issues. The diagram expands, if needed, to show the location of critical issues.
⟳	Refresh Explorer Data	Refresh the data shown in the diagram.

Use the Groups and Services Explorer

1. From the main menu, click on **Explore**.
2. Select the **Groups & Services** tab.
3. Select a group or service and click the **More Details** icon.
   A new page displays.
4. Click the **Explorer** tab.
5. Perform any of the following tasks:

Button	Function/Task	Description
—	Change the layout	Drag nodes/items to change how they are displayed.

Button	Function/Task	Description
—	View object information	Hover over the item to see its name. Click on the item/object to open a details pane.
(rocket icon)	Action	This button provides access to the following options:
(save icon)	Save	Save all changes that you made to the layout of the topology diagram.
(nodes icon)	Get All Nodes	Expand nested groups and display the nodes in a tree diagram.
(center icon)	Center	Center the diagram on the page.
(revert icon)	Revert Network	Revert the diagram to its default display.
(red dot icon)	Critical Issue Locator	Show critical issues. The diagram expands, if needed, to show the location of critical issues.
(refresh icon)	Refresh Explorer Data	Refresh the data shown in the diagram.

Use the Components Explorer

1. From the main menu, click on **Explore**.
2. Select the **Components** tab.
3. Select a group or service and click the **More Details** icon.
   A new page displays.
4. Click the **Explorer** tab.
5. Perform any of the following tasks:

Button	Function/Task	Description
—	Change the layout	Drag nodes/items to change how they are displayed.

63

Button	Function/Task	Description
—	View object information	Hover over the item to see its name. Click on the item/object to open a details pane.
	Action	This button provides access to the following options:
	Save	Save all changes that you made to the layout of the topology diagram.
	Get All Nodes	Expand nested groups and display the nodes in a tree diagram.
	Center	Center the diagram on the page.
	Revert Network	Revert the diagram to its default display.
	Critical Issue Locator	Show critical issues. The diagram expands, if needed, to show the location of critical issues.
	Refresh Explorer Data	Refresh the data shown in the diagram.

Managing SLA Reporting

Delete this text and replace it with your own content.

Task	Description
"Configure SLO for a Business Service" on page 66	For each business service that you configure, you can set service level objectives (SLO). You can set the SLA goal, as well as the time period and business hours to use in SLA calculations. If you do not want to set SLOs for each business service, you can use the default settings provided by VDX Analytics
"Configure Downtime for SLA Reporting" on page 67	Configure the health states that you want to include in downtime calculations.
"View and Save SLA Availability Data for a Business Service" on page 67	View SLA performance data for a business service and generate a PDF report.
"Generate an On-Demand SLA Report for Multiple Business Services" on page 68	Generate a PDF report of the SLA performance data for multiple business services.
"Schedule an SLA Report" on page 70	Schedule SLA reports and automatically send them to recipients by email.
"Manage Scheduled SLA Reports" on page 71	Change or delete the schedules for SLA reports.
"Exclude Component Outages from SLA Calculations" on page 71	Select one or more components that contributed to downtime and exclude them from SLA calculations.

Configure SLO for a Business Service

Set service level objectives (SLO) for each business service that you configure. This procedure explains how to set the SLA goal, as well as the time period and business hours to use in SLA calculations. To configure the health states that you want to include in downtime calculations, see "Configure Downtime for SLA Reporting" on page 67.

If you do not want to set the SLO for each business service, you can use the default settings provided by VDX Analytics. The default settings are as following:

- The SLA goal is 99%.
- The week begins on the first day of the week configured for your server, which varies according to your location. For example, in some countries, the first day of the week is Monday, while in other countries it is Sunday.
- The time zone is based on the local time of the web server.
- The time period for the calculation is one month.
- Business hours and days are disabled; availability is calculated over a 24-hour period, 7 days a week.

If you edit the SLO settings after you initially configure them, or change the components included in the business service, the SLA calculations are updated for the time period since the change was made. Calculations are not made retroactively.

1. From the main menu, select **Data Analysis > Business Services**.
2. Open a business service and click the **SLA** tab.
3. Click the **Action** button and then click the **Service Level Objectives** button.
4. Enter the following information in the dialog box:
   - **Set a Goal**—Enter the percentage of availability that the service requires. You can enter a percentage with up to three decimal places. If you configure notifications for the business service, VDX Analytics triggers a notification when this goal is breached.
   - **Set a Threshold**— Use this field in conjunction with the notification feature. If you configure notifications for the business service, VDX Analytics can choose to trigger a notification when this threshold is breached. VDX Analytics automatically calculates a threshold based on the goal that you set; however, you can change this value. Because this threshold is always higher than your goal, it allows VDX Analytics to warn you when your SLA goal is close to being breached.
   - **Set a time period**—Select whether you want the SLA calculated over a day, a week, or a month.
   - **Set a time zone**—Select the time zone to use for calculations.
   - **Toggle**—Use the toggle to control whether any downtime that occurs in a 24-hour period impacts your SLA calculations, or whether only downtime that occurs during business hours is used in your SLA calculations. If you choose to use business hours only, define the hours and days.
5. Click **Save**.

> **Tip:** Alternatively, you can perform this task without opening the business service. From the Business Services page, click the icon at the end of the entry for the business service and select the appropriate menus and options.

Configure Downtime for SLA Reporting

Use this procedure to configure the health states that you want to include in downtime calculations. You must be an administrator to perform this procedure.

1. From the main menu, select **Settings > General Settings**.
2. In the **Downtime** section, select the states that you want to include in downtime reporting.

