MARTELLO

VANTAGE DX

DEPLOYMENT GUIDE FOR ENTERPRISES

RELEASE 3.21
DOCUMENT DATE: MAY 12, 2025

NOTICE

Trademarks

Deployment Guide for Enterprises
Release 3.21 - May 12, 2025

Contents

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

CHAPTER 1

Introduction

Document Purpose and Intended Audience

This document provides information about how to deploy the Vantage DX solution and perform the initial setup tasks for your company. It describes how to deploy the modules in the Vantage DX solution; however, the modules that are available to you depend on your license package. This guide may contain information about functionality that is not available in your deployment.

After you have deployed Vantage DX, refer to "Related Documentation" on page 7 for information about how to use each of the Vantage DX modules to access and manage performance data.

This guide is intended for use by system administrators and IT managers.

Related Documentation

This guide provides information about the initial deployment of Vantage DX. For complete information about using the components of the Vantage DX solution, refer to the following documentation, available on the Martello website. You can download the documentation from:

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

Application Notes

- Understanding Vantage DX
- Monitor and Troubleshoot Microsoft Teams Call Quality
- Monitor a Hybrid Exchange Environment
- Monitor Co-Authoring Platforms
- Manage Alerts and Incidents
- Manage Complex Data in VDX Analytics
- Business Services and SLA Performance Data on VDX Analytics
- Customize Monitored Sites in Vantage DX Monitoring

Vantage DX Solution-Level Documentation

- Vantage DX Release Notes
- Vantage DX Product Overview
- Performance Data in Vantage DX

VDX Analytics

- VDX Analytics Integration Guide
- VDX Analytics User Guide

Vantage DX Monitoring

- Vantage DX Monitoring User Guide

Revision History

Document Date	Description
May 12, 2025	Vantage DX 3.21 Deployment Guide for Enterprises

CHAPTER 2

Understanding the Deployment Process

The following sections provide an overview of the initial deployment process. We recommend that you deploy Vantage DX in stages:

Integrate your Microsoft Data

The first step in the deployment process is to integrate yourMicrosoft Call Quality Dashboard (CQD) and your Microsoft 365 subscription with Vantage DX. After you configure these two integrations, Vantage DX retrieves call quality data from your Microsoft CQD, as well as status information about Microsoft 365 services.

After you configure these integrations, we recommend that you collect data for two weeks. This amount of data will help you analyze performance and identify trends. You can use this information to quickly identify problem areas, and to plan the most effective locations to deploy Vantage DX Monitoring robots.

For information about how to configure these integrations, see "Integrate Data from your Microsoft Tenant" on page 31.

Analyze Data and Identify Critical Locations

The next step in the process is to identify critical locations using the data in the dashboards.

We recommend that you identify two types of locations to deploy Vantage DX Monitoring robots:

- **Sites to monitor proactively**—Choose at least one business-critical site, such as your corporate headquarters, or sites where you have VIP users.

- **Sites or users who experience problems**—Select sites where you have known issues, or where you have identified problems based on your analysis of the data available in Vantage DX dashboards.

The 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 usage of meeting rooms and the health state of devices associated with meeting rooms.

Follow the steps outlined in "Data Analysis Process" on page 10 to identify problem areas in your environment.

Data Analysis Process

Use the following procedure to review and analyze the data that Vantage DX has collected from its integration with your Microsoft CQD.

Tip:
We recommend that you collect data for a period of two weeks when usage is typical. For example, we recommend that you do not base your analysis on a time period when there are holidays and call volumes may be lower than usual.

1. Select **Analyze > Teams Overview Dashboard**.
2. Use the time filter field to set the time period to use for your analysis. Choose one of the following options:
   - If you are analyzing the last 14 days, click the clock icon and set the **Quick Select** to the last 14 days; click **Apply**.
   - If you are analyzing data collected in a previous period, click **Show Dates** and click **~ a day ago**. Select the **Absolute** tab and select a start date. Click the **now** field and select the **Absolute** tab; select an end date. Click **Update**.
3. Review the data on the Teams Overview Dashboard:
   - By default, the Teams Overview Dashboard displays data for remote users as well as users who are located in an office. If you want to focus your analysis on one type of user, click in the Work Location widget to filter the data.

- The Calls by Location map indicates where poor or failed calls occurred. A heat map around the pin indicates locations that had a higher volume of poor or failed calls. Poor calls and failed calls display by default, but you can use the Layers menu to show or hide data if you want to focus on a specific health state, such as failed calls.
- The Top Affected Users table lists the users who were most affected by poor call quality, up to a maximum of 50. If you wish, you can click the Export icon to download this data as a raw or formatted (CSV) file.
- The Top Affected Locations table lists the locations that were most affected by poor call quality, up to a maximum of 50. If you wish, you can click the Export icon to download this data as a raw or formatted (CSV) file.

4. View detailed data:
    - To view information about a specific user, go to the Top Affected Users table and hover over the user name. Click the **Plus** (+) icon and select **Go to Users Dashboard**. The Users Dashboard contains detailed information about the most recent calls that the user participated in. If you filtered the data according to Work Location before you drilled down to this dashboard, the filter is automatically applied. If you did not filter data, you can choose to do so using the Work Location widget on this dashboard. We recommend that you use the data on the Users Dashboard to identify VIP users who work remotely, and who experience call quality issues.
    - To view information about a specific location, go to the Top Affected Locations table and hover over a location name. Click the **Plus** (+) icon and select **Go to Locations Dashboard**. The Locations Dashboard contains data about the reasons for poor calls at a location, as well as information about the ISP, the call volume, the call type and connection details. If you filtered the data according to Work Location before you drilled down to this dashboard, the filter is automatically applied. If you did not filter data, you can choose to do so using the Work Location widget on this dashboard. You can use this information to identify trends, such as whether the majority of poor calls occur on wireless or WiFi connections.

Deploy Robots

The number of Vantage DX Monitoring robots that you can deploy depends on your license package.

We recommend that you start by deploying up to 10 robots, distributed in the following way:

- **Sites or users experiencing call quality issues**—Deploy up to 8 robots at sites where you have known issues, or where you have identified problems based on your analysis of the dashboard data. These sites can be business locations or the computer of a remote user.
    - When you deploy robots at a business location, you can install the robot either on a machine that is connected to your LAN or that is connected

by WiFi; you can determine which type of connection is most important to monitor based on the dashboard data.

- Deploy a robot on the machine of a user who is affected by poor call quality. We recommend this approach for VIP users who work remotely.

- **Business-critical sites**—Deploy a minimum of 2 robots at each business-critical site. For each business-critical site, we recommend one robot on a machine connected to the LAN, and one robot on a machine that connects to the network through WiFi.
- **Sites to monitor proactively**—If you have not deployed all 10 robots based on this criteria, select other important business sites that you want to monitor proactively, or install robots on different floors at the same site.

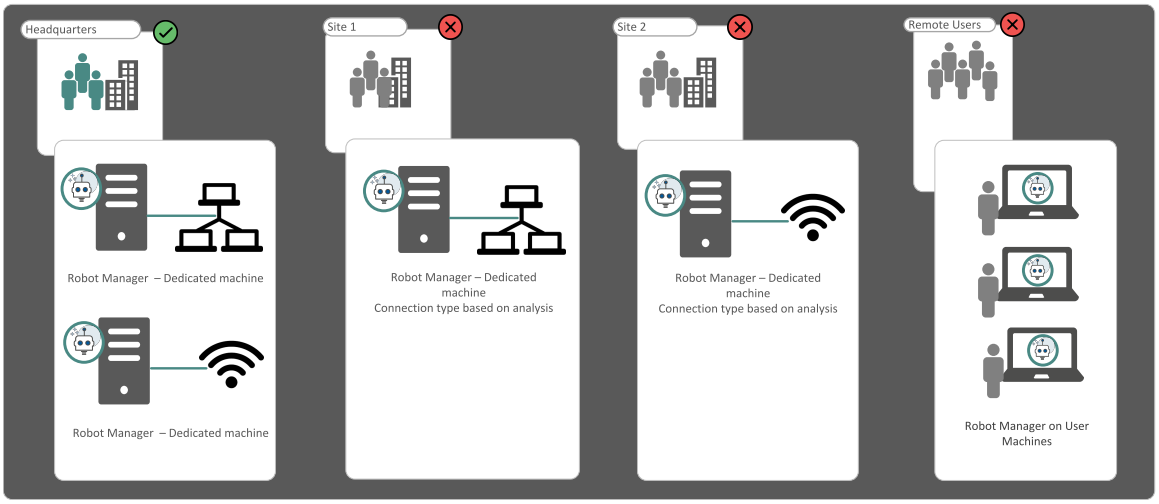
Tip:
When you deploy Vantage DX Monitoring robots at business sites, we recommend that you install the robots on machines that are located close to large numbers of users, and that are similar as possible to your users' machines. Plan to install each robot on a dedicated machine.

For information about how to deploy robots, see "Configure Synthetic Transactions" on page 42 and "Configure Network Diagnostics" on page 52.

Example

The following image shows an example of how you can deploy Vantage DX Monitoring robots to proactively monitor business-critical sites, sites with known issues, and VIP users who work remotely.

