MARTELLO

VANTAGE DX

DEPLOYMENT GUIDE FOR ENTERPRISES

RELEASE 3.15
DOCUMENT DATE: FEBRUARY 26, 2024

NOTICE

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

Trademarks

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

Windows and Microsoft are trademarks of Microsoft Corporation.

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

Deployment Guide for Enterprises
Release 3.15 - February 26, 2024

Contents

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

CHAPTER 5

CHAPTER 6

CHAPTER 7

CHAPTER 8

CHAPTER 9

CHAPTER 10

CHAPTER 12

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 all of 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
- Microsoft Performance Data in Vantage DX

VDX Analytics

- VDX Analytics Integration Guide
- VDX Analytics User Guide

Vantage DX Monitoring

- Vantage DX Monitoring User Guide

VDX Diagnostics

- VDX Diagnostics Administration Guide for Enterprises

Revision History

Document Date	Description
February 26, 2024	Vantage DX 3.15Deployment Guide for Enterprises

CHAPTER 2

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" on page 9
- "Supported Browsers" on page 11
- "Permissions and Access" on page 11
- "Account Requirements" on page 12
- "Network Connections" on page 15
- "Machine Requirements" on page 18

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.

- "Real User Monitoring" on page 9
- "Customers, Sites, and Services in VDX Diagnostics" on page 10
- "Robot Managers and Workloads in Vantage DX Monitoring" on page 10

Real User Monitoring

The first integration that you configure in a Vantage DX deployment is between VDX Analytics and the Microsoft Call Quality Dashboard (CQD). This integration provides monitoring data for real users.. If you business has multiple tenants, you need to configure an integration for each tenant.

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

CQD-TENANTNAME

Customers, Sites, and Services in VDX Diagnostics

In VDX Diagnostics, you must configure a Site Group for your business, as well as Sites (locations) and Services (endpoints to test). We recommend that you use a naming convention that you can apply to all of the configurations.

Examples

Site Groups:

BUSINESSNAME or SUBSIDIARY

Sites:

BUSINESSNAME-OFFICE. For the site name, use the name of the office or building where the probe is deployed. If the probe is deployed on the equipment of a specific user, enter the user principle name (UPN) as the site name. For the site location, use the format `<City, Region, Country>`, where `<Country>` is the 2-letter country code.

Services (endpoints to test):

BUSINESSNAME/SUBSIDIARY-LOCATION-SERVICENAME

Robot Managers and Workloads in Vantage DX Monitoring

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 type of deployment or the deployment environment. For example: PRD for a production environment. DEV for a development environment.
- 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.
- Optionally, you can identify the connection type, such as WIFI or Wired.

Examples

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

PRD-CITY-R1

For example: `PRD-PARIS-R1`

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`.

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.

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 11
- "Groups Required for SSO" on page 12

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

When you grant consent, you give the Vantage DX application the following permissions:

- Read directory RBAC settings
- Read all usage reports
- Sign in and read user profile
- Read all users' full profiles
- Read Teams devices
- Read organization information
- Read all company places
- Read all users' full profiles
- Read all usage reports
- Read service health

Groups Required for SSO

In Azure AD, create the following groups and assign them to the Vantage DX Enterprise application:

- Service Administrators
- Service Operators
- Read-Only users

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 Azure, 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 12
- "Advanced Accounts " on page 13

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 and Teams Advanced workloads. For other workloads, see "Advanced Accounts " on page 13.

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. An attendee user account with a provisions 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.
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/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 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 15
- "Advanced Connections" on page 17

Basic Connections

The following table lists the connectivity requirements for theVantage DX modules.

Protocol and Port	Source IP	Endpoint / Destination	Description
HTTPS			
443	Probe (machine where installed)	<instancename>.vantage-dx.com/npv-ui	Probe connection to Vantage DX.
443	Robot Manager (machine where installed)	<instancename>.vantage-dx.com	Robot connection to Vantage DX
ICMP			
Type 0	Any	Probe (machine where installed)	Echo reply
Type 11	Any	Probe (machine where installed)	TTL exceeded
Type 8	Probe (machine where installed)	Any	Echo request
TCP			
443	Robot Manager (machine where installed)	One of the following: • **Western European region:** eager-swan.rmq.cloudamqp.com • **Eastern United States region:** sharp-fuchsia-mongoose.rmq4.cloudamqp.com • **Australia:** active-olive-lemming.rmq4.cloudamqp.com	Robot connection to Vantage DX

Protocol and Port	Source IP	Endpoint / Destination	Description
443	Robot Manager (machine where installed)	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
AMPQS			
5671 (Installations prior to June 2023)	Robot Manager (machine where installed)	One of the following: • **Western European region:** eager-swan.rmq.cloudamqp.com • **Eastern United States region:** sharp-fuchsia-mongoose.rmq4.cloudamqp.com • **Australia:** active-olive-lemming.rmq4.cloudamqp.com	Robot connection to Vantage DX

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:

- <your instance>-vantage-dx-com-7ec3ca.kb.westeurope.azure.elastic-cloud.com
- *.elastic-cloud.com:*
- https://www.googletagmanager.com
- https://www.google-analytics.com
- https://stats.g.doubleclick.net
- https://*.tile.openstreetmap.org
- *.msauth.net
- *.microsoft.com
- *.microsoftonline.com