Related Topics

- To configure service level objectives, see "Configure SLO for a Business Service" on page 66.
- To see SLA performance, see "View and Save SLA Availability Data for a Business Service" on page 67.
- To generate an SLA performance report for multiple business services, see "Generate an On-Demand SLA Report for Multiple Business Services" on page 68

View and Save SLA Availability Data for a Business Service

Use this procedure to view SLA availability data for a business service and generate a PDF report. If you edited the SLO settings after you initially configure them, or changed the components in the business service, ensure that you reload the page to see updated data.

The SLA availability data includes the following information:

- **Summary**—Shows the following information about the current SLA status:
  - The availability of the service as a percentage of the SLA goal.
  - The SLA goal.
  - The amount of uptime, in hours, during the specified time period.
  - The targeted amount of uptime, in hours, during the specified time period.
- **Timeline**—Shows the daily status for the selected time period. The SLA goal displays as a line, and bar graphs show the daily status in comparison to the SLA goal. You can hover over the bar graph to see hourly information.
- **Components impacting SLA**—A list of the components that have impacted the SLA during the period shown in the graph. The list shows the duration of

the impact, the name of the component, the perspective, the start and end time of the impact, and the source integration.

1. From the main menu, select **Data Analysis > Business Services**.

2. Open a business service and click the **SLA** tab.

3. Optional. To save SLA data in a PDF, click the **Action** icon and click the **PDF** button.

Generate an On-Demand SLA Report for Multiple Business Services

Generate a PDF report for multiple business services. You can choose a weekly or monthly view of SLA data. For a weekly view, you can choose a time period of one week up to 26 weeks. For a monthly view, you can choose a time period of one month up to 36 months.

To successfully generate a complete multi-service SLA report, the SLO settings for all of the business services to be included in the report should be consistent. The business service SLO settings affect the report generation as follows:

- All business services to be included in the report must have the same weekly or monthly SLO time period. You cannot generate a report for business services with a mix of weekly or monthly SLOs.
- If the business services in the report have different SLO goals, time zones, or business hours, the report does not include combined SLA statistics for all of the business services in the report.

The report contains a general summary of the report information, followed by the combined SLA statistics for all business services included in the report. The remainder of the report contains a breakdown of SLA statistics for each individual business service.

The report includes the following information:

- **Report summary**—Shows general report information including report title, number of services included, weekly or monthly time increments, the specified date range, the health states defined as downtime for the services (as configured in the administrator General Settings), and the report description.
- **Combined SLA statistics**—Shows a view of the combined SLA statistics for all business services in the report:
  - A graph shows the combined actual percent SLA availability versus the configured SLA percent availability goal for all services for the entire reporting period.
  - A graph shows the combined actual uptime versus the targeted amount of uptime for all services for the entire reporting period.
  - A table lists the combined average SLA availability for each week or month in the reporting period. For any weeks or months in the reporting

period with SLA issues, the services that most impacted the SLA availability for those weeks or months are also listed.

- **Individual SLA statistics**—Shows a view of the individual SLA statistics for each business service in the report:
    - A graph shows the actual percent SLA availability versus the configured SLA percent availability goal for this service for the entire reporting period.
    - A graph shows the actual uptime versus the targeted amount of uptime for this service for the entire reporting period.
    - SLA per period—A table lists the average SLA availability for this service for each week or month in the reporting period.
    - Timeline—A chart shows the SLA status for this service over the reporting time period. The average SLA % displays as a line, and bar graphs show a color representation of the SLA status for the weeks or months in the reporting time period according to the SLA goal.
    - Components impacting SLA—A table lists information about the components that have impacted the SLA for this service during the reporting period, including the duration of the impact, the name of the component, the perspective, the start and end time of the impact, and the source integration.
    - Component outages—Tables list details about any component outages, including the outage start time and duration, and whether the outage has been included or excluded from the SLA statistics (as configured on the business service SLA tab).

Use this procedure to generate an SLA availability report for multiple business services.

1. From the main menu, select **Data Analysis > Business Services**.
2. Select multiple services and click **Generate SLA Report**.
   A dialog box displays.
3. In the **Report Options** tab of the dialog box, choose the desired type of view:
    - Month
    - Week
4. Select the start week or month, and the end week or month for the desired time period.
5. Enter a title and description for the report.
   The **Issues** tab displays any potential issues with the selected report options, including SLO setting discrepancies for the selected services to be included in the report.
6. If applicable, review and fix any issues displayed on the **Issues** tab.
7. Click **Generate**, and then click **Close**.
   The report generation begins and continues in the background. When the report is complete, an Information Event notification displays, indicating that

the report is ready for download. The notification remains available for 24 hours.

8. When the notification displays, click the notifications icon, and then click **Download**.
   The report opens and can be saved to a local drive.

Related Topics

- To specify how downtime is calculated, see "Configure Downtime for SLA Reporting" on page 67.
- To configure service level objectives, see "Configure SLO for a Business Service" on page 66.
- To exclude components and recalculate SLA information, see "Exclude Component Outages from SLA Calculations" on page 71.
- To view and save SLA data for a single business service, see "View and Save SLA Availability Data for a Business Service" on page 67.

Schedule an SLA Report

Use this procedure to schedule SLA reports and automatically send them to recipients by email. You can schedule reports for periods ranging from 1 to 3 months.

1. From the main menu, select **Data Analysis > Business Services**.
2. Select one or more business services and click **Schedule SLA Report**.
3. On the **Scheduling Options** tab, enter the following information:
   - **Last**—Enter the number of weeks that you want to report to include
   - **Include current period**—Enable this option if you want to include data up to the current date.
   - **Title**—Enter a title for the report.
   - **Description**—Enter a description for the report.
4. Click the **Delivery & Recipients** tab and complete the following fields:
   - From the **Delivery Method** drop-down, select the email platform to use.
   - In the **Select Recipients** section, select one or more roles to send the report to.
5. Click **Schedule**.

