Quick Start Guide

Deployment Requirements

Use the information in this guide to verify that your environment meets the requirements to deploy Vantage DX.

Provide Details about your Environment

Provide the following information to Martello:

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

Grant Permissions to the VDX Application

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

Configure Groups for SSO

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

- Service Administrators
- Service Operators

Ensure that you choose Security as the group type. If you have existing groups with these names, you do not need to create new ones. Provide the Object ID of each group to Martello. For information about assigning groups to SaaS applications in Entra, see the following Microsoft documentation:

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

Deployment Requirements

Create Accounts

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

Module	Requirements
Vantage DX Analytics Integrations	

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

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

Deployment Requirements

Enable Network Connections

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

Protocol and Port	Endpoint / Destination	Description
HTTPS		
443	<instancename>.vantage-dx.com	Robot connection to Vantage DX
	https://extreme-ip-lookup.com/	Robot connection used for network diagnostics
ICMP		
Type 0	Inbound packets	Destination host unreachable; needed only if you are configuring network diagnostics with ICMP
Type 3	Inbound packets	TTL exceeded
Type 11	Inbound packets	Echo request
Type 8	Outbound packets	Echo reply; needed only if you are configuring network diagnostics with ICMP
TCP		
443 (AMPQS 5671 for installations prior to June 2023)	One of the following: • **Western European region:** eager-swan.rmq.cloudamqp.com • **Eastern United States region:** sharp-fuchsia-mongoose.rmq4.cloudamqp.com	Robot connection to Vantage DX

Deployment Requirements

Protocol and Port	Endpoint / Destination	Description
443	All required Microsoft Office 365 URLs and IP addresses. For more information, see the following website: https://docs.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide	Robot connection to Microsoft workloads
443	ecs.communication.azure.com	Robot connection to the Azure Communication Services (ACS) endpoint.
443	acsresource<your-tenant-name>.canada.communication.azure.com	Robot connection to the Azure Communication Services (ACS) endpoint.
443	20.202.0.0/16	Robot connection to a range of ACS public IP addresses. For more information, see the following website: https://learn.microsoft.com/en-us/azure/communication-services/concepts/voice-video-calling/network-requirements#firewall-configuration
UDP		
3478 to 3481	20.202.0.0/16	Robot connection to a range of ACS public IP addresses. For more information, see the following website: https://learn.microsoft.com/en-us/azure/communication-services/concepts/voice-video-calling/network-requirements#firewall-configuration