- *.live.com

Remote Agent

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 discovery endpoint: https://cqdrepositoryapiprodv3centralus.azurewebsites.net/tenant/dataservice
- The Regional 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 and VDX Diagnostics Probes

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

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

Machine Requirements

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

- "Specifications" on page 18
- "Antivirus Exclusions" on page 19
- "Certificates" on page 20

Specifications

Use the specifications listed in the following table when you install any of the following components:

- Vantage DX Monitoring Robot Manager services
- Vantage DX Diagnostics probes
- VDX Analytics remote agents

Table 1: Machine Requirements

Component	Minimum	Recommended
Operating system	Windows 10 (64-bit)	Windows 10 (64-bit) or later

Component	Minimum	Recommended
Processor	2.5 Ghz Quad-Core or 4 vCPUs	2 Ghz or faster
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 This dedicated machine can host both the Robot Manager service and the Vantage DX Diagnostics probe.	✓	
Vantage DX Diagnostics probes We recommend that you install the probe on the same machine where you install the Robot Manager service.		✓
VDX Analytics remote agent		✓
Additional requirements: Vantage DX Monitoring Robot Manager		
Power settings	Always on	—
Browser	Google Chrome	The current version is recommended; two previous versions are supported.

Antivirus Exclusions

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

We recommend that you exclude the processes and directories listed below from the files scanned by your antivirus software.

Processes

- Gsx.Robot

- Gsx.RobotManager
- Gsx.Robot.exe

Directory

- C:\Program Files (x86)\GSX Solutions*

Ports

- Ports 51000 to 65535

URLs

- The following URL must be accessible: https://<instance>.vantage-dx.com/gizmo/downloads/

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.

CHAPTER 3

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" on page 21
- "Analyze Data and Identify Critical Locations" on page 21
- "Deploy Robots" on page 23
- "Deploying Probes" on page 24
- "Example" on page 24

Integrate your Microsoft Data

The first step in the deployment process is to integrate your Microsoft 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 your 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 VDX Diagnostics probes and 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 and VDX Diagnostics probes:

- **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 22 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:

- 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. You can install the robot 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 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.
- 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:

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 52.

Deploying Probes

The number of VDX Diagnostics probes that you can deploy depends on your license package.

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

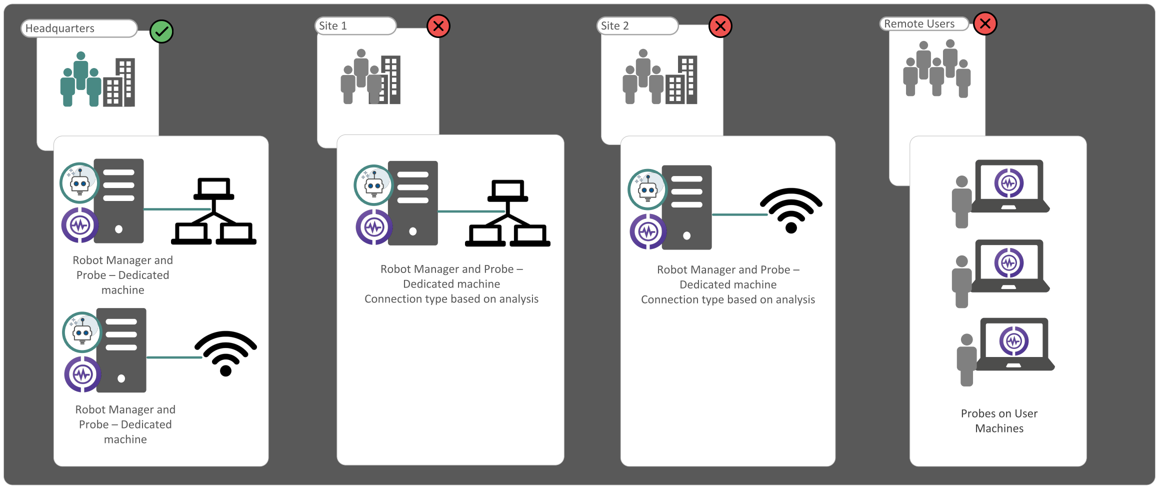
- Deploy one probe at each business-critical site. We recommend that you install a probe at any location where you have installed a robot manager. You can install the probe on the same machine that hosts the robot manager.
- Deploy one probe at each site where you have known issues, or where you have identified problems based on your analysis of the dashboard data.
- Deploy one probe on the machine of a user who is affected by poor call quality, based on your analysis of the dashboard data. We recommend this approach for VIP users who work remotely.

For more information about deploying probes, see "Configure Network Path Monitoring" on page 42.