> **Tip:**
> If you want to temporarily stop scheduled reports, you can use the **Toggle to disable SLA Report scheduling** on the **Scheduling Options** tab. This toggle allows you to retain your configuration options and suspend and resume the report as needed.

Manage Scheduled SLA Reports

Use this procedure to change or delete the schedules for SLA reports.

1. From the main menu, select **Data Analysis > Business Services**.
2. Click **Manage SLA Reports**.
3. In the Report Schedules section, search for the name of a schedule. When you select a schedule, the Business Services section lists the business services associated with that schedule.
4. Choose one of the following options:
   - Click the edit icon to change the report schedule.
   - Click the delete icon to remove the schedule.

> **Tip:**
> If there are too many business services associated with the schedule to display on the panel, use the **Search** field in the business services section. Simply type the name of the business service; do not press **Enter**.

Exclude Component Outages from SLA Calculations

Use this procedure to select one or more outages that contributed to downtime and exclude them from SLA calculations. For example, if a component was out of service due to maintenance, but maintenance mode was not scheduled, you can choose that specific outage and exclude it from the SLA calculations.

When you exclude an outage, it takes a few minutes before VDX Analytics recalculates the SLA. An exclamation icon (!) displays while SLA calculations are outdated. VDX Analytics automatically updates the calculation after a few minutes and the icon is cleared. You can update the calculation manually by clicking the Refresh icon on the SLA tab, or the Refresh button on the business services overview page.

1. From the main menu, select **Data Analysis > Business Services**.
2. Open a business service and click the **SLA** tab.
3. On the **SLA** tab, review the **Components Impacting SLA** table and locate the entry that you want to exclude.
4. Expand the entry, select the check box, and click **Exclude**.
5. In the dialog box, add a note and click **Save**.
   The SLA calculations update automatically.

Managing Notifications and Incidents

Use the information in this section to complete the following tasks:

Task	Description
Notifications for Boards and Business Services	
"Configure Notifications for Boards and Business Services" on page 73	Configure a notification that is triggered when a board or business service is shared, when its state changes, or when there is a new alert or new incident. Notifications can also be triggered when an SLA goal has been breached, or when it is about to be breached.
Dashboard Notifications	
Configure notifications for dashboards: • "Understanding Dashboard Notifications" on page 76 • "Configure Dashboard Notifications" on page 77	Configure notifications based on the call quality metrics that Vantage DX retrieves from your Microsoft Call Quality Dashboard.
Notifications for Application Health	
"Configure Notifications for Application Health" on page 83	Configure notifications that are triggered when warnings or errors are raised for an integration or for the Vantage DX application.
Incidents and Alerts	

Task	Description
"Configure Incident Automation" on page 85	If you have integrated an ITSM system with VDX Analytics, you can automate the creation of incidents.
"Link an Alert to an Existing Incident" on page 86	Link an alert on a board or business service to an existing incident in your ITSM system.
"Create a New Incident for an Alert" on page 86	Create a new incident in your ITSM system for an alert that is reported on a board or business service.
"Resolve an Alert" on page 87	When an alert on a board or business service has been resolved, you can close the incident in your ITSM system from within VDX Analytics.
"Configure the Interval for Notifications and Incidents" on page 87	Optional. Configure the time interval at which VDX Analytics sends notifications. If your organization is using incident automation, the setting also determines the interval at which VDX Analytics creates incidents.

Configure Notifications for Boards and Business Services

You can configure VDX Analytics to send a notification when a board or business service is shared, when its state changes, or when there is a new alert is raised or resolved, or when there is a new incident. You can also receive notifications when your SLA goal has been breached, or when it is about to be breached.

VDX Analytics checks for these events every 5 minutes. At the end of the 5-minute interval, VDX Analytics sends a separate notification for each type of event. The following table lists the types of events that can trigger a notification, and describes how notifications are sent for that event.

Table 2: Notifications in VDX Analytics

Event	Description
Alerts	VDX Analytics sends one notification that contains information about all the alerts that have occurred within the last 5 minutes.

Event	Description
Incidents	VDX Analytics sends one notification that contains information about all the incidents that have been created within the last 5 minutes.
State changes for boards and business services	VDX Analytics sends one notification for a state change that has occurred within the last 5 minutes. If the state has changed multiple times within that 5-minute interval, only the most recent change is reported.
Shared boards and business services	VDX Analytics sends a notification only when the board or business service is shared with another role.
Service SLA about to breach	VDX Analytics checks the SLA calculations for business services every 5 minutes and sends sends one notification if the threshold that you set has been breached in that interval.
Service SLA breached	VDX Analytics checks the SLA calculations for business services every 5 minutes and sends sends one notification if the goal that you set has been breached in that interval.

You can configure notifications to send emails, to post a message to a Microsoft Teams channel, or to execute PowerShell scripts. The option to execute PowerShell scripts gives you the flexibility to configure a range of actions in response to the notification. For example, you can execute a PowerShell script that generates an SMS message or that sends a message to a Slack channel. If you choose to execute 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

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](#)

Before you Begin

If you want to configure email notifications, ensure that you have configured an email integration and an email address before you begin. You can configure an email address to use for notifications when you configure a role. For more information, see "Create a Role" on page 89.

If you are sending notifications to a Teams channel, ensure that you have configured the integration for the Teams notifications.