Figure 1: Example of a Vantage DX Deployment

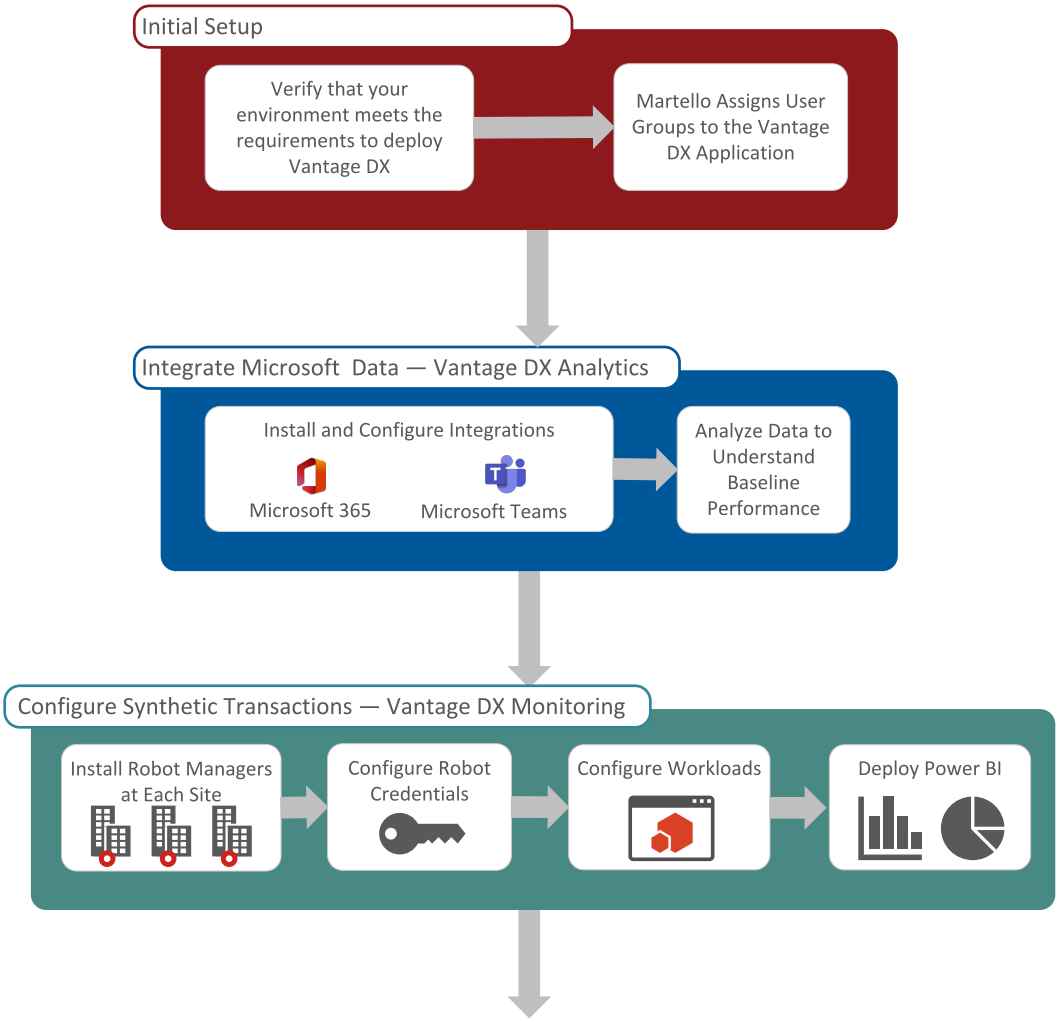


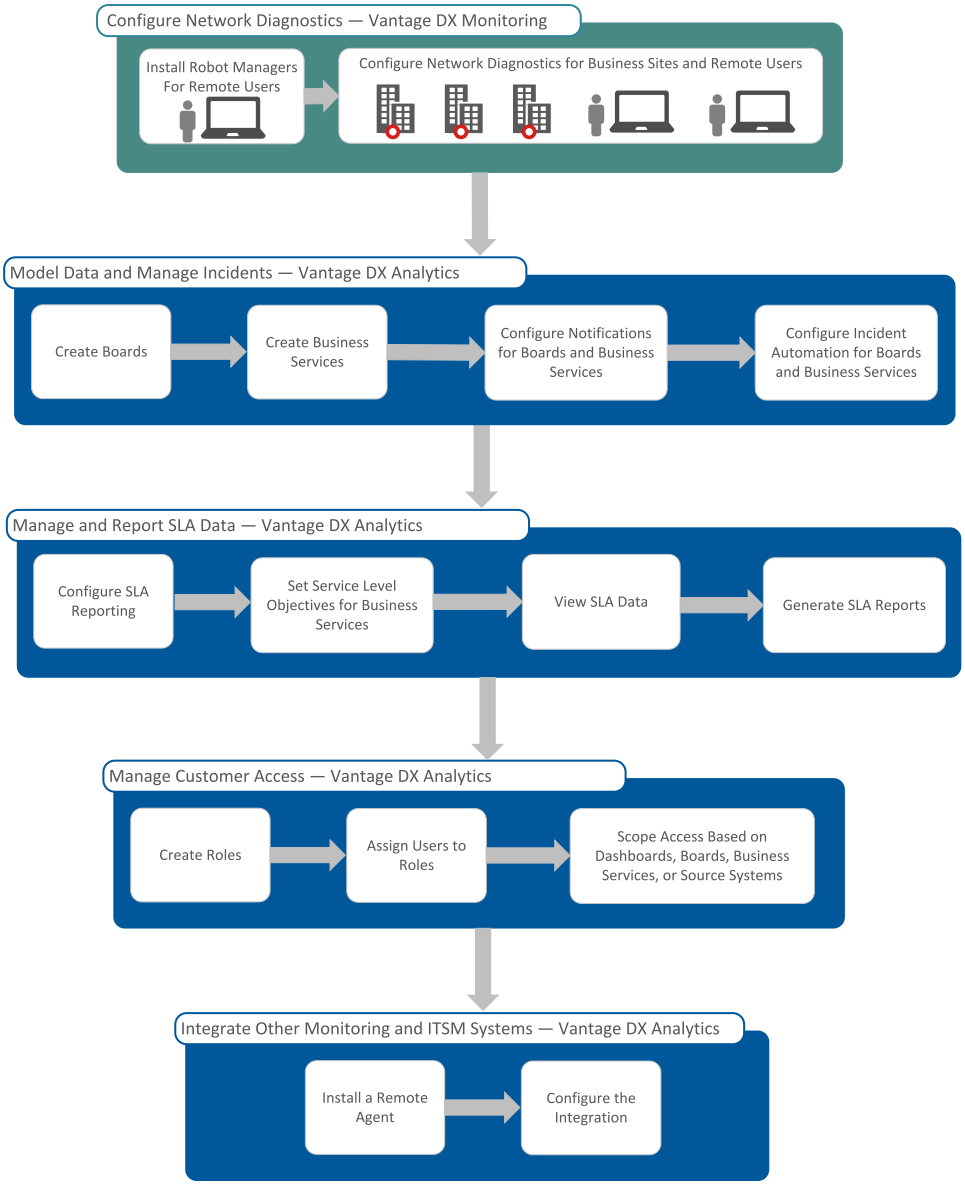
CHAPTER 3

Deployment Workflow

The following image provides an overview of the deployment tasks that you complete when you set up Vantage DX.

Figure 2: Deployment Workflow




Configure Network Diagnostics — Vantage DX Monitoring
Install Robot Managers For Remote Users
Configure Network Diagnostics for Business Sites and Remote Users
Model Data and Manage Incidents — Vantage DX Analytics
Create Boards
Create Business Services
Configure Notifications for Boards and Business Services
Configure Incident Automation for Boards and Business Services
Manage and Report SLA Data — Vantage DX Analytics
Configure SLA Reporting
Set Service Level Objectives for Business Services
View SLA Data
Generate SLA Reports
Manage Customer Access — Vantage DX Analytics
Create Roles
Assign Users to Roles
Scope Access Based on Dashboards, Boards, Business Services, or Source Systems
Integrate Other Monitoring and ITSM Systems — Vantage DX Analytics
Install a Remote Agent
Configure the Integration

CHAPTER 4

Requirements

The following sections list the information that you need to provide to Martello before you deploy the Vantage DX solution, as well as the requirements for each component.

Naming Conventions

Because you can use Vantage DX to manage multiple sites, it is essential that you establish a naming convention that you can apply to all of the configurations. Use the information in the following sections to establish the naming conventions that you will use in Vantage DX.

Microsoft CQD Integration

When you configure an integration, you must enter a name for the integration that will display in the VDX Analytics interface. For example:

TENANTNAME

Vantage DX Monitoring Robot Managers and Workloads

It is important to follow a naming convention when you configure Robot Managers and workloads in Vantage DX Monitoring. Using a standardized approach to naming will help you find components easily in VDX Analytics. For example, use naming conventions that help you identify the following:

- The city where the Robot Manager is deployed. For example, use a 3-letter indicator of the city name, or an airport code.

- The robot number, to differentiate between the robots deployed at the same location, such as R1 and R2.
- If you are deploying the Robot Manager on the machine of a remote user, we recommend that you enter the user's email address as the Robot Manager alias; this will allow you to correlate the network diagnostics with call quality data for the user.
- Optionally, you can identify the connection type, such as WIFI or Wired.
- If you are deploying robots in both a production environment and a development environment, indicate the type deployment environment. For example: PRD for a production environment. DEV for a development environment.

Examples: Robot Managers

For Robot Managers, we recommend that you use a naming convention such as the following:

PRD-CITY-R1

For example: `PRD-PARIS-R1`

For Robot Managers deployed on the machines of remote users, we recommend using the email alias of the user as the Robot Manager alias. For example:

`JSMITH@EXAMPLE.COM-R1`

Examples: Monitoring Configurations

For monitoring configurations, we recommend that you use a naming convention such as the following:

WORKLOAD or [SUBSIDIARY NAME] WORKLOAD

For example, `Teams` or `[ACME SUBSIDIARY] Internal Mail Routing`.

Permissions and Access

To integrate Vantage DX with your Microsoft tenant, ensure you meet the requirements listed in the following sections:

- "Permissions for the VDX Application" on page 16
- "Groups Required for SSO" on page 17

Permissions for the VDX Application

The Vantage DX application must be registered in Azure Active Directory and you must grant consent for the application to retrieve data from your Microsoft tenant.

The Vantage DX application requires tenant-wide admin consent in the Azure portal. Click the following URL and click **Accept** to grant consent when prompted:

https://login.microsoftonline.com/common/adminconsent?client_id=0d75f118-91b7-4a02-8c52-25d8a1590a7c

The following table lists the permissions that you give to the Vantage DX application when you grant consent.

Table 1: Permissions Required by the Vantage DX Application

API/Permission Name	Type	Description
GroupMember.Read.All	Application	Read all group memberships
Group.Read.All	Application	Read groups and their properties
Organization.Read.All	Application	Read organization information
OrgContact.Read.All	Application	Read organization contacts
Place.Read.All	Application	Read all company places
Reports.Read.All	Delegated	Read all usage reports
Reports.Read.All	Application	Read all usage reports
RoleManagement.Read.Directory	Delegated	Read directory RBAC settings
ServiceHealth.Read.All	Application	Read service health
TeamworkDevice.Read.All	Application	Read Teams devices
User.Read	Delegated	Sign in and read user profile (no admin consent required)
User.Read.All	Delegated	Read all users' full profiles
User.Read.All	Application	Read all users' full profiles

Groups Required for SSO

In Entra ID (formerly Azure AD), create the following groups and assign them to the Vantage DX Enterprise application:

- Service Administrators
- Service Operators

Ensure that you choose Security as the group type. If you have existing groups with these names, you do not need to create new ones. Provide the Object ID of each

group to Martello. For information about assigning groups to SaaS applications in Entra, see the following Microsoft documentation:

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-saasapps

Account Requirements

Use the following sections to understand the accounts that are required for an initial deployment of Vantage DX, and the accounts that are required for more advanced configurations:

- "Basic Accounts" on page 18
- "Advanced Accounts " on page 19

Basic Accounts

The following table lists the Microsoft 365 accounts that are required to get started with Vantage DX.