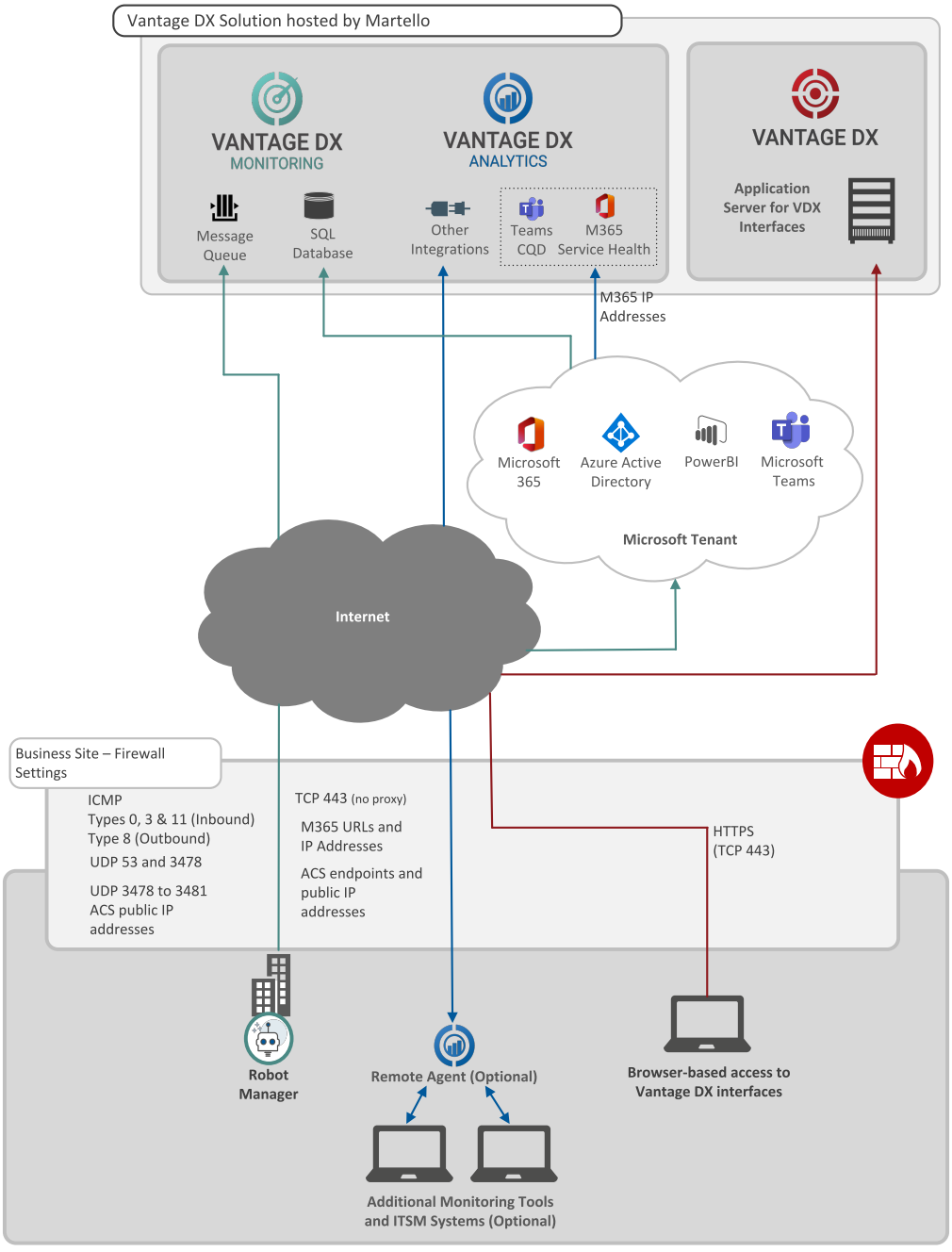
Deployment Requirements

Protocol and Port	Endpoint / Destination	Description
53	Custom endpoints for network diagnostics.	Robot connection when you configure network diagnostics using UDP Direct Mode. When you use UDP, ensure that your firewall also permits the inbound ICMP packets listed above.
3478	Teams endpoint for network diagnostics.	Robot connection when you configure network diagnostics to the Teams endpoint. When you use UDP, ensure that your firewall also permits the inbound ICMP packets listed above.

Connection Overview

The following diagram provides an overview of the ports and protocols required for Vantage DX.

Deployment Requirements



Machine Requirements

The machine where you deploy a Vantage DX Monitoring Robot Manager must meet the following minimum requirements:

- Windows 10 or higher (64-bit) operating system

- Power settings: always on
- In office locations, the machine should be dedicated for use with Vantage DX and not in use for other purposes.
- For remote users, the Robot Manager can be co-located with other applications.

Note:
Deploying a Robot Manager on the machine of a remote user is supported for network diagnostics only; it is not supported for synthetic transactions.

Verify Requirements

We recommend that you perform the tests listed in the following table to ensure that you have met the minimum system requirements.

Module	Description
Vantage DX Analytics	
Microsoft Call Quality Dashboard (CQD)	Use the Vantage DX Validation Tool to verify that the account for the integration with the Microsoft CQD meets the requirements: https://vdxvalidation.vantage-dx.com/ The Validation Tool also verifies that the Vantage DX application has the permissions it needs to integrate with your Microsoft tenant.
Vantage DX Monitoring	
Robot Manager	Run one of the following tests, depending on your location: **Western European region:** Invoke-WebRequest https://eager-swan.rmq.cloudamqp.com/ -UseBasicParsing **Eastern United States region:** Invoke-WebRequest https://sharp-fuchsia-mongoose.rmq4.cloudamqp.com/ -UseBasicParsing

Deployment Requirements

Module	Description
Robot Manager	On the machine where the Robot Manager Service is installed, run the following tests in PowerShell to ensure connectivity: • Test-NetConnection -ComputerName ecs.communication.azure.com -port 443 • Test-NetConnection -ComputerName 20.202.248.2 -port 443  **Note:** There is no easy method for testing whether your firewall allows the required UDP connections. We recommend that you submit a change request to you internal team to ensure that your firewall allows the required connections.