If you are using a PowerShell script to manage notifications, ensure that you have configured the PowerShell integration. In addition:

- Ensure that you enter the full name of the PowerShell script in the integration settings.
- You must download and install a remote agent; see "Download a Remote Agent" on page 30 for more information.
- If you are configuring a notification to trigger a PowerShell script, ensure that you copy the script to following folder on the machine where the remote agent is installed: **C:\Program Files\Martello\Martello Vantage DX Analytics Agent\PSScripts**

1. From the Data Analysis menu, select one of the following options:
   - **Boards**
   - **Business Services**
2. Open a board or a business service, and click the **Members** tab.
3. Click the **Action** button and then click the **Notification Settings** button. A dialog box displays.
4. Select an option from the **Trigger** drop-down list.

> **Note:**
> The trigger **New Teams Outage for Board** is designed for use with boards that have three or more Robot Managers at different locations that are monitoring the Teams Advanced workload. This trigger is not supported for business services. When you select this trigger, Vantage DX notifies you if Robot Managers from three or more different locations report critical issues when accessing Teams.

5. Select an option from the **Action** drop-down list:
   - Email Notification
   - Microsoft Teams Notification—Select the Teams channel integration from the list.
   - PowerShell script—Select a PowerShell script from the drop-down menu or type the name of the script.

   The available Action options are dependent on the integrations that are configured for your environment.
6. Click **+** to add the notification.
7. Select the **Recipient List** tab. Adding recipients is only required for email notifications.
   The option to Notify All Recipients is enabled by default.
8. To send notifications to specific recipients, click the slider to disable the default and select recipients from the list.
9. Click **Save**.

> **Tip:** Alternatively, you can perform this task without opening the board or the business service. From the Boards page, click the icon in the top corner of the board, or from the Business Services page, click the icon at the end of the entry for the business service. Select the appropriate menus and options.

Understanding Dashboard Notifications

You can configure notifications based on call quality metrics that Vantage DX retrieves from your Microsoft Call Quality Dashboard. Dashboard notifications work differently than other notifications in Vantage DX:

- Notifications for boards and business services are triggered when there are changes to the state of the board or business service, when a board or business service is shared, or when an SLA threshold is reached.
- Dashboard notifications are based on searches and are triggered when the search criteria is met. The searches use a syntax designed specifically for dashboard data.

When you configure a dashboard notification, you specify search criteria and a time frame for the data. For example, you can configure a search for users who experienced more than 5 poor calls in the past 48 hours. To use this feature, each search must be pinned to its own board. You can then configure a notification that is triggered if the search criteria is met.

To help you get started with dashboard notifications, Vantage DX automatically creates a set of boards based on searches for CQD data. The main board is named "Microsoft Teams <integration name>," where <integration name> is the name that you specify when you configure the integration between Vantage DX and your

Microsoft CQD. The main board contains a sub-board for each of the following searches:

- Users with poor calls within 24 hours
- Users with poorly rated calls within 7 days
- Users with Wi-Fi Signal strength issues within 7 days
- Locations with poor calls within 1 month

If you want to receive notifications when the search criteria is met, you can configure notifications for the board that corresponds with any of these searches.

Because these boards are based on searches, the health state of these boards is determined by the search results. If there are no results that match the search criteria—for example, if there are no users who experienced poor calls within the past 24 hours—the health state of the board is green. If there are results that match the search criteria, the health state of the board is red.

You can view the default boards by clicking the main menu and selecting **Data Analysis > Boards**.

> **Note:**
> If your instance of Vantage DX was deployed prior to Release 3.17 (June 2024), it will not include these default boards. However, the searches are available under the **Explore** menu, and you can use them to create boards. Ensure that you pin only one search to each board.

Configure Dashboard Notifications

Use the information in this section to configure notifications based on call quality metrics that Vantage DX retrieves from your Microsoft Call Quality Dashboard or from your Zoom integration.

Several types of notifications are available. You can configure Vantage DX to send emails, to post a message to a Microsoft Teams channel, or to execute a PowerShell script. The option to execute a PowerShell script gives you the flexibility to configure a range of actions in response to the notification. For example, you can execute a PowerShell script that generates an SMS message or that sends a message to a Slack channel. If you choose to execute 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

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

Before you Begin

If you want to configure email notifications, ensure that you have configured an email address before you begin. You can configure an email address to use for notifications when you configure a role. For more information, see "Create a Role" on page 89.

If you are sending notifications to a Teams channel, ensure that you have configured the integration for the Teams notifications.

If you are using a PowerShell script to manage notifications, ensure that you have configured the PowerShell integration. In addition:

- Ensure that you enter the full name of the PowerShell script in the integration settings.
- You must download and install a remote agent; see "Download a Remote Agent" on page 30 for more information.
- If you are configuring a notification to trigger a PowerShell script, ensure that you copy the script to following folder on the machine where the remote agent is installed: **C:\Program Files\Martello\Martello Vantage DX Analytics Agent\PSScripts**

The procedure you need to perform depends on whether your instance of Vantage DX was initially deployed prior to Release 3.17 (June 2024), or after that release. Choose one of the following options:

- "Teams Notifications" on page 78
- "Zoom Notifications" on page 80
- "Vantage DX Instances Prior to Release 3.17 (June 2024) " on page 82