Module	Requirements
Vantage DX Analytics Integrations	

Module	Requirements

Microsoft Call Quality Dashboard (CQD)	Set up the Microsoft CQD and configure a Microsoft 365 account that VDX Analytics can use to access the CQD. Ensure that the account meets the following requirements:
	• The account is configured in Azure Active Directory (AD).
	• The account is cloud-native.
	• The authentication method meets one of the following conditions:
	  • Native Azure multi-factor authentication (MFA) used in a passive authentication flow.
	  • MFA is disabled if using another type of authentication.
	• The account is not federated.
	• At a minimum, the account must be assigned a Teams Communication Support Engineer role or a Global Reader role. The account must have permission to access end user identifiable information (EUII). Refer to the information on the following Microsoft website to see the roles that can access EUII:
	https://docs.microsoft.com/en-us/microsoftteams/turning-on-and-using-call-quality-dashboard#assign-roles-for-accessing-cqd
	We recommend that you do not use a Teams Administrator role for this purpose.

Vantage DX Monitoring	
Robot Manager	A minimum of two user accounts that are dedicated to monitoring; these accounts can be used by up to five robots. Ensure that the accounts meet the following requirements: • All accounts must have a valid Office 365 E3 or E5 license. • Multi-factor authentication is disabled. • Password expiry is not configured. These accounts are used to monitor the Teams Advanced workloads. For other workloads, see "Advanced Accounts " on page 19.

Advanced Accounts

The information in this section applies to accounts used by the Robot Manager service.

The number of accounts you need depends on the workload that you are monitoring and the number of robots that you deploy:

Workload	Account Information
Exchange Free/Busy	A user account with a provisioned mailbox and a set timezone. An attendee user account with a provisioned mailbox and set timezone. The first user should have the rights to check the free/busy status of the attendee. If the user accounts are in different organizations, the attendee's organization calendars must be accessible from the organizer's organization.
Exchange Online	Up to 30 robots can use one account. You need a user account with a provisioned mailbox and a set timezone.
Exchange Server	The user account that connects to the Exchange server must be a member of the "View-Only Organization Management" security group in the Active Directory.
Exchange MAPI	A user account with a provisioned mailbox and a set timezone.
Mail Routing	A user account with a provisioned mailbox and a set timezone.
Office 365 Web Apps	A user account with the intended Microsoft 365 application provisioned. • The account must be cloud-only (ADFS is not supported) • The account must be licensed for the intended Office 365 application
One Drive	A user account with OneDrive provisioned. Up to 30 robots can use one account.

Workload	Account Information
Teams Advanced	Teams Advanced requires two user accounts. These accounts can be used by up to five robots. If you are deploying more than five robots, you must create additional accounts. The accounts must meet the following requirements: • The accounts must be licensed for Teams. • The accounts must belong to same tenant. • A private team is automatically created at the first scan of a robot. The user accounts must be set as the Teams admins.  **Tip:** If you are monitoring Teams Advanced from multiple regions—for example, if you are using Microsoft 365 Multi-Geo— use separate credentials for the robots at each location.
Teams Phone	This workload requires a Teams user account with a Teams Phone license at each location. The accounts you create must be dedicated to Teams Phone. Teams allows a user to participate in one call at a time; therefore, you cannot use these same credentials to test other workloads. In addition to these accounts, this workload requires an external phone number that is set to auto-answer or Interactive Voice Response (IVR) service. Ensure that the external phone number is not assigned to a Teams user; if it is assigned to a Teams users, Teams will automatically convert the call to cloud call and will not use Teams Phone. The accounts cannot use MFA for this workload.
Teams Video	You need two accounts per robot. • The accounts must be cloud only; ADFS is not supported. • The accounts must be licensed for Teams. • The accounts must belong to the same tenant. • The accounts must have provisioned calendars.

Network Connections

Use the following sections to understand the network connections that are required for an initial deployment of Vantage DX, and the connections that are required for more advanced configurations:

- "Basic Connections" on page 22
- "Advanced Connections" on page 24

Basic Connections

The following table lists the connectivity requirements for the machine where the Vantage DX Monitoring Robot Manager service is installed.

Protocol and Port	Endpoint / Destination	Description
HTTPS		
443	<instancename>.vantage-dx.com	Robot connection to Vantage DX
	https://extreme-ip-lookup.com/	Robot connection used for network diagnostics
ICMP		
Type 0	Inbound packets	Destination host unreachable; needed only if you are configuring network diagnostics with ICMP
Type 3	Inbound packets	TTL exceeded
Type 11	Inbound packets	Echo request
Type 8	Outbound packets	Echo reply; needed only if you are configuring network diagnostics with ICMP
TCP		

Protocol and Port	Endpoint / Destination	Description
443 (AMPQS 5671 for installations prior to June 2023)	One of the following: • **Western European region:** eager-swan.rmq.cloudamqp.com • **Eastern United States region:** sharp-fuchsia-mongoose.rmq4.cloudamqp.com	Robot connection to Vantage DX
443	All required Microsoft Office 365 URLs and IP addresses. For more information, see the following website: https://docs.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide	Robot connection to Microsoft workloads
443	ecs.communication.azure.com	Robot connection to the Azure Communication Services (ACS) endpoint.
443	acsresource<your-tenant-name>.canada.communication.azure.com	Robot connection to the Azure Communication Services (ACS) endpoint.
443	20.202.0.0/16	Robot connection to a range of ACS public IP addresses. For more information, see the following website: https://learn.microsoft.com/en-us/azure/communication-services/concepts/voice-video-calling/network-requirements#firewall-configuration
UDP		

Protocol and Port	Endpoint / Destination	Description
3478 to 3481	20.202.0.0/16	Robot connection to a range of ACS public IP addresses. For more information, see the following website: https://learn.microsoft.com/en-us/azure/communication-services/concepts/voice-video-calling/network-requirements#firewall-configuration
53	Custom endpoints for network diagnostics.	Robot connection when you configure network diagnostics using UDP Direct Mode. When you use UDP, ensure that your firewall also permits the inbound ICMP packets listed above.
3478	Teams endpoint for network diagnostics.	Robot connection when you configure network diagnostics to the Teams endpoint. When you use UDP, ensure that your firewall also permits the inbound ICMP packets listed above.

Advanced Connections

This section lists endpoints that may require adjustments to your firewall permissions.

Dashboard Data

To display data retrieved from the Microsoft CQD in Vantage DX dashboards, your firewall must permit the following connections on port 443:

- *.elastic-cloud.com:*
- https://*.tile.openstreetmap.org

- https://*.pendo.io
- wss://*.pendo.io

Remote Agent

VDX Analytics has an optional remote agent. A remote agent is needed when it is not possible to connect to the source system from the Vantage DX web server due to network boundaries. For example, you may need a remote agent because of firewall restrictions. You also need to use a remote agent if you are integrating other monitoring systems or ITSM systems with Vantage DX. If you are using a remote agent, the machine where you install the remote agent must be able to access the following URLs:

- The CQD database endpoint: cqd.teams.microsoft.com
- Microsoft Graph Endpoint: graph.microsoft.com
- Extreme-ip GeoIP lookup endpoint: https://extreme-ip-lookup.com/
- Your Vantage DX instance: https://<instancename>.vantage-dx.com/iq

Vantage DX Monitoring Robot Managers

The machines where you install Vantage DX Monitoring Robot Managers must be able to access the following URLs on port 80:

- Online Certificate Status Protocol (OCSP): http://ocsp.digicert.com
- Certificate Authority:
  - http://r3.i.lencr.org/
  - http://r3.o.lencr.org

Machine Requirements

Use the following sections to understand the machine requirements when you deploy Vantage DX Monitoring robots and Vantage DX Analytics remote agents.

- "Specifications" on page 25
- "Certificates" on page 27

Specifications

You can deploy a Vantage DX Monitoring Robot Manager at your business sites to monitor Microsoft workloads and to perform network diagnostics. If you are also using a VDX Analytics remote agent, you can deploy it on the same machine. It is optional to deploy a remote agent; install it only if you need to overcome network boundaries. For example, if you want to configure an integration between VDX Analytics and a monitoring system that is installed on-premises, you can use the remote agent to communicate with VDX Analytics in the cloud without any open inbound ports.

Ensure that the machine where you install these components meets the specifications listed in "Machine Requirements for Business Sites" on page 26.

If you are deploying a Vantage DX Monitoring Robot Manager on the machine of a remote user for the purposes of network diagnostics, ensure the user's machine meets the specifications listed in "Machine Requirements for Remote Users" on page 27.

Table 2: Machine Requirements for Business Sites

Component	Minimum	Recommended
Operating system	Windows 10 (64-bit) or Windows Server 2012 R2	Windows 10 22H2 and later, Windows 11 22H2 and later, or Windows Server 2016 (version 1607) and later
Processor	2.5 Ghz Quad-Core or 4 vCPUs	2.5 Ghz or faster or 4 or more vCPUs
Memory	8 GB	8 GB or higher
Available Disk Space (Program Files)	8 GB	16 GB or greater
.NET Framework	4.7.2	4.7.2 or higher
Dedicated machine required?	**Yes**	**No**
Vantage DX Monitoring Robot Manager service ***A VDX Analytics remote agent can be installed on the same machine; otherwise, the machine must be dedicated to Vantage DX.	✓	
VDX Analytics remote agent		✓
Power settings	Always on	Always on
Browser	Google Chrome	The current version is recommended; two previous versions are supported.

Table 3: Machine Requirements for Remote Users

Component	Minimum	Recommended
Operating system	Windows 10 (64-bit)	Windows 10 22H2 and later or Windows 11 22H2 and later
Processor	2.5 Ghz Quad-Core or 4 vCPUs	2.5 Ghz or faster or 4 or more vCPUs
Memory	8 GB	8 GB or higher
Available Disk Space (Program Files)	8 GB	16 GB or greater
.NET Framework	4.7.2	4.7.2 or higher
Browser	Google Chrome	The current version is recommended; two previous versions are supported.

