



USER GUIDE

RELEASE 3.17

DOCUMENT DATE: JUNE 28, 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.

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.

© Copyright 2024, Martello Technologies Corporation
All rights reserved

User Guide
Release 3.17 - June 28, 2024

Contents

CHAPTER 1

| | |
|-------------------------|---|
| Introduction | 7 |
| Document Purpose | 7 |
| Intended Audience | 7 |
| Revision History | 7 |

CHAPTER 2

| | |
|-----------------------------------|----|
| About Vantage DX Monitoring | 8 |
| Components | 8 |
| VDX Monitoring Web UI | 8 |
| Robots | 9 |
| Workloads | 9 |
| Security | 11 |

CHAPTER 3

| | |
|--------------------------------|----|
| About the Interface | 12 |
| Dashboards | 12 |
| System Dashboards | 12 |
| Custom Dashboards | 13 |
| Dashboard Components | 13 |
| Status Cards | 14 |
| Graphs | 15 |
| Tables | 16 |
| Time Period | 16 |
| Settings | 16 |
| Credentials | 17 |
| Notification Systems | 17 |
| Configurations | 17 |
| Robots | 18 |
| Statuses & Notifications | 18 |
| Dashboards | 19 |
| Authentication | 19 |

CHAPTER 4

| | |
|--|----|
| Configure Workloads | 21 |
| Create Monitoring Configurations | 21 |

| | |
|---------------------------------------|----|
| Assign Configurations to Robots | 22 |
| Add Location Tags to Robots | 23 |

CHAPTER 5

| | |
|--|----|
| Configure Statuses and Alert Notifications | 24 |
| Configure Vantage DX Monitoring Alert Notification Systems | 25 |
| Apply Alert Notification Systems to Workloads | 28 |
| Apply Alert Notification Systems to Robots | 29 |
| Edit Performance Thresholds | 29 |
| Add a Filter to Robots for a Custom Status | 30 |
| Create a Custom Status | 30 |
| Apply Robot Filters to the Custom Status | 31 |

CHAPTER 6

| | |
|---|----|
| Configure Dashboards | 32 |
| Create a New Custom Dashboard | 32 |
| Create a Custom Dashboard from a System Dashboard | 33 |
| Enable or Disable Dashboards | 34 |

CHAPTER 7

| | |
|---|----|
| Power BI Reports | 36 |
| Share a Report Using Power BI Service | 36 |
| VDX Monitoring Power BI Report Pages | 37 |

CHAPTER 8

| | |
|-----------------------------------|----|
| Metrics Collected | 41 |
| Dashboard Metrics | 45 |
| AAD Connect | 46 |
| ADFS | 46 |
| Exchange | 47 |
| Exchange Advanced Free/Busy | 48 |
| Exchange DAG | 48 |
| Exchange Edge | 49 |
| Exchange Mailbox Servers | 50 |
| Exchange MAPI | 52 |
| Mail Routing | 53 |
| Mail Routing Hybrid | 54 |

| | |
|-----------------------------------|----|
| MS Service Health | 55 |
| Network | 56 |
| Office 365 Operations | 57 |
| OneDrive | 58 |
| Teams | 59 |
| Teams Advanced | 61 |
| URL | 63 |
| Power BI Metrics | 64 |
| Top Level Dashboard | 66 |
| Exchange UX | 67 |
| OneDrive and SharePoint UX | 68 |
| Teams Login | 69 |
| Teams for Export | 70 |
| Teams Voice | 70 |
| UX Analysis | 72 |
| Metric Analysis | 73 |
| Mail Routing | 76 |
| Cross Analysis | 76 |
| Exchange Server Performance | 77 |
| Exchange Advanced Free/Busy | 78 |
| Exchange MAPI UX | 78 |

CHAPTER 9

| | |
|--|----|
| Default Thresholds | 80 |
| ADFS Thresholds | 82 |
| Exchange Advanced Free/Busy Thresholds | 82 |
| Exchange Edge Thresholds | 83 |
| Exchange Mailbox Server Thresholds | 83 |
| Client Access Thresholds | 84 |
| Database Thresholds | 84 |
| Lagged Copies Thresholds | 85 |
| System Thresholds | 85 |
| Transport Thresholds | 87 |
| Exchange MAPI Thresholds | 88 |
| Microsoft Exchange Thresholds | 88 |
| Exchange OWA Thresholds | 90 |
| Hybrid Mail Routing Thresholds | 91 |
| Internal Mail Routing Thresholds | 92 |
| Office 365 Web App Thresholds | 92 |

| | |
|---|----|
| OneDrive Thresholds | 92 |
| Roundtrip Mail Routing Thresholds | 93 |
| SharePoint Page Thresholds | 94 |
| SMTP Gateways Thresholds | 94 |
| Teams Thresholds | 95 |
| Teams Advanced Thresholds | 95 |
| Teams Video Thresholds | 96 |
| URL Thresholds | 97 |

CHAPTER 10

| | |
|--|-----|
| Troubleshooting | 98 |
| Page Loading and Data Display Errors | 98 |
| Notification System Errors | 100 |
| Power BI Errors | 101 |

CHAPTER 11

| | |
|---------------|-----|
| Contact | 102 |
|---------------|-----|



Introduction

Document Purpose

This document provides information about how to use Vantage DX Monitoring to access real-time information in dashboards, manage alert notifications, understand metrics, and generate reports.