Example

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

Figure 1: Example of a Vantage DX Deployment

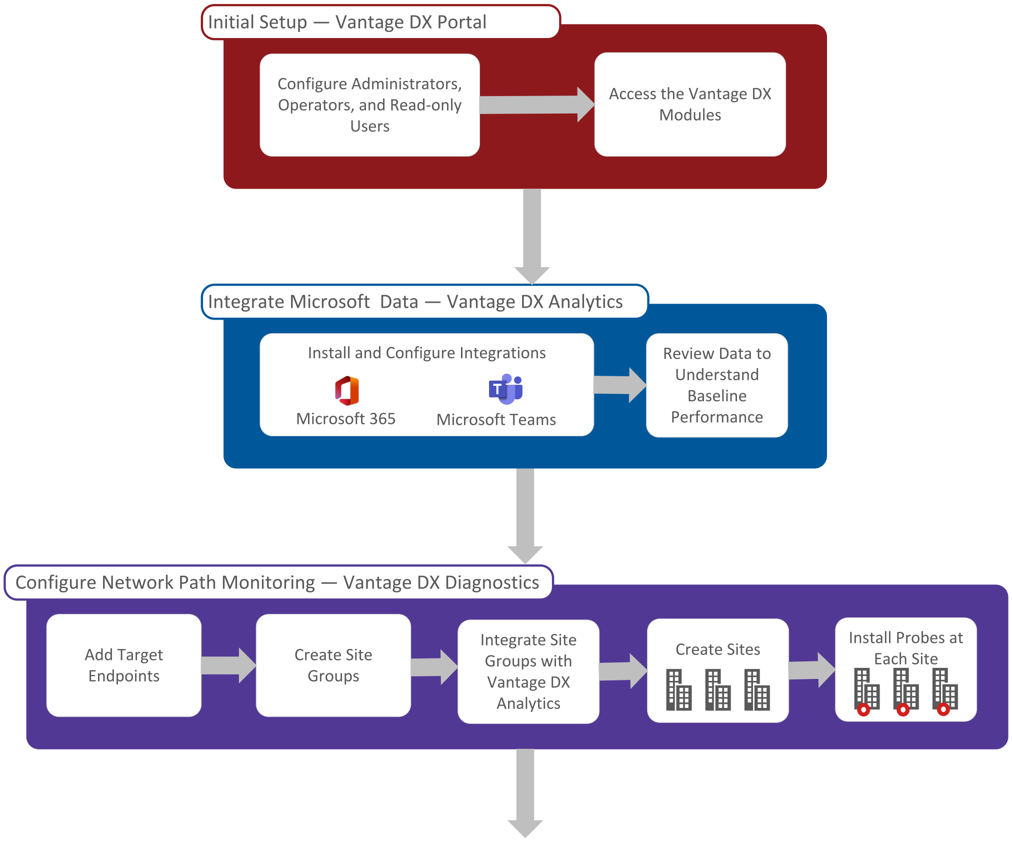

Headquarters
Robot Manager and Probe – Dedicated machine
Robot Manager and Probe – Dedicated machine
Site 1
Robot Manager and Probe – Dedicated machine
Connection type based on analysis
Site 2
Robot Manager and Probe – Dedicated machine
Connection type based on analysis
Remote Users
Probes on User Machines