Certificates

The information in this section applies to the machine where the Robot Manager is installed.

The machine where the Robot Manager is installed must have a certificate under the Computer Local Certificates. During the Robot Manager installation, a self-signed certificate is automatically installed in the “Personal” certificate store. This certificate is used to encrypt communication between Vantage DX Monitoring and the Robot Manager using the certificate's Private/Public keys.

Note: We recommend that you use the default installation procedure. This ensures that each Robot Manager has a different certificate, which enhances security.

Supported Browsers

You can access the Vantage DX modules using any of the following browsers on a Windows or MacOS device:

- Chrome
- Firefox
- Microsoft Edge

Note: Access from mobile browsers is not supported.

CHAPTER 5

Initial Setup

This section describes the initial tasks that you need to complete when you deploy Vantage DX. It explains how to set up administrators and operators for your organization, as well as how to configure basic the system integrations that you will need.

Vantage DX uses Entra ID (formerly Azure Active Directory) to authenticate users so that they can log in using their Microsoft credentials. When you use Vantage DX to provide managed services, you can configure single sign-on (SSO) for your own organization, and your customers can also use SSO to access the VDX Analytics interface.

Use the following table to complete the setup tasks.

Task	Description
"Configure Users" on page 29	Add administrators, operators, and read-only users for your Vantage DX instance.
"Access Vantage DX" on page 29	Access the Vantage DX management interfaces.
"Install an Integration for Email Notifications" on page 1	Enable an email system that you can use for notifications.
"Install an Integration for Teams Notifications" on page 1	Configure an integration that allows you to send Vantage DX notifications to a Teams channel.

Note: After you have completed the deployment tasks, you can configure role-based access to integrations, boards, and business services. For more information, see "Manage User Access" on page 92.

Configure Users

Vantage DX uses Azure Active Directory to authenticate users so that they can log in using their Microsoft credentials.

Before you can use Azure AD for authentication, you must register the Vantage DX application in the Azure AD admin center and provide consent for it to access user information. You must also create user groups in Azure AD and assign them to the application. Follow the procedure below to complete these tasks. For more information about assigning user groups to an application Azure AD, see the following Microsoft documentation:

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-saasapps

1. Create the following groups in Azure AD and record the Object ID for each one. Ensure that you choose Security as the group type.
    - **Service Administrators**—Users assigned to this group have read-write access to everything in Vantage DX.
    - **Service Operators**—Users assigned to this group have:
        - Administrative permissions in Vantage DX Monitoring.
        - Read-write access to any integrations, boards, and business services that the administrator provisions for this role in VDX Analytics.
2. Sign into the URL listed below using an administrator account for the tenant. When you are prompted to grant permissions, click **Accept**. https://login.microsoftonline.com/common/adminconsent?client_id=0d75f118-91b7-4a02-8c52-25d8a1590a7c
3. In Azure AD, select **Enterprise Applications** and click on **Vantage DX**.
4. Select **Users and groups**, and then click **+Add user/group**.
5. In the **Add Assignment** pane, select **Users and groups** to open the Users and groups list.
6. Search for the groups that you created and click **Select** for each of them, then click **Assign**.
7. Provide the Object ID of each group to your Martello Delivery Engineer, who will complete the setup of this feature.

Access Vantage DX

When you log into Vantage DX, the VDX Analytics interface opens as the default management tool. You can navigate to Vantage DX Monitoring from within VDX Analytics, or you can go directly to the interface using its specific URL. Use the following procedure to access the Vantage DX management interfaces.

To access Vantage DX Modules from within VDX Analytics

1. Go to the Vantage DX portal: `https://<your_instance>.vantage-dx.com/`

2. Click **Continue with Microsoft** to log in.
   VDX Analytics launches.
3. View a component that is retrieved from Vantage DX Monitoring and click the **Go To Source**  button to navigate to the UI for that Vantage DX module.

To Access a Module Directly

Append the appropriate suffix to your Vantage DX instance:

- **VDX Analytics**—Append /iq to your Vantage DX instance URL. For example, `https://<your_instance>.vantage-dx.com/iq`.
- **Vantage DX Monitoring**—Append /gizmo to your Vantage DX instance URL. For example, `https://<your_instance>.vantage-dx.com/gizmo`

CHAPTER 6

Integrate Data from your Microsoft Tenant

Use the information in this section to begin monitoring the call quality that your Teams users are experiencing, as well as the health state of your Microsoft services. Complete the setup tasks listed in the following table.

Task	Description
"Install the Microsoft CQD Integration" on page 31	Configure the integration between the Microsoft CQD and VDX Analytics. This integration allows you monitor call quality data about your users in near-real time.
"Install the Microsoft 365 Integration" on page 37	Configure the integration between your Microsoft 365 subscription and VDX Analytics. This integration allows you to monitor the health state of your Microsoft services, including the status of licenses.
"Configure Meeting Room Data" on page 39	Optional. If you have meeting rooms and devices configured in the Microsoft Teams admin portal, we recommend that you create a rule in VDX Analytics that consolidates the meeting room data from Microsoft 365 with the usage data from the Microsoft Teams CQD.

Install the Microsoft CQD Integration

Use this procedure to integrate the Microsoft Call Quality Dashboard (CQD) with VDX Analytics.

Before you Begin

Log into the Microsoft Call Quality dashboard through the Office 365 portal and verify that the CQD is activated and accessible.

1. From the main menu, select **Settings > Customer Management**.
2. Click on the customer name to open the profile.
3. Click the **Add** (**+**) button at the bottom of the page.
4. Select **Microsoft Teams Call Quality Dashboard** from the dialog box.
5. Enter the information required for the monitoring system.
6. Click **Save**.

Configure the following properties when you integrate the Microsoft Teams CQD with VDX Analytics to monitor remote users:

Property	Description
Set-up	
Integration Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Credentials	
Azure Login Name	The Microsoft 365 account that VDX Analytics can use to access the CQD.
Azure Login Password	The password for the Microsoft 365 account.
MFA Shared Secret (Optional)	The optional shared secret is used for multi-factor authentication for Azure Active Directory. To use this option, the account that VDX Analytics uses to connect to your Microsoft CQD must use Azure MFA with a passive authentication flow. In addition, the account must be cloud-native. To generate the password for this field, see the following Knowledge Base article: https://helpcenter.martellotech.com/s/article/000001082
Leverage Martello VDX Enterprise App	This option is enabled by default. We recommend that you do not change the setting. It allows the integration to use the permissions that you granted to the Martello VDX App when you first registered it.
Data Processing	

Property	Description
Tenant Size	Select the tenant size based on the number of users, or select Custom to provide an alternate value. The selected tenant size sets the defaults for the rest of the data processing values.
Data Retrieval Period	The number of days of data from the CQD to display in VDX Analytics. This value changes based on the size of the selected tenant. If you selected a custom tenant size, you must provide a value.
Max Data Query Time (minutes)	The maximum time in minutes allowed for a single CQD query. This value changes based on the size of the selected tenant. If you selected a custom tenant size, you must provide a value.
Data Window Incremental (minutes)	Vantage DX queries the CQD and loads call information into its database at 15-minute intervals, or at the value set in the Operation Interval field. The Data Window Incremental setting determines the length of time, in minutes, that VDX looks back when it queries the CQD. This lookback period a sliding window, based on the time that VDX last loaded call information into the database. In the CQD, call data is typically available 30 minutes after the end of the call. For conference calls, data about all attendees becomes available after the last attendee disconnects from the call. For example, if VDX queries the CQD and collects call information at 11am, then the next query will use 11am as its starting point and will look back from that time. The default value is 120 minutes, so in this example, VDX would look back to 9am. VDX retrieves any available information about calls that ended within that window. The default value for the Data Window Incremental setting is 120 minutes. If you select a custom tenant size, we recommend that you set 120 minutes as the value in this field.
Use Incremental Sync Start	When enabled, this option retrieves data beginning from the day of the integration, as opposed to VDX Analytics also retrieving historical data. This default value for this option changes, depending on the selected tenant size. If you selected a custom tenant size, you can enable or disable this option.

Property	Description
Split Properties over Multiple Queries	This option is disabled by default and cannot be enabled unless you selected a custom tenant size. Enable this option only if you are advised to do so by a Martello support engineer.
Add Good Calls as Information Events	Select this option if you want each call to display as a separate component in VDX Analytics. This option is disabled by default and cannot be enabled unless you selected a custom tenant size. **Warning:** This option significantly increases the amount of data that VDX Analytics retrieves and stores. If you select this option, it may impact the performance of VDX Analytics.
Discovery Interval (minutes)	The interval for collecting components and relationships from the integrated system. This value changes based on the size of the selected tenant. If you selected a custom tenant size, you must provide a value.
Operation Interval (minutes)	The interval for collecting alerts, incidents, and component health states. This value changes based on the size of the selected tenant. If you selected a custom tenant size, you must provide a value.
Thresholds	
Poor Call Warning Ratio (%)	The threshold used by VDX Analytics to trigger a warning about the health status of a user device. Use this field to specify the percentage of poor calls that must occur during the time period used to calculate health status. The time period is set in the Hours to Look Back for Health Status field. By default, the call warning ratio is 20%.
Poor Call Critical Ratio (%)	The threshold used by VDX Analytics to trigger a critical alert about the health status of a user device. Use this field to specify the percentage of poor calls that must occur during the time period used to calculate health status. The time period is set in the Hours to Look Back for Health Status field. By default, the call critical ratio is 30%.

Property	Description
Jitter (ms)	Set the jitter threshold to use. 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. Jitter is averaged over 15-second intervals for the duration of the call. Microsoft classifies call quality as poor when the average exceeds 30 ms. By default, VDX Analytics raises an alert when jitter exceeds the 30 ms threshold, but you can use this field to change the threshold that triggers an alert.
Round Trip Time (ms)	Set the round trip time (RTT) threshold to use. RTT is the time in milliseconds that it takes a data packet to travel from point A to B and return. It is determined by the physical distance between the two points, the speed of transmission, and the overhead taken by the routers in between. RTT is averaged over 15-second intervals for the duration of the call. A value over 500 ms can cause poor call quality. By default, VDX Analytics raises an alert when RTT exceeds the 500 ms threshold, but you can use this field to change the threshold that triggers an alert.
Packet Loss (%)	Set the packet loss threshold to use. The number of packets lost in a 15-second interval. Packet loss is calculated as a percentage. For example, if 1000 packets are sent in a 15-second interval and 50 are lost, the packet loss rate is 5%. By default, VDX Analytics raises an alert when packet loss exceeds the 10% threshold, but you can use this field to change the threshold that triggers an alert.
Localization	
Timezone	Data collected by the Microsoft CQD is stored in UTC. You can use this setting to have VDX Analytics convert from UTC to another time zone.

