VANTAGE DX

Quick Reference Guide

Requirements

1 Provide Details about your Environment

Provide the following information to Martello:

- What is the name of your Office 365 tenant? For example, `<tenant>.onmicrosoft.com`. If you know your Tenant ID, include that as well.
- Do you have specific Conditional Access Policies (CAP)?
- Do you use Azure AD Premium to provide AD Identity Protection?
- Do you use SSL packet inspection?

2 Set Up SSO with Azure AD

To use SSO, grant the Vantage DX application tenant-wide admin consent in the Azure portal. Sign into the following URL using an administrator account for the tenant. When you are prompted to grant permissions, click **Accept**.

https://login.microsoftonline.com/8d02b55e-eb6f-4a82-a33f-7cb2dba8f91c/adminconsent?client_id=0d75f118-91b7-4a02-8c52-25d8a1590a7c

Create groups in Azure AD to use for Service Administrators, Service Operators, and Read-Only users. Provide the Object ID of each group to Martello.

3 Set Up the Microsoft Call Quality Dashboard

Before you configure the integration with VDX Analytics, you must set up the Microsoft CQD and configure an Office 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).
- Multi-factor authentication is disabled.
- 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.

4 Prepare to Integrate Microsoft 365 Service Data

Before VDX Analytics can retrieve data about the health of your Microsoft 365 services, you must register the application in Azure Active Directory and grant the required permissions. Complete the steps in the following Knowledge Base article:

https://support.martellotech.com/knowledgeBase/15513875

Requirements

5 Verify Requirements for VDX Diagnostics

Firewall

- Port 443 is open
- ICMP is allowed for outbound and inbound communications:
- Inbound: Type: 0 (Echo Reply) and Type: 11 (TTL Exceeded)
- Outbound: Type: 8 (Echo Request)

You may need to configure additional firewall rules for inbound ICMP if you have configured NAT.

We recommend that you run the following connectivity tests in PowerShell to ensure connectivity before you install and configure the probes:

- Test-NetConnection -computername <company_name>.vantage-dx.com -port 443
- tracert world.tr.teams.microsoft.com
- ping <endpoint FQDN>

You must be able to access the following URL: https://<instancename>.vantage-dx.com/npv-ui

Machine

- Windows 10 (64-bit) operating system
- Minimum 2 GB RAM
- 70 MB disk space
- No need for a dedicated machine;

Client

- Chrome version 95 and later
- Firefox version 93 and later
- Edge version 95 and later
- Recommended screen resolution: 2560 x 1440 or higher.

6 Verify Requirements for VDX Monitoring

We recommend that you install the Robot Manager service on a machine that is as similar as possible to the machines used by your end users. This practice helps ensure that the performance data collected by the robots is realistic and reflects the experience of your end users. It also helps you determine if anything included in your standard deployment is impacting the performance of the service. The machine should be dedicated to the Robot Manager and not in use for other purposes.

Machine

- Windows 10 (64-bit) operating system
- Minimum 4 GB RAM; 8 GB or higher recommended
- 2.5 GHz Dual Core Processor; Teams Video may require additional CPU.
- PowerShell 4.0 or higher
- 4.7.1 .NET Framework
- Power settings: always on

Requirements

Network

Ensure that the machine where Robot Manager is installed can access all required Microsoft Office 365 URLs and IP addresses. For more information, see the following URL:

https://docs.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide

The machine where Robot Manager is installed must be able to:

- Access eager-swan.rmq.cloudamqp.com on port 5671 (TCP).
- Access Vantage DX on port 5671. It must have direct connectivity and must not use a proxy.
- Resolve *.vantage-dx.com
- Download from cbmtprod.z6.web.core.windows.net on port 443 (TCP)

The computer that you use to access VDX Monitoring must be able to access the following URL: https://*.vantage-dx.com/gizmo

Accounts

The Robot Manager service requires one or more user accounts that are dedicated to monitoring. The number of accounts you need depends on the workload that you are monitoring and the number of robots that you deploy. This Quick Reference Guide provides information for the Teams and Teams Advanced workloads. For other workloads, see the Accounts information in the *Vantage DX Cloud Deployment Guide*.

All accounts must have a valid Office 365 E3 or E5 license in order to monitor the workloads.

To avoid interruptions in data collection, ensure that you disable multi-factor authentication for these accounts, and do not set a password expiry.

Accounts for 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 and must belong to same tenant.
- The accounts must have permissions to create Microsoft 365 groups.

If you are monitoring Teams Advanced from multiple locations, use separate credentials for the robots at each location.

Requirements

7 Review Connection Requirements

The following diagram provides an overview of the settings required for Vantage DX to connect to your environment.