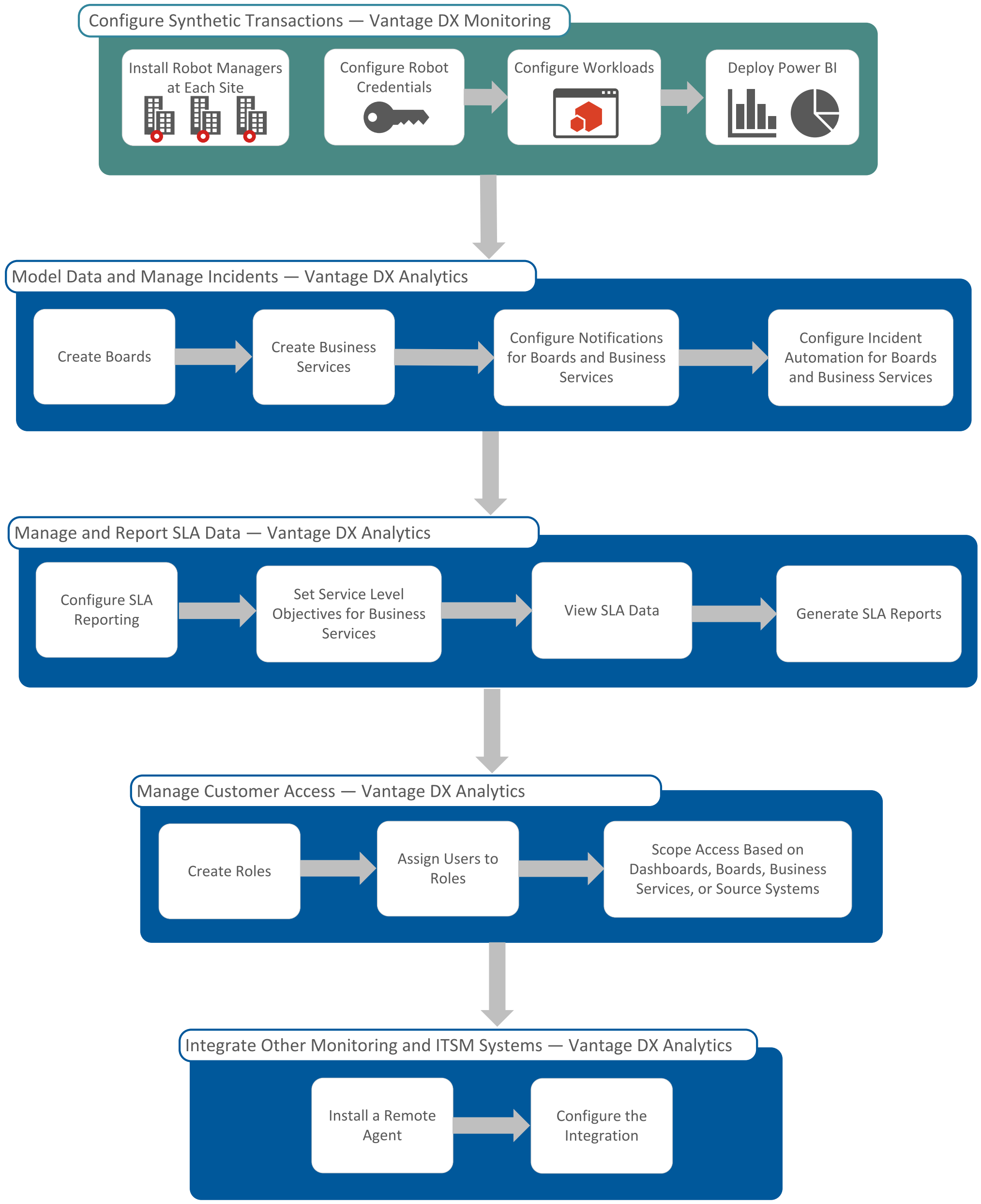
CHAPTER 4

Deployment Workflow

The following image provides an overview of the deployment tasks that you complete when you set up Vantage DX. The colors and the labels indicate the management interface that you use to complete each task.

Figure 2: Deployment Workflow


Initial Setup — Vantage DX Portal
Configure Administrators, Operators, and Read-only Users
Access the Vantage DX Modules
Integrate Microsoft Data — Vantage DX Analytics
Install and Configure Integrations
Microsoft 365
Microsoft Teams
Review Data to Understand Baseline Performance
Configure Network Path Monitoring — Vantage DX Diagnostics
Add Target Endpoints
Create Site Groups
Integrate Site Groups with Vantage DX Analytics
Create Sites
Install Probes at Each Site


Configure Synthetic Transactions — Vantage DX Monitoring
Install Robot Managers at Each Site
Configure Robot Credentials
Configure Workloads
Deploy Power BI
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

Initial Setup

Use the following table to complete the setup tasks.

Task	Description
"Configure Users" on page 28	Add administrators, operators, and read-only users for your Vantage DX instance.
"Access Vantage DX" on page 29	Access the Vantage DX management interfaces.

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 76.

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 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 the Vantage DX application 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.
     - The ability to create sites and install probes in VDX Diagnostics.
   - **Read-Only**—Users assigned to this group have read-only access to information in Vantage DX.

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 and VDX Diagnostics from within VDX Analytics, or you can go directly to those interfaces using their specific URLs. 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/auth`
2. Click **Administration Console** and log in.
   VDX Analytics launches.
3. View a component that is retrieved from Vantage DX Monitoring or VDX Diagnostics, 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`.

- **VDX Diagnostics**—Append /npv-ui to your Vantage DX instance URL. For example, `https://<your_instance>.vantage-dx.com/npv-ui`.
- **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**.
   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**.

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)	The amount of time in minutes that the CQD query will look back from the last call that was loaded into the database. The default value is 120 minutes; however, if you select a custom tenant size, you must enter a value.
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.
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.

Property	Description
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%.
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.

Property	Description
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.
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.

Property	Description
Office Display Names	Optional. Use this field if you want to customize the office names that are displayed in the dashboards. To use this feature, complete the following steps: **1.** Create a .CSV file that lists the office names you wish to display. Enter one line for each office, using the following format: `<ipaddress>,<officename>,add` **2.** Upload the file to OneDrive. Ensure that the file is shared with the Microsoft 365 account that is assigned to the integration and that the file is downloadable. **3.** Click the main menu and select **Settings**. **4.** On the Integrations tab, locate the Microsoft CQD integration and clicking the **Edit** icon. **5.** In the **Office Display Names** field, enter the OneDrive link to the .CSV file that you shared with the Microsoft 365 account in Step 2. **6.** Click **Save**. If you do not use this option, offices are identified by their IP addresses only.
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.

Property	Description
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.
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 11.

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**.