Property	Description
Localize Call Times	Select this option to show calls in the local timezone of the participant. When you select this option, the local time is shown for each endpoint in the call. VDX Analytics uses the geolocation to determine the local timezone. If geolocation information is not available, the timezone defaults to UTC.
Building Data	Optional. Enable this option if you have uploaded building data to your Microsoft CQD and want to view it in Vantage DX. When you enable this option, Vantage DX displays the building name, country, region and city information retrieved from the building data file. Because the Microsoft CQD correlates VPN and local IP range information from the building data with call data, this information is also integrated with the call quality data displayed in Vantage DX. This option is designed as an alternative to using the Dynamic Office feature in Vantage DX. If you choose to use CQD building data instead of dynamic offices, information that Vantage DX retrieved about dynamic offices prior to the change will continue to display for up to 90 days.
Privacy Protection	
Anonymize Data	Select this check box if you do not want to show identifiable information for your users, such as names, email addresses, and IP addresses. User information displays as number strings.
Disable Caller Resolution	Select this check box if you do not want to show identifiable information about call recipients. When you choose this option, VDX Analytics displays the name of the user who placed a call, but does not show the name of the call recipient
External Users	
Track External Users	Select this check box to include external users in the number of attendees who participated in Teams meetings. Vantage DX Analytics displays objects for external users and devices and provides a link to the meeting in which they participated.
Track External Users in Location Groups	Select this check box if you want to include external users in the groups that Vantage DX Analytics creates for cities and countries.

Property	Description
Options	
Health Status Period (hours)	The number of hours used to calculate the health status of objects. By default, this field is set to 48 hours; however, you can edit this value if you want to calculate the health status over a different period of time.
Disable Dashboard Data Retrieval	Select this check box if you do not want VDX Analytics to retrieve and store data for the dashboarding feature. If you select this option, ensure that you also disable the dashboarding feature using the options on the **Settings > General Settings** page.

Install the Microsoft 365 Integration

Use this procedure to integrate your Microsoft 365 subscription with VDX Analytics.

Before you Begin

The Vantage DX Analytics application must be registered in Azure Active Directory and you must grant consent for the application to retrieve data. If you have configured SSO, the application is already registered and has the necessary permissions. If you have not performed this step, click the following link to automatically register the application, and then follow the prompts on the screen to sign in and grant consent:

https://login.microsoftonline.com/common/adminconsent?client_id=0d75f118-91b7-4a02-8c52-25d8a1590a7c

For a list of permissions that you are granting to the application, see "Permissions for the VDX Application" on page 16.

1. From the main menu, select **Settings > Customer Management**.
2. Click on the customer name to open the profile.
3. Click the **Add** button at the bottom of the page.
4. Select **Microsoft 365** from the dialog box.
5. Enter the information required for the monitoring system.
6. Click **Save**.

Configure the following properties when you integrate Microsoft 365 with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.

Property	Description
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Leverage Martello VDX Enterprise App	Select this checkbox if you have used the automated option to register the application in Azure AD. When you select this option, you need to provide your Tenant ID only; you do not need to enter a Client ID or a Client Secret Key.
Tenant ID	Required. For information about how to find your Microsoft tenant GUID, see https://docs.microsoft.com/en-us/onedrive/find-your-office-365-tenant-id.
Client ID	The Application (Client) ID from the above Azure Application registration. This information is required only if you are registering the application and granting consent manually.
Client Secret Key	The Client Secret associated with the Azure Application registration. The Client Secret can have an expiry date configured; if your Client Secret has an expiry date, you will need to regenerate it and update the integration when it expires. This information is required only if you are registering the application and granting consent manually.
Collect Teams Devices	Optional. Select this checkbox to collect information about the following Teams meeting room devices: • Teams Room devices • Surface Hub devices • Teams Panel devices • Collaboration Bar devices • Teams Display devices • Touch Console devices

Property	Description
Collect IP Phones	Optional. Select this checkbox to collect information about the following Teams meeting room IP Phone devices: • IP Phone devices • Low-Cost Phone devices • SIP devices
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

Note:
If you prefer to register the application and grant consent manually, refer to the following Knowledge Base article:

https://helpcenter.martellotech.com/s/article/Microsoft-365-Integration-VDX-A-Requirements

If you follow the manual process, ensure that you grant the permissions listed in "Permissions for the VDX Application" on page 16.

Configure Meeting Room Data

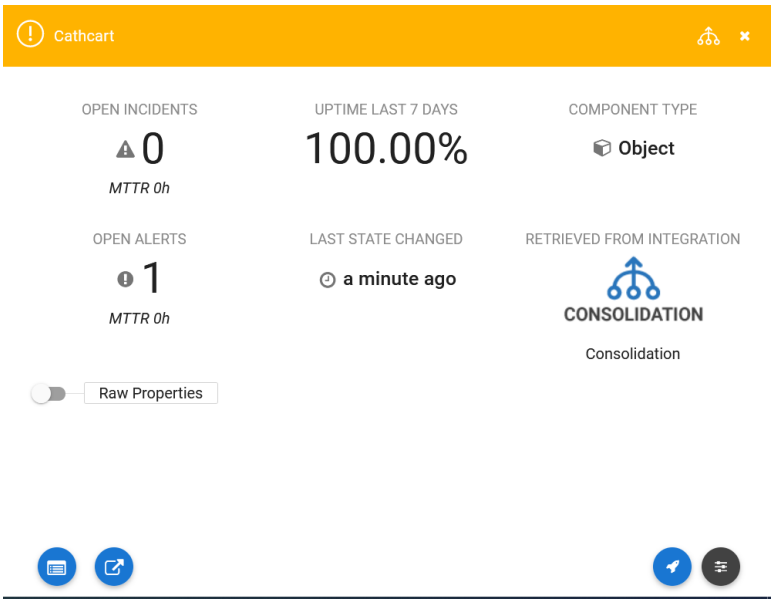
As part of the integration with Microsoft 365, VDX Analytics retrieves data about the meeting room devices that are configured in the Microsoft Teams admin portal, including:

- General information, such as the model number, serial number, and MAC address.
- Health state.
- Peripherals associated with the meeting room device, and their status.

VDX Analytics also retrieves data related to meeting rooms from the integration with the Microsoft Teams Call Quality Dashboard (CQD). If you have meeting rooms and devices configured in the Microsoft Teams admin portal, we recommend that you create a rule in VDX Analytics that consolidates the meeting room data from Microsoft 365 with the meeting room and usage data from the Microsoft Teams CQD. Doing so allows you to view and manage one component that contains all of the data that is available for that meeting room. For example, you can use the consolidated component to see the properties of the meeting room and its devices,

as well as information such as the location, the ISP, number of calls, and information about the call types.

When you create a consolidation rule, VDX Analytics creates a component; the component name is based on the name of the account that is used to log into the meeting room device. The interface lists Consolidation as the source system for the new component because it is created by VDX Analytics rather than retrieved directly from another system. The following image shows an example of a meeting room component that was created using a consolidation rule. In this example, "Cathcart" is the name of the account used to log into the meeting room device, which is also the name of the meeting room.



Use the following procedure to configure a rule that consolidates the meeting room data from Microsoft 365 with the meeting room data from the Microsoft Teams CQD. You must be an administrator to perform these steps.

1. From the VDX Analytics main menu, select **Settings** and click the **Consolidation Rules** tab.
2. Click the expansion icon next to **Object**.
   This setting determines the type of component that VDX Analytics creates.
3. Click **Add Rule**.
4. Enter the following information:
   - **Rule Name**—Enter a name for the rule, such as Teams Meeting Rooms.
   - **Description**—Enter a description of the rule.
5. Choose one of the following options and enter the information shown in the **Field Mapping** section:

Option 1: Create a rule that consolidates a meeting room and its devices—as well as non-meeting room devices such as IP phones and SIP devices—into one component. To use this option, ensure that you have selected the "Collect IP Phones" option in the Microsoft 365 integration settings.

Row	Field	Description
1	Integration Type	Microsoft Teams Call Quality
	Field Name	source.Office365CQD.Id
	Match Type	Exact Match
2	Integration Type	Microsoft 365
	Field Name	source.Office365.Id
	Match Type	Exact Match
3	Integration Type	Microsoft 365
	Field Name	source.Office365.currentUser.id
	Match Type	Exact Match

Option 2: Create a rule that consolidates data about meeting rooms only, and does not include non-meeting room devices.

Row	Field	Description
1	Integration Type	Microsoft Teams Call Quality
	Field Name	source.Office365CQD.Id
	Match Type	Exact Match
2	Integration Type	Microsoft 365
	Field Name	source.Office365.Id
	Match Type	Exact Match

6. Click **Save**.
7. Click the **Action** button and then click the **Start Consolidation** icon.
8. Click **Ok**.

CHAPTER 7

Configure Synthetic Transactions

Use the information in this section to install Vantage DX Monitoring Robot Managers at key business locations and begin monitoring Microsoft workloads. Complete the setup tasks listed in the following table.

Task	Description
"Understanding Synthetic Transactions" on page 43	Review this information to understand the how Vantage DX Monitoring works.
"Install Robot Manager" on page 45	The Robot Manager is a Windows service. Install it on every machine where you plan to deploy robots.
"Edit Monitoring Credentials" on page 46	Edit the initial credentials that robots use to access workloads.
"Add Monitoring Credentials" on page 46	Configure additional credentials that robots can use to access workloads.
"Create Monitoring Configurations" on page 47	For each workload that you want to monitor, create a configuration that specifies the parameters for the environment. Parameters include information such as credentials, addresses, port numbers, and other information specific to your network.
"Assign Configurations to Robot Managers" on page 47	Specify the applications that you want the robots to monitor at each site.
"Add Location Tags to Robot Managers" on page 48	Configure location tags to display robots on a map in Power BI.
"Import the Power BI Template for Cloud Deployments" on page 49	Import the template if you want to be able to view performance metrics in Power BI.

Task	Description
"Remove a Robot Manager" on page 51	After you have uninstalled a Robot Manager, remove it from the interface.

