MARTELLO | *GSX* is a subsidiary of Martello Technologies

VANTAGE DX MONITORING

RELEASE NOTES

RELEASE 3.20

DOCUMENT DATE: FEBRUARY 19, 2025

NOTICE

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

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

Trademarks

MarWatch™, Savision, GSX, Martello Technologies, 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.

Release Notes
Release 3.20 - February 19, 2025

CHAPTER 1

CHAPTER 2

CHAPTER 3

Introduction

Vantage DX Monitoring is a monitoring tool that provides the information you need in order to understand service delivery issues on Microsoft applications and resources. It provides you with proactive alerts so that you can work directly on issues before they become a problem for your business.

Vantage DX Monitoring 3.20

The following sections provide a summary of the changes introduced in Vantage DX Monitoring Release 3.20, as well as any known issues.

- "New in this Release" on page 1
- "Known Issues" on page 1

New in this Release

This release includes the following changes and enhancements:

- "Updates to the Azure Active Directory Workload" on page 5
- "Updates to Authentication Methods" on page 5

Updates to the Azure Active Directory Workload

To prepare for upcoming changes in the Microsoft environment, the Azure Active Directory (AAD) workload in Vantage DX Monitoring has been updated with the following changes:

- The workload has been renamed to Microsoft Entra Connect.
- The configuration now requires your Microsoft Tenant ID.
- The configuration now uses your custom enterprise application for the permissions needed to perform tests and retrieve data. Ensure that your app provides the following Application permissions:
    - Group.Read.All—Read groups and their properties.
    - OrgContact.Read.All—Read organization contacts.
    - Users.Read.All—Read all users' profiles.

Updates to Authentication Methods

Due to changes in the Microsoft environment, Basic Authentication is no longer supported. The Basic Authentication option was previously available for the following workloads:

- Exchange Online
- Exchange Free/Busy

- Hybrid Mail Routing
- Internal Mail Routing
- Roundtrip Mail Routing
- SMTP Gateways

If you enabled Basic Authentication for any of these workloads, Vantage DX Monitoring cannot retrieve data. An alert is raised, with the message that "The Autodiscover service couldn't be located." To ensure continued monitoring of these workloads, please disable the setting. Vantage DX Monitoring will automatically switch to using Microsoft Authentication Library (MSAL) and data will be retrieved.

Fixed Issues

The following issues were fixed in this release.

Issue Type	Issue
Application	Vantage DX Monitoring displays a critical issue for the Round Trip Mail Routing workload, indicating that some email properties are missing and only a subset of the tests can be evaluated. This issue occurs if you are using Mimecast for email security.
Application	When you refresh a Vantage DX Monitoring dashboard, a blank page displays. This issue occurs in on-premises installations with SSO enabled.

Known Issues

The following items are known issues in this release of Vantage DX Monitoring:

- "Increased Requirements for Teams Video " on page 6
- "Custom Dashboard Status Card Errors for Office Subscriptions and Skype" on page 7

Increased Requirements for Teams Video

Due to changes in the Teams Video workload, there are increased requirements for the machine where the Robot Manager is installed. If the machine does not meet the requirements, some performance metrics may not be available. To avoid this issue, ensure that the machine where the Robot Manager is installed meets the requirements listed in the following table.

Table 1: Robot Manager Server—Requirements for Teams Video

Component	Minimum Requirement	Recommended
Browser	Google Chrome	The current version is recommended; two previous versions are supported.
Operating System	Windows 10	—
Memory	8 GB	8 GB or higher
Processors	4 vCPUs	4 or more vCPUs
PowerShell	4.0	4.0 or higher
.NET Framework	4.7.1	4.7.1 or higher
Power settings	Always On	—

Custom Dashboard Status Card Errors for Office Subscriptions and Skype

The Office Subscription and Skype for Business statuses are now obsolete and have been removed from the MS Service Health dashboard. However, any custom dashboards that were created prior to Release 2.4, which contain those obsolete statuses, will display an error on the health status cards.

Contact

For additional information, please visit our support page at
https://support.martellotech.com, or email our Support Team at vdx-
support@martellotech.com.

MARTELLO