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

Property	Description
Source	Read-only. The name of the source system.
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://support.martellotech.com/knowledgeBase/15513875

If you follow the manual process, ensure that the Microsoft Graph API has the following permissions:

- Organization.Read.All
- Reports.Read.All
- ServiceHealth.Read.All
- TeamworkDevice.Read.All or TeamworkDevice.ReadWrite.All (optional, for data collection from Teams meeting room devices)

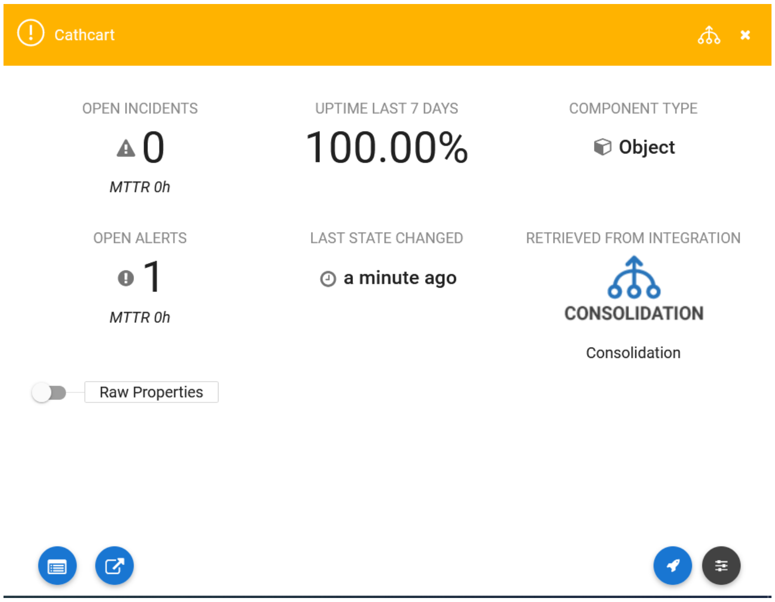
Configure Meeting Room Data

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.



Cathcart

OPEN INCIDENTS 0 MTTR 0h

UPTIME LAST 7 DAYS 100.00%

COMPONENT TYPE Object

OPEN ALERTS 1 MTTR 0h

LAST STATE CHANGED a minute ago

RETRIEVED FROM INTEGRATION CONSOLIDATION Consolidation

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 Network Path Monitoring

Use the information in this section to begin monitoring the network paths between your users and business-critical endpoints. Complete the setup tasks listed in the following table.

Task	Description
"Add Target Endpoints" on page 43	VDX Diagnostics is configured to monitor the Microsoft Teams endpoint by default. You can monitor additional endpoints, such as Microsoft 365 SharePoint, O365 Outlook Exchange Server, and Salesforce.
"Create a Site Group" on page 44	Create a site group to represent your company.
"Configure the Vantage DX Analytics Integration" on page 46	Configure an integration between the site group and VDX Analytics.
"Create a Site" on page 47	Create sites within each site group to represent the physical locations of your offices.
Choose one of the following options: • "Install a Windows Probe" on page 48 • "Install a Probe Using Deployment Software" on page 48	Install a Windows probe at each site.

Task	Description
Choose one of the following options: - "Configure a Windows Probe" on page 49 - "Configure a Software Deployed Probe" on page 50	Configure each probe to connect with VDX Diagnostics. Follow the procedure that corresponds to the method you used to install the probe.

Add Target Endpoints

At the support organization level, add the target endpoints that you want to monitor.

The Microsoft Teams endpoint is included by default for your support organization. You can also monitor custom endpoints, such as Microsoft 365 SharePoint, O365 Outlook Exchange Server, or Salesforce. When you configure a custom endpoint, it is available to all of the site groups within your support organization. You can further customize it for each site group.

To add custom endpoints to your support organization, perform the following steps:

Before you Begin

- You must know the target endpoint URL or IP address.
- The provided FQDN or IP address must be able to respond to ICMP ping requests.

1. Click **Manage** to access the Application Management page, then click **Support Organization**.
2. On the Manage Support Organization page, beside the Services heading, click the **Add** link and set the following options.
   - **Name**—Type a descriptive name for the target endpoint.
   - **Default Target**—The URL/FQDN or IP address for the endpoint. This default target can be further customized per site group.
   - **Frequency**—Specify how often to check the network path for the endpoint. Select one of:
     - Every 5 minutes
     - Every 15 minutes
     - Every 30 minutes
3. Click **Save**.

Next Step

- "Create a Site Group" on page 44

Create a Site Group

A site group represents your entire enterprise company. You only need one site group. The site group allows you to have a global view of the monitored site locations within your enterprise.

To create a site group, complete the following steps.

Before you Begin

- The endpoints to be monitored must already be configured at the Support Organization level.

1. Click **Manage** to access the Application Management page, then click **Site Groups**.
2. On the **Manage Site Groups** page, click **Create Site Group**.
3. Provide a **Name** for the site group in the **Create New Site Group** section.
4. In the **Monitor Services** section toggle the applicable endpoints options to **On**.
5. Configure the following options for each of the enabled endpoints, then click **Save**:

Option	Description
Target	The monitored endpoint. For Microsoft Teams, select one of the following: • Discover Microsoft Teams Server (recommended). This option presents an exact server IP address to which a Microsoft Teams Server can connect. • General Microsoft Teams Server • Custom—Supply the URL **Warning:** Unless you have been specifically directed by Martello, do not change the Microsoft Teams settings. If you have changed these settings prior to reading this warning, you can reset the values for Target back to "Discover Microsoft Teams Server" and the ToS value to 184. For the other custom endpoints, you can use the default target value configured for the Support Organization, or you can provide a custom endpoint as a URL or IP address. Any changes to the target are applicable to this site group only.
Packet ToS	Use the Priority slider to specify a Type of Service value to define the traffic classification for network data and the associated DSCP value. Alternatively, you can type the ToS value into the text box. The default value is 184.
Protocol	Select the protocol to use: • ICMP • TCP • UDP **Note:** Only ICMP is supported for this release of VDX Diagnostics.
Port	Specify the port to use if the protocol is set to TCP or UDP.