Understanding Synthetic Transactions

Robot Manager is a Windows service that you install on machines located at critical business sites. It manages the robots that perform synthetic transactions at that site. The Robot Manager service sends the results of the synthetic transactions to the Vantage DX Monitoring server using encrypted communication.

Robots perform synthetic transactions, which are tests that simulate the activities that your users typically do. The robots perform these tests at the sites where your users are located, to provide you with insight into the user experience at each site. You can use the Vantage DX Monitoring Web UI to configure the activities and workloads that the robots test.

Robots require credentials to log into your applications and perform tests. For example, a robot that monitors Office 365 workloads requires credentials for an Office 365 user account.

Vantage DX Monitoring provides placeholders for these credentials. These placeholders are assigned to workloads by default; when you edit them, the workloads are automatically updated to use the correct credentials. The following table lists the placeholders and the workloads that they are assigned to.

Table 4: User Credentials for Robots

Credential	Placeholder	Workload
Office 365 User	myusername@example.com	AAD Connect ADFS Exchange Free/Busy Exchange MAPI Exchange Online Exchange OWA Hybrid Mail Routing Internal Mail Routing Office 365 Health Office 3665 WebApp OneDrive Roundtrip Mail Routing Sharepoint Page SMTP Gateway Teams Teams Advanced

Credential	Placeholder	Workload
Exchange Mailbox Server Credential	domain\username	Exchange DAG Exchange Mailbox Server
On-Premises User	myusername@example.com	Exchange Free/Busy Hybrid Mail Routing
Exchange Edge Server Credential	domain\username	Exchange Edge Server
Office 365 Echo User	myusername@example.com	Teams Advanced

Note:
Synthetic transactions are designed for use at your business sites only; do not deploy them on the machines of remote users.

Install Robot Manager

Use this procedure to install the Robot Manager service.

Perform this procedure on each machine where you plan to deploy robots.

1. In a browser, go to `https://<instance-name>/gizmo/downloads/Gsx.RobotManager.zip` where `<instance-name>` is the name of your Vantage DX deployment.
2. Extract the following files:
   - `Gsx.RobotManager.msi`—This file is used by the script.
   - `Install-GsxRobotManager.ps1`—This file is the script to run.
   - `Transform.mst`—This file is used by the script.

   No specific location is required.
3. Open PowerShell as Administrator.
4. Enter the cmdlet `Set-ExecutionPolicy RemoteSigned`
5. Choose **[A] Yes to All**.
6. To run the `Install-GsxRobotManager.ps1` script, navigate to the script location path in PowerShell and run the following command:
   `.\Install-GsxRobotManager.ps1`

7. Choose **[R] Run once** after the Security Warning.
8. In the Web UI, refresh the Robots management page and verify that all Robot Managers display the correct version.
   To access the interface, append `/gizmo` to your Vantage DX instance URL. For example, `https://<your_instance>.vantage-dx.com/gizmo`

Edit Monitoring Credentials

Use this procedure to edit credentials that robots use to access workloads.

Perform this procedure in the Vantage DX Monitoring Web UI. To access the interface, append `/gizmo` to your Vantage DX instance URL. For example, `https://<your_instance>.vantage-dx.com/gizmo`

1. Select **Settings > Credentials** from the navigation panel.
2. On the credential that you want to edit, click ⋮ and select **Edit**.
3. Edit any of the following information as needed, and then click **Save**.
   - **Alias**—Type a brief name or description for the monitoring credential.
   - **Username**—Type the username that the robot will use.
   - **Password**—Type the password associated with the account.
   - **Confirm Password**—Type the password again for confirmation.

Add Monitoring Credentials

Use this procedure to add credentials that robots can use to access workloads.

Perform this procedure in the Vantage DX Monitoring Web UI. To access the interface, append `/gizmo` to your Vantage DX instance URL. For example, `https://<your_instance>.vantage-dx.com/gizmo`

1. Select **Settings > Credentials** from the navigation panel.
2. Enter the following information, and then click **Add**.
   - **Alias**—Type a brief name or description for the monitoring credential.
   - **Username**—Type the username that the robot will use.
   - **Password**—Type the password associated with the account.
   - **Confirm Password**—Type the password again for confirmation.

Next Steps

- "Create Monitoring Configurations" on page 47

Create Monitoring Configurations

For each workload that you want to monitor, you need to create a configuration that specifies the parameters for your environment. For example, depending on the workload that you want to monitor, you may need information such as credentials, addresses, port numbers, or other information specific to your network. After you create a configuration, you can assign it to a robot to monitor.

Perform this procedure in the Vantage DX Monitoring Web UI. To access the interface, append `/gizmo` to your Vantage DX instance URL. For example, `https://<your_instance>.vantage-dx.com/gizmo`

1. Select **Settings > Configurations** and click the **Add** button.
2. From the **Create configuration** panel, select the workload you want to monitor, then click **Next**.
3. Enter a name for the configuration. The name you enter displays on the interface.
4. Complete the settings for the workload. You can click the tooltip to see information about each setting.
5. Click **Save**.

Tip: You can edit a configuration, duplicate it, or remove it by clicking the **Actions** button and selecting an option.

Next Steps

- "Assign Configurations to Robot Managers" on page 47

Assign Configurations to Robot Managers

Use this procedure to select the applications that you want the robots at each site to monitor.

Perform this procedure in the Vantage DX Monitoring Web UI. To access the interface, append `/gizmo` to your Vantage DX instance URL. For example, `https://<your_instance>.vantage-dx.com/gizmo`

Before you Begin

- "Create Monitoring Configurations" on page 47
- This procedure uses local system credentials. If there is a proxy server installed between the Robot Manager machine and the robot test site, which requires authentication, you cannot use local system credentials. In that case, ensure that you use credentials that can authenticate with the proxy server and that can access the Windows service where the monitored application runs.

1. Select **Settings > Robots** and select the Robot Manager that you want to configure.
   You can select several Robot Managers at once, or you can check the **Select all in page** box to select all the Robot Managers displayed on the current page.
2. Click **Select configurations**.
3. From the **Configurations** drop-down list, select the workloads that you want to monitor.
4. In the **Windows Service credentials** section, use the **Local system** toggle to select the credentials you want the robot to use:
   - On—The robots use the local system credentials to log into the workloads.
   - Off—Choose this option only if there is a proxy server installed between the Robot Manager machine and the robot test site, which requires authentication. Use the drop-down list to select the credentials that the robots can use to authenticate with the proxy server.
5. Click **Deploy Config**.
   The configurations display on the Robots management page. A status is shown for each:
   - Green—Indicates when the last scan occurred.
   - Blue—Pending status. Scanning is in progress.
   - Red—Indicates an issue with the configuration. A tooltip is available for red statuses. Click on it to display information about the issue.

Tip: You can remove a configuration from a Robot Manager by clicking the X on the configuration name.

Next Steps

- "Add Location Tags to Robot Managers" on page 48

Add Location Tags to Robot Managers

Use this procedure to add a tag that indicates the location of your robots. Tags are required for Power BI to display your robots on a map.

1. Select **Settings > Robots** and select the Robot Manager that you want to configure.
   You can select several Robot Managers at once. You can check the **Select all in page** box to select all the Robot Managers displayed on the current page.
2. Click **Add Tags**.
3. In the **Key** field, select **Location**.
4. In the **Value** field, enter the name of a location or select from a list of existing tags. Use the following format when you enter the location: <City, Region, Country> where <Country> is the 2-letter country code. For example: Ottawa, Ontario, CA.

5. Click the **+** button to confirm the tag and then click **Add**.

Import the Power BI Template for Cloud Deployments

Use the following procedure to open the Vantage DX Monitoring template in Microsoft Power BI and then configure and import the data source in the Power BI Service. The procedure makes the report data accessible in the cloud.

Warning: We strongly recommend that you do not make any changes to this template. Any changes are unsupported and may result in errors or inconsistencies in your reported data, or an inability to retrieve data to populate this report.

Before you Begin

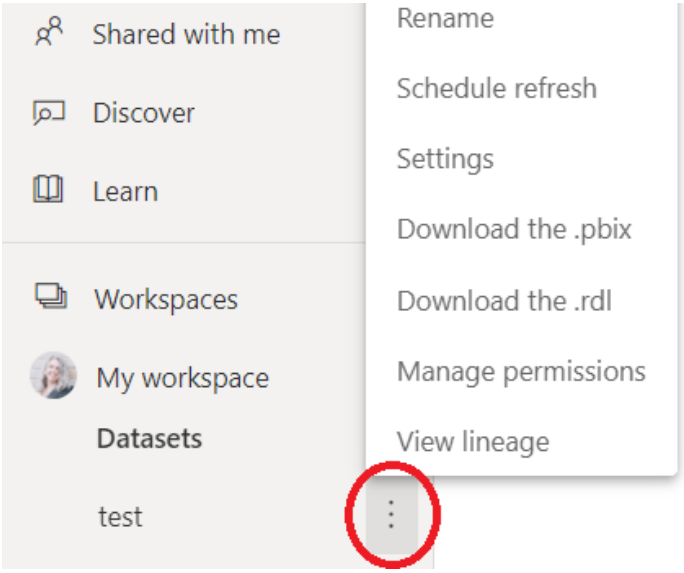
- Download and install the latest version of Power BI. For information and instructions see: https://docs.microsoft.com/en-us/power-bi/fundamentals/desktop-get-the-desktop
- A workspace created in Power BI. See https://docs.microsoft.com/en-us/power-bi/collaborate-share/service-create-the-new-workspaces.
- Ensure that you have the latest version of the Power BI Template. Contact gsx-support@martellotech.com to obtain the template.
- Ensure that you have a Power BI license to publish reports. We recommend a Power BI Pro license so that you can share your reports with a team.

1. Double-click on the `Vantage DX Monitoring Report-<version>.pbit` file to launch load the Power BI template.
2. Provide the following information:
   - Server—The SQL server database that is listed in your Welcome email.
   - Database—The name of the database that is listed in your Welcome email.
   - Range Start—Use 01/01/2020 or any date prior to the installation of Vantage DX Monitoring.
   - Range End—Use 01/01/25 or any date later than today's date.
   - Offset hour—If you want the reports to display your local time zone, enter the number of hours that your local time zone is offset from the UTC time zone. For example, if your local time zone is UTC minus 3 hours, enter `-3`. If your local time zone is UTC plus 4.5 hours, enter `4.5`.
3. If prompted, click the link at the bottom of the **Welcome** page and enter the Power BI license associated with your Office 365 account.
4. On the **Gizmo Analytics** page, click the drop-down next to the **Load** button and select **Edit**.