Teams Notifications

1. Optional. Perform this step if you use Teams Phone and want to receive notifications about PSTN performance.

- Click **Explore** and on the **Saved Searches** tab, find the search named "Users with SIP response 408 within 7 days."
- Click on the search to open it. The query displays in the **Search** bar. Edit the query to replace "www.abcd.com" with the address of your PSTN trunk; ensure that you retain the quotation marks around the address. Click **Save**.
- Enter a name for the search. The name must be different than the default name. For example, enter a name such as "Users with SIP Errors."
- From the **Target Tabs** drop-down, select **Users**. Click **Save & Add Rule**.
- Enable the toggle so that the board status is based on whether the search returned results. If there are no results that match the search criteria—for example, if there are no users who received a 408 response within the last 7 days—the health state of the board is green. If there are results that match the search criteria, the health state of the board is red.
- Click **Add Rule to Board**.
- Click **Create a Board**.
- Enter a name (such as "Users with SIP response errors") and click **Pin It**. A confirmation message displays. Click the link in the message to go to your new board.
- Click the **Action** icon and click **Pin**.
- On the **Choose a Board** tab, use the **Search** field to find the board named "Microsoft Teams <integration name>," where <integration name> is the name that you specified when you configured the integration between Vantage DX and your Microsoft CQD.
- Select it from the list. Your new board for users with SIP errors is now pinned as a sub-board of your "Microsoft Teams <integration name>" board.

2. Select **Data Analysis > Boards** from the main menu and locate the board named "Microsoft Teams <integration name>," where <integration name> is the name that you specified when you configured the integration between Vantage DX and your Microsoft CQD. The main board contains a sub-board for each of the following searches:
   - Users with poor calls within 24hrs
   - Users with poorly rated calls within 7 days
   - Users with Wi-Fi Signal strength issues within 7 days
   - Locations with poor calls within 1 month
   - Users with SIP response errors (available only if you performed Step 1).

3. To receive notifications when any of these conditions occur, click the **More** icon (three dots) in the top corner of the sub-board and select **Edit > Notifications**.
   A dialog box displays.

4. From the **Trigger** drop-down list, select **Board State Change**.

5. Select an option from the **Action** drop-down list:
   - Email Notification

- Microsoft Teams Notification—Select the Teams channel integration from the list.
- PowerShell script—Select a PowerShell script from the drop-down menu or type the name of the script.

The available Action options are dependent on the integrations that are configured for your environment.

6. Click **+** to add the notification.
7. Select the **Recipient List** tab. Adding recipients is only required for email notifications.
   The option to Notify All Recipients is enabled by default.
8. To send notifications to specific recipients, click the slider to disable the default and select recipients from the list.
9. Click **Save**.

Zoom Notifications

Use this procedure to configure a notification if a Zoom user has experienced a MOS of less than 3.5 in the past 24 hours.

1. Select **Data Analysis > Boards** from the main menu and locate the board named "Zoom <integration name>," where <integration name> is the name that you specified when you configured the integration.
2. Open thesub-board named "Zoom Users with poor experience within 24 hours."
3. To receive notifications when this condition occurs, click the **More** icon (three dots) in the top corner of the sub-board and select **Edit > Notifications**.
   A dialog box displays.
4. From the **Trigger** drop-down list, select **Board State Change**.
5. Select an option from the **Action** drop-down list:
   - Email Notification
   - Microsoft Teams Notification—Select the Teams channel integration from the list.
   - PowerShell script—Select a PowerShell script from the drop-down menu or type the name of the script.

   The available Action options are dependent on the integrations that are configured for your environment.

6. Click **+** to add the notification.
7. Select the **Recipient List** tab. Adding recipients is only required for email notifications.
   The option to Notify All Recipients is enabled by default.
8. To send notifications to specific recipients, click the slider to disable the default and select recipients from the list.
9. Click **Save**.

Vantage DX Instances Deployed in Release 3.17 (June 2024) or Later

1. Optional. Perform this step if you use Teams Phone and want to receive notifications about PSTN performance.

   - Click **Explore** and on the **Saved Searches** tab, find the search named "Users with SIP response 408 within 7 days."

   - Click on the search to open it. The query displays in the **Search** bar. Edit the query to replace "www.abcd.com" with the address of your PSTN trunk; ensure that you retain the quotation marks around the address. Click **Save**.

   - Enter a name for the search. The name must be different than the default name. For example, enter a name such as "Users with SIP Errors."

   - From the **Target Tabs** drop-down, select **Users**. Click **Save & Add Rule**.

   - Enable the toggle so that the board status is based on whether the search returned results. If there are no results that match the search criteria—for example, if there are no users who received a 408 response within the last 7 days—the health state of the board is green. If there are results that match the search criteria, the health state of the board is red.

   - Click **Add Rule to Board**.

   - Click **Create a Board**.

   - Enter a name (such as "Users with SIP response errors") and click **Pin It**. A confirmation message displays. Click the link in the message to go to your new board.

   - Click the **Action** icon and click **Pin**.

   - On the **Choose a Board** tab, use the **Search** field to find the board named "Microsoft Teams <integration name>," where <integration name> is the name that you specified when you configured the integration between Vantage DX and your Microsoft CQD.

   - Select it from the list. Your new board for users with SIP errors is now pinned as a sub-board of your "Microsoft Teams <integration name>" board.

2. Select **Data Analysis > Boards** from the main menu and locate the board named "Microsoft Teams <integration name>," where <integration name> is the name that you specified when you configured the integration between Vantage DX and your Microsoft CQD. The main board contains a sub-board for each of the following searches:

   - Users with poor calls within 24hrs

   - Users with poorly rated calls within 7 days

   - Users with Wi-Fi Signal strength issues within 7 days

   - Locations with poor calls within 1 month

   - Users with SIP response errors (available only if you performed Step 1).

3. To receive notifications when any of these conditions occur, click the **More** icon (three dots) in the top corner of the sub-board and select **Edit > Notifications**.
   A dialog box displays.