Option	Description
Packet Size	Specify the packet size in bytes for data transmission.
Packet Count	The number of pings per hop. Select one of: • 10 • 30 • 50

Next Steps

- "Configure the Vantage DX Analytics Integration" on page 46

Configure the Vantage DX Analytics Integration

Use this procedure to integrate Vantage DX Diagnostics with Vantage DX Analytics.

Every site group in VDX Diagnostics must have an integration configured in Vantage DX Analytics. This integration allow you to view the VDX Diagnostics components and alerts in VDX Analytics.

To configure the integration, complete the following steps.

Before you Begin

- The site group in VDX Diagnostics must already exist.
- A license for the site group in VDX Analytics must be in place.

1. Click **Manage** to access the Application Management page, then click **Site Groups**.
2. On the **Manage Site Groups** page, select the site group for the integration.
3. Next to the Vantage DX Diagnostics Configuration Integration, click **Show**.
4. Make note of the following information, as you will need it to configure the integration in VDX Analytics:
   - Vantage DX Diagnostics URL
   - Site Group GUID
   - Username
   - Password
5. Navigate to VDX Analytics.
6. From the main menu in VDX Analytics select **Settings**.
7. On the **Integrations** tab, click the **Add** button at the bottom of the page.
8. Select **Vantage DX Diagnostics** from the list of integration options.
9. Enter the following information.

Property	Description
Source	Read-only. The name of the source system.
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.
Vantage DX Diagnostics URL	The URL for the VDX Diagnostics environment. Copy and paste the URL from the VDX Diagnostics Site Group page.
Site Group GUID	The site group specific GUID. Copy and paste the GUID from the VDX Diagnostics Site Group page.
Username	The generated username for the VDX Diagnostics site group. Copy and paste the username from the VDX Diagnostics Site Group page.
Password	The generated password for the VDX Diagnostics site group. Copy and paste the password from the VDX Diagnostics Site Group page.
Number of alerts for service to be critical	The number of alerts reported by VDX Diagnostics before the status of an endpoint is shown as critical in VDX Analytics.
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.

10. Click **Save**.

Next Steps

- "Create a Site" on page 47

Create a Site

Use this procedure to create a site that represents a physical office location, or that represents a remote user.

1. Click **Manage** to access the Application Management page, then click **Sites**.
2. On the **Manage Sites** page, click **Create Site**.
3. On the **Create Site** page, provide the site information, then click **Save**:

- **Name**—Provide a name for the site.
  - For an office, enter the office or building name.
  - For a specific user, enter the user principal name (UPN) of the user.
- **Address**—Provide the city and country using the format `City, Country`, where `Country` is the 2-letter country code. For example Vancouver, CA.

Next Steps

- Install and a configure a probe for the site. See "Install a Windows Probe" on page 48.

Install a Windows Probe

Use the following procedure to install a Windows probe for each of your sites. This procedure must be completed for each configured sites. Each probe must be installed on a machine that is located at the site you are configuring.

Before you Begin

- A site must already be configured. See "Create a Site" on page 47.

1. Click **Manage** to access the Application Management page, then click **Sites**.
2. On the **Manage Sites** page, select the site where you want to install the probe, then click the **Windows - Download** link to download the installer.
3. Extract the file and ensure that the installer is not blocked by your operating system. After you download the installer, follow these steps:
   - Right-click on the MSI file.
   - Click **Properties**.
   - In the **Security** section, select the **Unblock** checkbox.
   - Click **OK**.
4. Run the file to install the probe software on a machine that is located at the site being configured.
5. If prompted, click **Yes** to allow the application to make changes to the computer.
6. Follow the instructions in the Install Wizard to complete the installation.
7. When the install process is complete, click **Finish** to exit the Wizard.

Next Steps

- Configure the probe to communicate with VDX Diagnostics. See "Configure a Windows Probe" on page 49.

Install a Probe Using Deployment Software

Use the following procedure to install a Vantage DX Diagnostics probe for each of your sites. You must be an administrator to perform this procedure.

Before you Begin

- A site must already be configured. See "Create a Site" on page 47.

1. Click **Manage** to access the Application Management page, then click **Sites**.
2. On the **Manage Sites** page, select the site where you want to install the probe, then click the **Windows - Download** link to download the installer.
3. Extract the file and ensure that the installer is not blocked by your operating system. After you download the installer, follow these steps:
   - Right-click on the MSI file.
   - Click **Properties**.
   - In the **Security** section, select the **Unblock** checkbox.
   - Click **OK**.
4. Run the installer using your own deployment software. To complete the installation without user input, ensure that you run the installer with the `/quiet` option.

Next Steps

- Configure the probe to communicate with VDX Diagnostics. See "Configure a Software Deployed Probe" on page 50.