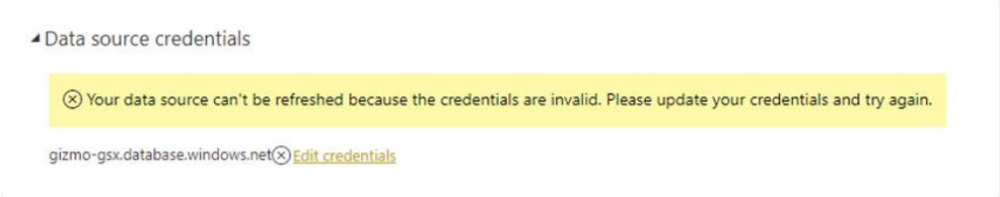
5. With the Vantage DX Monitoring Power BI template open in Power BI Desktop, from the home menu, click **Publish**.
6. Save the report when prompted.

> **Warning:** If prompted to apply pending query changes, click **Apply Later**.

7. Supply your Power BI credentials if prompted.
8. On the **Publish to Power BI** page, click the workspace where you want to share the report, then click **Select**.
9. Once the report is generated, click the link to open the report in Power BI Service.
   Power BI opens in a browser window and the report is displayed.
10. On the left menu pane, scroll down to **My Workspaces >Datasets**, and expand the Datasets menu option.
11. Hover your mouse over the dataset for the report, then click the three vertical dots to display the menu.



12. From the menu, select **Settings**.
13. On the **Datasets** tab, expand the **Parameter** section, provide the following information, then click **Apply**:
    - Database—The SQL server database to use.
    - Server—The name of the database.
14. On the Datasets tab, expand the **Data source credentials** section. If the following error is displayed, click **Edit credentials**:



15. Provide the following user credentials, then click **Sign In**.
    - **Authentication method**: Select the method to use from the list.
    - **User name**: The user name for the data source.
    - **Password**: The password for the data source.
    - **Privacy level setting for this data source**: Select the privacy level to use from the list.
16. Return to the left menu pane, scroll down to **My Workspaces >Datasets**. For the same dataset, click the three vertical dots to open the menu and select **Refresh now**.
17. Wait for the refresh to complete.
    You can view the status of the refresh by clicking the **Refresh history** link on the **Datasets** tab.

Remove a Robot Manager

Use this procedure to remove a Robot Manager from the interface.

Note:
This procedure removes the Robot Manager from the interface only; if the machine is running and the Robot Manager service is still installed, the Robot Manager will re-register and display again in the UI. We recommend that you uninstall the Robot Manager service from the machine before you remove it from the interface.

1. Select Settings > Robots and select one or more Robot Managers.
2. In the Actions column, click the trash can icon to remove the Robot Manager from the list.
   A confirmation message displays.
3. Click **Remove**.

CHAPTER 8

Configure Network Diagnostics

Use the information in this section to install Vantage DX Monitoring Robot Managers at key business locations or on the laptops of remote users and configure network diagnostics. Complete the setup tasks listed in the following table.

Task	Description
"Understanding Network Diagnostics" on page 53	Review this information to understand how Vantage DX monitors the network path to a specified endpoint.
"Install a Robot Manager" on page 53	Optional. Follow this procedure only if you have not already installed the Robot Manager service on machines at your business site, or if you want to perform network diagnostics for a remote user. When you install a Robot Manager at a business site, Vantage DX uses that Robot Manager to perform both synthetic transactions and network diagnostics. If you have already installed a Robot Manager at your business site for the purposes of synthetic transactions, you do not need to install a separate Robot Manager to perform network diagnostics at your business site.
"Configure Custom Endpoints for Network Diagnostics" on page 55	Optional. Vantage DX Monitoring provides a default configuration that monitors the network path to the Teams service. Follow this procedure if you want to configure network diagnostics for other endpoints.

Task	Description
"Assign Network Diagnostics to a Robot Manager" on page 55	Assign network diagnostics configurations to Robot Managers. Follow this procedure for the default Teams configuration, as well as for any custom configurations you have created.
"Add a Work Location Tag" on page 56	If you deploy network monitoring for remote users, we recommend that you create a tag and add it to each Robot Manager that you have deployed on the machine of a remote user.
"Remove a Robot Manager" on page 51	If you uninstall a Robot Manager from a business site or from a user laptop, follow this procedure to remove it from the interface.

Understanding Network Diagnostics

In addition to testing the performance of Microsoft workloads, Vantage DX Monitoring robots can also test the network path between office sites and target endpoints that you want to monitor, such as Microsoft Teams, SharePoint, Salesforce, or other business-critical services.

The Robot Manager installs on a Windows machine at each of your business sites, or on the machine of a remote user. The robot monitors and reports on the flow of data along the network path between the site where it is installed and the target endpoint. It identifies the segment of the network where errors occur. For example, if a user or a location is experiencing high round-trip time (RTT), jitter, or packet loss, you can deploy a Robot Manager to determine the source of the problem. The test results will show whether the issue is occurring in the corporate network, the user's home network, the ISP's network, or the Microsoft network.

The Vantage DX interface provides a visual representation of the quality of the connection at each hop in a network path. This information is shown on network path diagrams to help you quickly understand where issues are occurring along the network path, how your end users are affected, and which networks are responsible for the issues. The interface also provides information about packet loss rate, round-trip latency, and jitter average for each network path.

Install a Robot Manager

Use this procedure if you are deploying network diagnostics on the machine of a remote user, or if you have not yet installed Robot Managers at your business sites.

Note:
When you install a Robot Manager at a business site, Vantage DX uses that Robot Manager to perform both synthetic transactions and network diagnostics. You do not need to install a separate Robot Manager to perform network diagnostics at your business site. If you have already installed a Robot Manager at your business site, proceed to "Assign Network Diagnostics to a Robot Manager" on page 55.

Before you Begin

- Add a custom rule to the Windows Defender firewall that allows the machine of the remote user to accept inbound ICMPv4 connections. Select the following ICMP types:
  - Destination Unreachable
  - Echo Request
  - Time Exceeded
- For more information about connectivity requirements, see "Network Connections" on page 22.

1. In a browser, go to `https://<instance-name>/gizmo/downloads/Gsx.RobotManager.zip` where `<instance-name>` is the name of your Vantage DX deployment.
2. Extract the following files:
   - `Gsx.RobotManager.msi`—This file is used by the script.
   - `Install-GsxRobotManager.ps1`—This file is the script to run.
   - `Transform.mst`—This file is used by the script.

   No specific location is required.
3. Open PowerShell as Administrator.
4. Enter the cmdlet `Set-ExecutionPolicy RemoteSigned`
5. Choose **[A] Yes to All**.
6. To run the `Install-GsxRobotManager.ps1` script, navigate to the script location path in PowerShell and run the following command: `.\Install-GsxRobotManager.ps1`
7. Choose **[R] Run once** after the Security Warning.
8. In the Web UI, refresh the Robots management page and verify that all Robot Managers display the correct version.
   To access the interface, append `/gizmo` to your Vantage DX instance URL. For example, `https://<your_instance>.vantage-dx.com/gizmo`

Next Steps

- "Configure Custom Endpoints for Network Diagnostics" on page 55.

Configure Custom Endpoints for Network Diagnostics

By default, Vantage DX Monitoring provides a configuration that monitors the network path to the Teams service, but you can also monitor custom endpoints. Use this procedure to configure the parameters needed to connect to custom endpoint and collect metrics.

Perform this procedure in the Vantage DX Monitoring Web UI. To access the interface, append `/gizmo` to your Vantage DX instance URL. For example, `https://<your_instance>.vantage-dx.com/gizmo`

Note:
If you are configuring network diagnostics for the path between your location and the Zoom service, use the following endpoint: web.zoom.us. This endpoint is used for all geographical locations.

1. In Vantage DX Monitoring, select **Settings > Configurations** and click the **Add** button.
2. From the **Create configuration** panel, select one of the following options:
3. Select **Network Diagnostics**, then click **Next**.
4. Enter a name for the configuration. The name you enter is used to identify the configuration on the interface.
5. Complete the settings for the endpoint. You can click the tooltip to see information about each setting.
6. Click **Save**.

Next Steps

- "Assign Network Diagnostics to a Robot Manager" on page 55

Assign Network Diagnostics to a Robot Manager

After you configure network diagnostics, you must assign the configuration to one or more Robot Managers. You can assign network diagnostics to Robot Managers located at your business sites or located on the machine of a remote user.

Complete this procedure for the default Teams configuration, as well as for any custom endpoints you have configured.

Perform this procedure in the Vantage DX Monitoring Web UI. To access the interface, append `/gizmo` to your Vantage DX instance URL. For example, `https://<your_instance>.vantage-dx.com/gizmo`

1. Select **Settings > Robots** and select the Robot Manager at the location where you want to perform network diagnostics.

You can select several Robot Managers at once, or you can check the **Select all in page** box to select all the Robot Managers displayed on the current page.

2. Click **Select configurations**.
3. From the **Configurations** drop-down list, select **Teams Network Diagnostics**.
4. If you have configured network diagnostics for custom endpoints, click the drop-down list again and select the configuration. Repeat this step until you have selected all network diagnostics configurations that you want the robot to monitor.
5. In the **Windows Service credentials** section, use the **Local system** toggle to select the credentials you want the robot to use:
   - On—The robots use the local system credentials to log into the workloads.
   - Off—Choose this option only if there is a proxy server installed between the Robot Manager machine and the robot test site, which requires authentication. Use the drop-down list to select the credentials that the robots can use to authenticate with the proxy server.
6. Click **Deploy Config**.
   The configurations display on the Robots management page. A status is shown for each:
   - Green—Indicates when the last scan occurred.
   - Blue—Pending status. Scanning is in progress.
   - Red—Indicates an issue with the configuration. A tooltip is available for red statuses. Click on it to display information about the issue.

Tip: You can remove a configuration from a Robot Manager by clicking the X on the configuration name.

Next Steps

- If you are configuring network diagnostics for a remote user, see "Add a Work Location Tag" on page 56.

Add a Work Location Tag

If you deploy network monitoring for remote users, we recommend that you create a tag and add it to each Robot Manager that you have deployed on the machine of a remote user. The tag allows you to easily differentiate Robot Managers that are at office locations from Robot Managers that are in non-office locations, which is helpful when you troubleshoot alerts.