4. From the **Trigger** drop-down list, select **Board State Change**.

5. Select an option from the **Action** drop-down list:

   - Email Notification
   - Microsoft Teams Notification—Select the Teams channel integration from the list.
   - PowerShell script—Select a PowerShell script from the drop-down menu or type the name of the script.

   The available Action options are dependent on the integrations that are configured for your environment.

6. Click **+** to add the notification.

7. Select the **Recipient List** tab. Adding recipients is only required for email notifications.
   The option to Notify All Recipients is enabled by default.

8. To send notifications to specific recipients, click the slider to disable the default and select recipients from the list.

9. Click **Save**.

Vantage DX Instances Prior to Release 3.17 (June 2024)

1. Select one of the following pre-defined searches:

   - From the **Explore** menu, select one of the following:

     - Users with poor calls within 24hrs
     - Users with poorly rated calls within 7 days
     - Users with Wi-Fi Signal strength issues within 7 days
     - Locations with poor calls within 1 month

   - If you are using Teams Phone, click **Explore** and on the **Saved Searches** tab, find the search named "Users with SIP response 408 within 7 days."

     - Click on the search to open it. The query displays in the **Search** bar.
     - Edit the query to replace "www.abcd.com" with the address of your PSTN trunk; ensure that you retain the quotation marks around the address.

2. In the Search bar, click **Save**.

3. Enter a name for the search. We recommend that you use a name that describes the search; this name will be used as the board name by default.

4. From the **Target Tabs** drop-down, select one of the following options:

   - **Locations**—When you select this option, the query returns results that are focused on locations that experienced problems.
   - **Users**—When you select this option, the query returns results that are focused on users that experienced problems.
   - **Offices**—When you select this option, the query returns results that are focused on the offices that experienced problems.

5. Click **Save and Add Rule**.

6. Enable the toggle so that the board status is based on whether the search returned results. If there are no results that match the search criteria—for

example, if there are no users who experienced poor calls within the past 24 hours—the health state of the board is green. If there are results that match the search criteria, the health state of the board is red.

7. Click **Add Rule to a Board**.

8. Click **Create a Board**.

> **Note:**
> You can add one query to a board. We recommend that you create a new board specifically for each query. If you use an existing board, ensure that there are no other rules or queries associated with it.

9. Click **Pin It**. Do not select a Health Roll-up Type; the board status is not based on this criteria and this setting is not needed.
   A confirmation message displays and provides a link to the new board.

10. Click the link to navigate to the new board.

11. Click the **More** icon (three dots) in the top corner of the board and select **Edit > Notifications**.
    A dialog box displays.

12. From the **Trigger** drop-down list, select **Board State Change**.

13. Select an option from the **Action** drop-down list:
    - Email Notification
    - Microsoft Teams Notification—Select the Teams channel integration from the list.
    - PowerShell script—Select a PowerShell script from the drop-down menu or type the name of the script.

    The available Action options are dependent on the integrations that are configured for your environment.

14. Click **+** to add the notification.

15. Select the **Recipient List** tab. Adding recipients is only required for email notifications.
    The option to Notify All Recipients is enabled by default.

16. To send notifications to specific recipients, click the slider to disable the default and select recipients from the list.

17. Click **Save**.

Configure Notifications for Application Health

You can configure VDX Analytics to send a notification when warnings or errors are raised for an integration or for the Vantage DX application.

Warnings and errors are raised when the following conditions occur:

- **Integration warnings** are raised when data retrieval is taking longer than expected.

- **Integration errors** are raised when VDX is unable to complete a health check or is unable to retrieve data, or when a license has expired.
- **System warnings** are raised when Elasticsearch is being updated or is almost at capacity, or when your Vantage DX license is about to expire.
- **System errors** are raised when Vantage DX is unable to:
    - Connect or synchronize with the remote agent.
    - Connect to Elasticsearch or execute tasks such as updates and queries.
    - Consolidate components.
    - Schedule or generate an SLA report.
    - Calculate or display the health state of a business service.
    - Calculate or display the health state of a board, or synchronizing data.
    - Update saved search counts.
    - Create automated incidents.
    - Set the Maintenance Mode schedule for board or business service
- A system error is also raised if your Vantage DX license has expired or is invalid.

By default, notifications related to application health are disabled. You must be an administrator to enable these notifications.

Before you Begin

If you want to configure email notifications, ensure that you have configured an email integration and assigned an email address to a role. For more information, see "Create a Role" on page 89.

If you are sending notifications to a Teams channel, ensure that you have configured the integration for the Teams notifications.

1. From the main menu, select **Settings**.
2. Click the **Application Health** tab.
3. Enable the **Application Health** toggle.
4. Select from the following options:
    - **System Warning**—Select this option if you want to receive notifications about system warnings.
    - **System Error**—Select this option if you want to receive notifications about system errors.
    - **Integration warnings**—Enable the Notify All toggle if you want to receive notifications about all integrations. If you want to receive notifications only about specific integrations, you can use the search field or scroll through the list of integrations and select specific ones to enable.
    - **Integration errors**—Enable the Notify All toggle if you want to receive notifications about all integrations. If you want to receive notifications only about specific integrations, you can use the search field or scroll through the list of integrations and select specific ones to enable.

5. Select one of the following integrations from the **Delivery Method** drop-down list:

   - Microsoft Teams Notifications
   - An email integration. If you choose an email integration, Vantage DX displays a list of roles and the email address associated with each role. Select one or more roles from the from the list.

6. Choose one of the following options to determine when the notification is sent. If you choose to send the notification after an interval of time, Vantage DX will check whether the error is still occurring before sending the notification. We recommend that you send notifications after an interval.