Configure a Windows Probe

After you install the probe software at a site, you must configure it to connect with Vantage DX Diagnostics. Complete this procedure for each installed Windows probe.

Before you Begin

- Ensure the probe software is already installed on a computer at the site.

1. Click **Manage** to access the Application Management page, then click **Sites**.
2. On the Site Management page, select the site you are configuring and generate the probe PIN by clicking **Generate PIN**.

> **Tip:** Make note of the Hostname and PIN displayed on this page.

3. From the Start Menu on the Windows computer where you installed the probe software, navigate to **Vantage DX Diagnostics > Vantage DX Diagnostics Config**.
   A command window appears.

Note: If you changed the name of the install directory during the installation, **Vantage DX Diagnostics Config** is found under that directory name instead.

4. In the command window, at the Vantage DX Diagnostics server FQDN prompt, type the **Hostname** and press **Enter**.
5. When prompted, type the PIN that you generated in step 1 and press **Enter**.
6. Once the Probe configuration successfully completes press **Enter** to exit the command window.
7. To confirm that probe is successfully installed go to the site configuration page in VDX Diagnostics and check that the Probe's status is now **Connected**.

Tip: You might need to reload the page in the browser to see the updated status.

Configure a Software Deployed Probe

After you install the probe software at a site, you must configure it to connect with Vantage DX Diagnostics. Complete this procedure for each probe that was installed via deployment software.

You must be an administrator in Vantage DX to perform the steps on the Vantage DX Diagnostics interface. You do not need to have administrator permissions on the computer where there probe software is installed.

Before you Begin

- Ensure the probe software is already installed on a computer at the site.

1. Click **Manage** to access the Application Management page, then click **Sites**.
2. On the Site Management page, select the site you are configuring and generate the probe PIN by clicking **Generate PIN**.

Tip: Make note of the Hostname and PIN displayed on this page.

3. On the computer where you installed the probe software, navigate to C:\Program Files\VantageDxDiagnostics\non-admin-probe-config.bat.
   Alternatively, you can enter “Non admin Vantage DX Diagnostics config” in the **Search** menu.
   A command window appears.

Note: If you changed the name of the install directory during the installation, **Vantage DX Diagnostics Config** is found under that directory name instead.

4. Execute the script and include the Hostname and PIN using the following format:

   ```
   .\non-admin-probe-config.bat <hostname> <pin>
   ```

   If you do not include the Hostname and PIN, the script will prompt you to enter them
5. After the script successfully completes, press Enter to exit the command window.
6. Wait up to 5 minutes for the probe configuration to complete.
7. To confirm that probe is successfully installed go to the site configuration page in VDX Diagnostics and check that the Probe's status is now **Connected**.

Tip: You might need to reload the page in the browser to see the updated status.

CHAPTER 8

Configure Synthetic Transactions

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

Task	Description
"Understanding Synthetic Transactions" on page 53	Review this information to understand the how Vantage DX Monitoring works.
"Install Robot Manager" on page 53	The Robot Manager is a Windows service. Install it on every machine where you plan to deploy robots.
"Edit Monitoring Credentials" on page 54	Edit the initial credentials that robots use to access workloads.
"Add Monitoring Credentials" on page 54	Configure additional credentials that robots can use to access workloads.
"Create Monitoring Configurations" on page 54	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 Robots" on page 55	Specify the applications that you want the robots to monitor at each site.
"Add Location Tags to Robots" on page 56	Configure location tags to display robots on a map in Power BI.
"Import the Power BI Template for Cloud Deployments" on page 56	Import the template if you want to be able to view performance metrics in Power BI.

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, to indicate the correct format. The following table lists the placeholders that Vantage DX Monitoring creates.

Table 2: User Credentials for Robots

Credential	Placeholder
Office 365 User	myusername@example.com
Exchange Mailbox Server Credential	domain\username
On-Premises User	myusername@example.com
Exchange Edge Server Credential	domain\username
Office 365 Echo User	myusername@example.com

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.

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.

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.

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 54

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.

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 Robots" on page 55

Assign Configurations to Robots

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

Before you Begin

- "Create Monitoring Configurations" on page 54
- 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 Robots" on page 56

Add Location Tags to Robots

Use this procedure to add a tag that indicates the location of your robots. Location tags allow you to easily identify the location of your robots. Tags are required for Power BI to display your robots on a map. If you are using Vantage DX Monitoring as part of the Vantage DX solution, location tags are needed to show location data in VDX Analytics dashboards.

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.

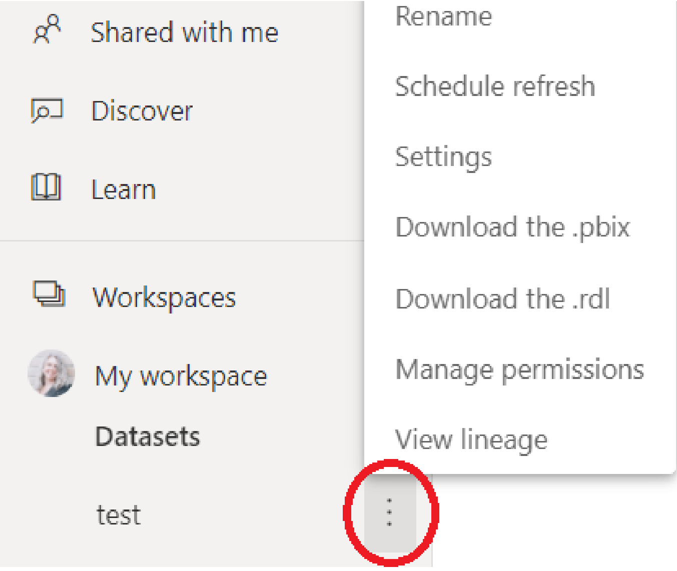
Before you Begin

- 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.