Perform this procedure in the Vantage DX Monitoring Web UI. To access the interface, append `/gizmo` to your Vantage DX instance URL. For example, `https://<your_instance>.vantage-dx.com/gizmo`

1. Select **Settings > Robots** and select all of the Robot Managers that are deployed in the machines of remote users.

You can select several Robot Managers at once.

2. Click **Add Tags**.
3. In the **Key** field, type **Work Location**.
4. In the **Value** field, enter **Remote**.
5. Click the **+** button to confirm the tag and then click **Add**.

Tip:
After you apply the tag, you can easily monitor the remote users. In VDX Analytics, click **Explore** and select the **Groups & Services** tab. In the search bar, type "Work Location." The tag you created in this procedure is shown as a Group component. Pin the component to a board to see alerts related to Robot Managers included in the group. You can also configure notifications for the board.

CHAPTER 9

Model Data

The information in this section explains how to use VDX Analytics to organize data using boards and business services. Complete the setup tasks listed in the following table.

Task	Description
"Understanding Boards and Business Services" on page 59	Use the information in this section to understand the ways that you can organize data retrieved from VDX Diagnostics, Vantage DX Monitoring, and other monitoring and ITSM systems.
"Perform a Search" on page 59	Search for objects, alerts, or incidents, and save your searches.
"Create a Board" on page 65	Organize objects from one or more monitoring systems. You can create boards that reflect your organizational structure.
"Create Sub-Boards" on page 66	Create sub-boards when you want to add child boards to a parent board.
"Create a Synced Board" on page 66	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 67	Create business services when you want to monitor critical services and report on the SLA of the service.
"Configure Rules" on page 68	Dynamically add objects to a board or business service using rules.

Task	Description
"Configure Exclusions" on page 69	Use exclusions in conjunction with rules to refine the scope of objects that are dynamically added to a board or business service.

Understanding Boards and Business Services

VDX Analytics provides two ways to organize your monitoring data:

- Boards
- Business services

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.

Business services are services that you deliver to your internal and external customers. Business services range from accounts receivable and email to VoIP calls and web sites.

Business service management (BSM) is a way of mapping the devices and applications that work together to support specific business services. When you map devices and applications to a business service, you can monitor your organization's IT resources in the context of the business workflow where those resources are used. For each business service that you define, you can map the IT components to the following ITIL workflow perspectives:

- End User
- Application
- Infrastructure
- Supplier services (other services that impact the current 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" on page 60

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 5: 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`

Integration	Search Term

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`

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`

Integration	Search Term

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`

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`

Integration	Search Term

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

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

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.
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.

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:

- "Create a New Board" on page 66 and then search for objects and pin them at a later time.
- Search for an object and "Create a Board from Search Results" on page 66.

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:

- "Create a New Business Service" on page 67 and then search for objects and pin them at a later time.
- Search for an object and "Create a Business Service from Search Results" on page 68.

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**.

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" on page 69
- "Create a Rule from an Existing Saved Search" on page 69

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.

CHAPTER 10

Manage Notifications and Incidents

The information in this section explains how to use VDX Analytics to configure notifications and manage incidents. Complete the setup tasks listed in the following table.

Task	Description
Notifications for Boards and Business Services	
"Configure Notifications for Boards and Business Services" on page 72	Configure an email 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. You can also configure notifications that are triggered when your SLA goal has been breached, or when it is about to be breached.
Notifications for Dashboards	
Configure notifications for dashboards: • "Understanding Dashboard Notifications" on page 75 • "Configure Dashboard Notifications" on page 1	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 81	Configure notifications that are triggered when warnings or errors are raised for an integration or for the Vantage DX application.

Task	Description
Notifications—All Types	
"Assign an Email Address for Notifications" on page 82	Specify the email address that you want Vantage DX to use for notifications.
"Configure the Interval for Notifications and Incidents" on page 83	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.
Incidents	
"Configure Incident Automation" on page 83	If you have integrated an ITSM system with VDX Analytics, you can automate the creation of 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 6: 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.
Incidents	VDX Analytics sends one notification that contains information about all the incidents that have been created within the last 5 minutes.

Event	Description
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 address before you begin. See "Assign an Email Address for Notifications" on page 82

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 "Install Remote Agents" on page 96 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 main 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.

The Actions available depend on the integrations that you have configured.

6. Click **+** to add the notification.
7. Select the **Recipient List** tab.
   The option to Notify All Recipients is enabled by default.
8. Click the slider to disable the default and instead select the role from the **Select Recipients** 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 93.

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 "Install Remote Agents" on page 96 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 77
- "Zoom Notifications" on page 79
- "Vantage DX Instances Prior to Release 3.17 (June 2024) " on page 79

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 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 "Assign an Email Address for Notifications" on page 82.

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**—By default, this option is enabled when you enable Application Health. You can de-select this option if you do not want to receive notifications about system warnings.
    - **System Error**—By default, this option is enabled when you enable Application Health. You can de-select this option if you do not 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**.

Assign an Email Address for Notifications

Use this procedure to specify the email address that you want VDX Analytics to use for notifications.

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.

You can assign one email address for each role.

Perform this procedure on the VDX Analytics interface.

1. From the main menu, select **Settings**.
2. Click the **Roles** tab and select a role.
3. Click the **Edit** icon.
4. On the **Claim Mappings** tab, enter an email address in the **Email** field. It is a best practice to use a distribution list for the notification address.
5. Click **Add**.

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.

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.

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**.

CHAPTER 11

Manage and Report SLA Data

Use the information in this section to configure how Service Level Agreements (SLAs) are calculated and to generate SLA reports for business services. Complete the setup tasks listed in the following table.

Task	Description
"Configure Downtime for SLA Reporting" on page 86	Configure the health states that you want to include in downtime calculations.
"Configure SLO for a Business Service" on page 86	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.
"View and Save SLA Availability Data for a Business Service" on page 87	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 88	Generate a PDF report of the SLA performance data for multiple business services.
"Schedule an SLA Report" on page 90	Schedule SLA reports and automatically send them to recipients by email.
"Manage Scheduled SLA Reports" on page 91	Change or delete the schedules for SLA reports.
"Exclude Component Outages from SLA Calculations" on page 91	Select one or more outages that contributed to downtime and exclude them from SLA calculations.

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 86.
- To see SLA performance, see "View and Save SLA Availability Data for a Business Service" on page 87.
- To generate an SLA performance report for multiple business services, see "Generate an On-Demand SLA Report for Multiple Business Services" on page 88

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 86.

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.

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 86.
- To configure service level objectives, see "Configure SLO for a Business Service" on page 86.
- To exclude components and recalculate SLA information, see "Exclude Component Outages from SLA Calculations" on page 91.
- To view and save SLA data for a single business service, see "View and Save SLA Availability Data for a Business Service" on page 87.

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.

CHAPTER 12

Manage User Access

Follow the procedures in this section if you want to allow your users to access specific boards or business services in VDX Analytics.

Task	Description
"Create a Role" on page 93	Create roles for the different types of users who will have access to VDX Analytics.
"Add Integrations to a Role" on page 93	Manage the integrations that can be viewed by users in different roles.
"Add Boards or Business Services to a Role" on page 94	Manage how users in different roles can access boards and business services.
"Add Dashboards to a Role" on page 94	Select the dashboards that users in each role can view.
"Scope Access" on page 95	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.
"Configure Access to Saved Searches" on page 95	Control who can see and use saved searches.

Create a Role

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.

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.

Perform this procedure on the VDX Analytics interface.

1. From the main menu, select **Settings**.
2. Click the **Roles** tab.
3. Click the **Add** button.
4. Enter a name for the role and click **Create**.
5. On the **Claim Mappings** tab, click the **Add** button.
6. In the **Claim Value** field, enter the name of the group provided to you by your Martello Delivery Engineer. If you need additional groups, contact your Martello Delivery Engineer.
7. 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.
8. Click **Add**.

Add Integrations to a Role

Perform this procedure on the VDX Analytics interface.

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**.

Note: If you are a service administrator and are configuring access for a customer, ensure that you select the Microsoft Teams Call Quality integration and the Microsoft 365 integration for the customer's tenant, as well as the Vantage DX Monitoring integration that you created for the customer.

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

Perform this procedure on the VDX Analytics interface.

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

Perform this procedure on the VDX Analytics interface.

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 93.

Scope Access

Perform this procedure on the VDX Analytics interface.

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 93.
- To manage the boards and business services that users can access, see "Add Boards or Business Services to a Role" on page 94.

Configure Access to Saved Searches

Perform this procedure on the VDX Analytics interface.

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**

CHAPTER 13

Integrate Additional Systems

Follow the procedures in this section if you want to integrate additional monitoring tools or an ITSM system with VDX Analytics. Complete the setup tasks listed in the following table.

Task	Description
"Install Remote Agents" on page 96	Install a remote agent so that your other monitoring tools or ITSM systems can connect to the VDX Analytics web server.
"Add an Integration" on page 97	Integrate your other monitoring tools or ITSM systems with VDX Analytics.

Install Remote Agents

If you are integrating other monitoring systems with Vantage DX Analytics, you must install a remote agent at your site.

The remote agent installs as a Windows service.

Before you Begin

- Ensure that the machine where you are installing the remote agent has .Net Framework 4.7.2 or higher.
- Contact your Martello Delivery Engineer to obtain the Client ID and Client Secret; you need to enter this information when you install the remote agent.

1. From the remote computer, open your browser and log into VDX Analytics.
2. From the main menu, select **Settings >Agents**.
3. Click the **Download Agent** icon in the bottom corner of the page.
   The AgentInstaller.zip file downloads.
4. Extract the files.
   There are two files: `Martello Vantage DX Analytics Agent-<version>.exe` and `Setup.cmd`.
5. Choose one of the following options:

- Double-click the `Setup.cmd` to launch the installer with the VDX Analytics web server URL pre-populated.
- Right-click on `Martello Vantage DX Analytics Agent-<version>.exe` and select **Run As Administrator**.

6. Click **Next** on the welcome screen.
7. Select **I accept the agreement** and click **Next**.
8. If you did not use the `Setup.cmd` file, enter the URL of the VDX Analytics web server.
9. Enter the Client ID and the Client Secret provided by your Martello Delivery Engineer and click **Verify**.
10. Enter the destination where you want to install the agent and click **Next**.
11. Click **Finish** when the installation is complete.
    After a few moments, the remote agent is listed as an available agent in VDX Analytics.

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**.

CHAPTER 14

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.