   - Send Immediately
   - Send after 1 Minute
   - Send after 3 Minutes
   - Send after 5 Minutes

7. Click **Save**.

Configure Incident Automation

Use this procedure to automate the creation of incidents in your ITSM system. When you enable this feature, VDX Analytics creates an incident for every new alert raised. If you have existing alerts, you can manually create an incident from the VDX Analytics interface; see "Link an Alert to an Existing Incident" on page 86.

1. From the Data Analysis menu, select one of the following options:

   - **Boards**
   - **Business Services**

2. Open a board or a business service.

3. Click the **Action** button and then click the **Configure Incident Automation** button.
   A dialog box displays.

4. Enter information for the **Incident Creation Properties** and **Incident Workflow Properties**. The information required depends on the ITSM system that is integrated with VDX Analytics.

5. By default, VDX Analytics resolves all alerts when the incident is closed. You can deselect this option if desired.

6. Click **Create**.

> **Tip:** Alternatively, you can also configure incident automation from a Saved Search, from the Boards page, or from the Business Services page. Click the icon in the upper corner of the saved search or board, or click the icon at the end of the business service row. Select the appropriate **Incident Automation** menus

and options, and enter the properties for incident creation and
incident workflow.

Link an Alert to an Existing Incident

Use this procedure to link an alert on a board or business service to an existing incident in your ITSM system.

1. From the Data Analysis menu, perform one of the following steps:
   - Click on **Explore** and click the **Alerts** tab.
   - Select **Boards**. Open a board and select the **Alerts** tab.
   - Select **Business Services**. Open a business service and select the **Alerts** tab.
2. From the **Alerts** tab, select an alert.
   A window opens to show the alert details.
3. Click the **Action** button and click the **Link** button.
4. Select an ITSM system as the **Source**.
5. Select an incident from the list. Use the search function if needed.
6. By default, VDX Analytics resolves all alerts when the incident is closed. You can deselect this option if desired.
7. Click **Link**.
   A message confirms that the alert has been successfully linked.

Create a New Incident for an Alert

Use this procedure when you want to create new incident in your ITSM system for an alert that is reported on a board or business service.

If you configured incident automation, VDX Analytics creates an incident and you do not need to perform this procedure.

1. From the Data Analysis menu, perform one of the following steps:
   - Click on **Explore** and click the **Alerts** tab.
   - Select **Boards**. Open a board and select the **Alerts** tab.
   - Select **Business Services**. Open a business service and select the **Alerts** tab.
2. From the **Alerts** tab, select an alert.
   A window opens to show the alert details.
3. Click the **Action** icon and click the **New Incident** button.
4. Select an ITSM system as the **Source**.
5. Complete the fields for the incident. The information required depends on the ITSM system that is integrated with VDX Analytics.
6. By default, VDX Analytics resolves all alerts when the incident is closed. You can deselect this option if desired.

7. Click **Create**.
   A message confirms that the alert has been successfully linked.

Resolve an Alert

Use this procedure when an alert on a board or business service has been resolved and you want to close the incident in your ITSM system from within VDX Analytics.

1. From the Data Analysis menu, perform one of the following steps:
   - Click on **Explore** and click the **Alerts** tab.
   - Select **Boards**. Open a board and select the **Alerts** tab.
   - Select **Business Services**. Open a business service and select the **Alerts** tab.
2. From the **Alerts** tab, select an alert.
   A window opens to show the alert details.
3. Click the **Action** icon and click the **Resolve** button.
   A message displays to confirm that the alert is resolved.

Configure the Interval for Notifications and Incidents

Use this procedure to configure the time interval at which VDX Analytics sends notifications. If your organization is using incident automation, the setting also determines the interval at which VDX Analytics creates incidents.

You must be an administrator to perform this procedure.

1. From the main menu, select **Settings**.
2. Click the **General Settings** tab.
3. Under **Notifications and Incident Automation**, enter a time interval in minutes. The default interval is 5 minutes, which is also the minimum that you can configure. The maximum interval is 30 minutes.
4. Click **Save**.

Managing Users

User permissions in VDX Analytics are based on roles. VDX Analytics includes two default roles:

- **Administrators**—Users assigned to this role have read-write access to everything in VDX Analytics.
- **Operators**—Users assigned to this role have access to any integrations, boards, and business services that the administrator provisions for the role.

Administrators can create additional roles, and can further refine permissions by scoping the extent of information that users can access.

> **Note:**
> If you are using Vantage DX to provide managed services for your customers, follow the procedures provided in the "Manage User Access" section the *Vantage DX Deployment Guide for Service Providers*.

Use the information in this section to complete the following tasks:

Task	Description
"Create a Role" on page 89	Create roles for the different types of users in your organization.
"Assign Users to Roles" on page 89	Assign users to a specific role.
"Add Integrations to a Role" on page 90	Manage the integrations that can be viewed by users in different roles.
"Add Boards or Business Services to a Role" on page 90	Manage how users in different roles can access boards and business services.

Task	Description
"Add Dashboards to a Role" on page 90	Select the dashboards that users in each role can view.
"Scope Access" on page 91	When a user accesses a board or service, the board or service may contain components from an integration that the user does not have permission to access. Configure whether the user can view all information on a board, regardless of the source, or limit the user to viewing data from specified integrations. The scope setting is global, and applies to all roles that are defined in VDX Analytics.
"Create a Consent Message" on page 91	Create a custom message that displays in a banner at the bottom of the page. Users must accept the message to remove the banner.
"Configure Access to Saved Searches" on page 92	Control who can see and use saved searches.

Create a Role

Use this procedure to create roles for the different types of users in your organization. You can use roles to manage access to data and functionality in VDX Analytics.

You must be an administrator to perform this procedure.