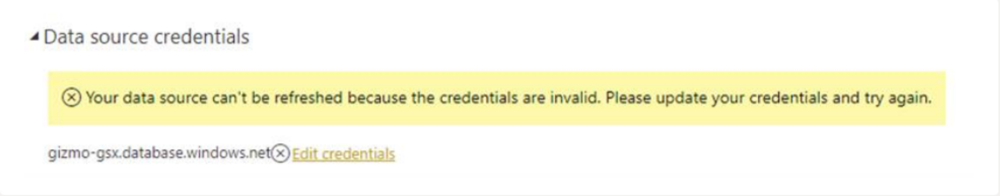
1. Double-click on the `Vantage DX Monitoring Report-<version>.pbit` file to launch load the Power BI template.
2. Provide the following information:
   - Server—The SQL server database that is listed in your Welcome email.
   - Database—The name of the database that is listed in your Welcome email.
   - 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**:



◢ Data source credentials

ⓧ Your data source can't be refreshed because the credentials are invalid. Please update your credentials and try again.

gizmo-gsx.database.windows.net ⓧ 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.

CHAPTER 9

Model Data and Manage Incidents

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

Task	Description
"Understanding Boards and Services" on page 61	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.
"Create a Board" on page 61	Organize objects from one or more monitoring systems. You can create boards that reflect your organizational structure.
"Create Sub-Boards" on page 62	Create sub-boards when you want to add child boards to a parent board.
"Create a Synced Board" on page 62	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 63	Create business services when you want to monitor critical services and report on the SLA of the service.
"Configure Rules" on page 65	Dynamically add objects to a board or business service using rules.
"Configure Exclusions" on page 66	Use exclusions in conjunction with rules to refine the scope of objects that are dynamically added to a board or business service.

Task	Description
"Assign an Email Address for Notifications" on page 66	Specify the email address that you want VDX Analytics to use for notifications.
"Configure Automatic Notifications" on page 66	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.
"Configure Incident Automation" on page 69	If you have integrated an ITSM system with VDX Analytics, you can automate the creation of incidents.

Understanding Boards and 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)

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 62 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 62.

Create a New Board

1. From the main menu, select **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. Click 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. From the main menu, select **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. Click the main menu and 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 63 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 64.

Create a New Business Service

1. From the main menu, select **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. Click 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 65
- "Create a Rule from an Existing Saved Search" on page 65

Create a New Rule

1. From the main menu, click **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. From 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.

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 Automatic Notifications

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 3: 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.
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 message 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 66

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 80 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.
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.

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 main 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.

CHAPTER 10

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 70	Configure the health states that you want to include in downtime calculations.
"Configure SLO for a Business Service" on page 71	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 72	View SLA performance data for a business service and generate a PDF report.
"Generate an SLA Availability Report for Multiple Business Services" on page 73	Generate a PDF report of the SLA performance data for multiple business services.
"Exclude Component Outages from SLA Calculations" on page 75	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 71.
- To see SLA performance, see "View and Save SLA Availability Data for a Business Service" on page 72.
- To generate an SLA performance report for multiple business services, see "Generate an SLA Availability Report for Multiple Business Services" on page 73

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 70.

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 **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 **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 SLA Availability 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 **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 70.

- To configure service level objectives, see "Configure SLO for a Business Service" on page 71.
- To exclude components and recalculate SLA information, see "Exclude Component Outages from SLA Calculations" on page 75.
- To view and save SLA data for a single business service, see "View and Save SLA Availability Data for a Business Service" on page 72.

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 **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 11

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 77	Create roles for the different types of users who will have access to VDX Analytics.
"Add Integrations to a Role" on page 77	Manage the integrations that can be viewed by users in different roles.
"Add Boards or Business Services to a Role" on page 78	Manage how users in different roles can access boards and business services.
"Add Dashboards to a Role" on page 78	Select the dashboards that users in each role can view.
"Scope Access" on page 79	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 79	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 the only integration you select is the Microsoft CQD integration for the customer's tenant.

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 77.

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.
   - **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 77.
- To manage the boards and business services that users can access, see "Add Boards or Business Services to a Role" on page 78.

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**
   - **Everyone**

CHAPTER 12

Integrate Additional Monitoring Tools

Follow the procedures in this section if you want to integration additional monitoring tools and ITSM systems with VDX Analytics. Complete the setup tasks listed in the following table.

Task	Description
"Install Remote Agents" on page 80	Install a remote agent so that your other monitoring tools can connect to the VDX Analytics web server.
"Add an Integration" on page 81	Integrate your monitoring 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**.

MARTELLO