1. From the main menu, select **Settings**.
2. Click the **Authorization** tab.
3. Click the **Add** button.
4. Enter a name for the role and click **Create**.
5. On the **Claim Mappings** tab, enter the name of the customer group in the **Claim Value** field. Use the format `/Customers/<customername>`.
6. In the **Email** field, enter the email address to use for notifications. It is a best practice to use a distribution list for this field.
7. Click **Add**.

Assign Users to Roles

Use this procedure to assign users to a specific role.

You must be an administrator to perform this procedure.

1. From the main menu, select **Settings**.
2. Click the **Authorization** tab.
3. Select a role from the list.
4. Click the **Add** button.

5. Enter the name of the user you want to add and click **Search**.
A list displays.

6. Select the user and click **Add**.

Add Integrations to a Role

Use this procedure to manage the integrations that can be viewed by users in different roles.

You must be an administrator to perform this procedure.

1. From the main menu, select **Settings**.

2. Click the **Authorization** tab and select a role.
A new page displays.

3. Click a role and select **Integrations**.

4. Click the **Add** button.

5. Select an integration from the list and click **Add**.

6. Optional. If you want users in this role to have read-only access to the integration, select the **Read-only** box.

Add Boards or Business Services to a Role

Use this procedure to allow users in a specified role to access boards and business services.

You must be an administrator to perform this procedure.

1. From the main menu, select **Settings**.

2. Click the **Authorization** tab and select a role.
A new page displays.

3. Select one of the following options:

   - **Boards**
   - **Business Services**

4. Click the **Add** button

5. Select one or more boards or business services from the list and click **Add**.

6. Optional. If you want users in this role to have read-only access to the board or business service, select the **Read-only** box.

Add Dashboards to a Role

Use this procedure to select the dashboards that users in each role can view.

You must be an administrator to perform this procedure.

1. From the main menu, select **Settings**.

2. Click the **Authorization** tab and select a role.
A new page displays.

3. Click a role and select **Dashboards**.

4. Click the **Add** button.

5. Select one or more dashboards from the list.

6. Click **Add**.

To view data in the dashboards, ensure that integrations are also added to the role. See "Add Integrations to a Role" on page 90.

Scope Access

You can refine roles by specifying the extent—or the scope—of information that users can access. The scope setting is global, and applies to all roles that are defined in VDX Analytics.

When you configure roles, you specify the integrations and the boards and services that users assigned to the role can access. However, boards and services may display components that are monitored by an integration that is not configured for a specific role. You can use the scope setting to determine whether:

- Users can view details about all components on a board or service, regardless of the source.
- Users are limited to viewing data from specified integrations.

1. From the main menu, select **Settings > Authorization**.

2. In the **Scope Components By Boards and Services** section, select one of the following options:

   - **Scope by source**—Users are restricted to viewing components from integrations they have access to. If you are using Vantage DX to provide managed services, you must select this option.
   - **Scope by boards and services**—Users can view details about all components on a board or service, even if the component is from an integration that they do not have access to. Detailed information includes properties, related alerts, and incidents.

Related Topics

- To manage the integrations that users can access, see "Add Integrations to a Role" on page 90.
- To manage the boards and business services that users can access, see "Add Boards or Business Services to a Role" on page 90.

Create a Consent Message

Use this procedure to add a message that displays in a banner at the bottom of the page. You can customize the message according to user roles. Users must accept the message to remove the banner.

You must be an administrator to perform this procedure.

1. From the main menu, select **Settings > General Settings**.

2. In the **Consent Messages** section, click the **Add** button.

3. Configure the following settings:
   - **Title**—Enter a descriptive title for the message.
   - **Roles**—Use the list to select the types of users who will see the message.
   - **Message**—Enter the text of your message.
   - **Disable background**—Select this option to require the user to accept the message before using the interface.
   - **Show every session**—Select this option to show the message every time the user accesses VDX Analytics.
4. Click **Save**.

Configure Access to Saved Searches

Use this procedure to control who can see and use saved searches.

You must be an administrator to perform this procedure.

1. From the main menu, select **Settings > Authorization**.
2. In the **Saved Searches Visibility** section, select one of the following options:
   - **Admin only**—If you are using Vantage DX to provide managed services, you must select this option.
   - **Everyone**

Managing Licensing

Use the information in this section to complete the following tasks:

Task	Description
"View License Information" on page 93	View information about your license, such as the expiry date.

View License Information

Use this procedure to view information about your license, such as:

- The type of license you have.
- The number of integrations supported for that license.
- The number of integrations currently configured.
- The expiry date.

1. From the main menu, select **Settings**.
2. Click the **Licensing** tab.
3. Click on a license to view details.

Managing Storage

Use the information in this section to complete the following tasks:

Task	Description
"Configure Storage Options" on page 94	Configure the length of time that data is stored in VDX Analytics.
"View Storage" on page 94	See the amount of storage spaced used by each integration.

Configure Storage Options

Use this procedure to configure the length of time that data is stored in VDX Analytics. By default, Vantage DX Analytics retains data for 90 days; this value is the maximum.

1. From the main menu, select **Settings**.
2. Click the **Storage** tab.
3. Under **Storage Retention**, enter the number of days that you want to retain data.
4. Click **Save**.

View Storage

Use this procedure to see the amount of storage spaced used by each integration.

1. From the main menu, select **Settings**.
2. Click the **Storage** tab.
3. Review the list of integrations to see the amount of data stored for each one. The total storage used is shown at the bottom of the list.

Tell Us How We Did

How did we do? Did you find the content you needed? Your feedback will help us improve our documentation.

Click here to provide feedback.

MARTELLO