Intended Audience

This guide is intended for use by IT system administrators, IT managers, and help desk personnel.

Revision History

| Document Date | Description |
|---------------|--|
| June 28, 2024 | VDX Monitoring User Guide Release 3.17 |



About Vantage DX Monitoring

VDX Monitoring is a monitoring tool that provides the information you need in order to understand service delivery issues on Microsoft applications and resources. In Microsoft environments, these applications and resources are known collectively as workloads.

Robots located at your critical business sites perform synthetic transactions on workloads—such as Microsoft Exchange, SharePoint, OneDrive, and Teams—while also testing network conditions. These robots continuously test the user experience from where your users are located to help you understand the service quality that you are delivering to your sites and business lines.

Based on these tests, VDX Monitoring provides you with proactive alert notifications so that you can work directly on issues before they become a problem for your business.

Use the information in the following sections to understand the components that make up VDX Monitoring, as well as the security measures that VDX Monitoring uses:

- ["Components" on page 8](#)
- ["Security" on page 11](#)

Components

Use the information in the following sections to understand the components that make up VDX Monitoring:

- ["VDX Monitoring Web UI" on page 8](#)
- ["Robots" on page 9](#)
- ["Workloads" on page 9](#)

VDX Monitoring Web UI

The VDX Monitoring Web UI is an application that displays detailed dashboards, metrics, and alert notifications for the Microsoft workloads that you monitor. The data it provides helps you measure the experience of your end-users. You can use the VDX Monitoring Web UI to customize how workloads are monitored. For

example, you can choose which workloads to monitor, set performance thresholds, and configure how you receive alert notifications.

Robots

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 VDX Monitoring Web UI to configure the activities and workloads that the robots test.

You can add tags to robots for the following purposes:

- Add a location tag to easily identify where the robot is located. For workloads that display in Power BI reports, you must add location tags to view the robot data on the map included in the Power BI report.
- Add a filter tag to apply customized performance thresholds, as defined in a custom status.

Workloads

A workload is an application or a resource that you can monitor. VDX Monitoring allows you to create monitoring configurations for the following workloads:

- AAD Connect (Azure AD Connect)
- ADFS (Active Directory Federation Services)
- Exchange DAG
- Exchange Edge Server
- Exchange Free/Busy
- Exchange Mailbox Server
- Exchange MAPI
- Exchange Online
- Exchange Online Network
- Exchange OWA
- Hybrid Mail Routing
- Internal Mail Routing
- Office 365 Health, which includes the following applications (if enabled):
 - Azure Information Protection
 - Dynamics 365
 - Exchange Online
 - Identity Service
 - Microsoft Forms
 - Flow in Microsoft 365
 - Microsoft StaffHub
 - Microsoft Teams
 - Microsoft Intune

- Office Client Applications
- Office for the Web
- Planner
- PowerApps in Microsoft 365
- Mobile Device Management for Office 365
- Yammer Enterprise
- Office 365 Portal
- OneDrive for Business
- Power BI
- SharePoint Online
- Office 365 Web App, which includes the following applications (if enabled):
 - Azure AD Management
 - Azure Portal
 - Delve
 - Dynamics
 - Excel
 - Office 365 Admin Portal
 - OWA
 - Office365
 - Office Pro Plus Pages
 - OneDrive
 - OneNote
 - Planner
 - Power Apps
 - Power Automate
 - Power BI
 - SharePoint
 - Streams
- OneDrive
- Roundtrip Mail Routing
- SharePoint Network
- SharePoint Page
- SMTP Gateways
- Teams
- Teams Advanced
- Teams Network
- Teams Video
- URL

Security

When you configure robots in the VDX Monitoring Web UI, you provide credentials that the robots can use to log into various workloads and perform synthetic transactions. Passwords are stored on disk to persist after a system restart and are encrypted and decrypted on-demand using industry standard encryption.

All passwords are kept in memory, and are encrypted and decrypted on-demand.

VDX Monitoring does not store Personally Identifiable Information (PII). It does store the following data:

- Results from synthetic transactions; these results typically include a date, a unique identifier, a statistic identifier, and a value.
- Service accounts—if you have configured them—for accessing monitored servers or third-party systems that VDX Monitoring integrates with.
- Fully qualified domain names (FQDN) for each of the installed Robot Managers.

All stored data is encrypted using AES-256.



About the Interface

The VDX Monitoring user interface provides you with the information you need when service delivery issues occur on your monitored workloads. This information is available through detailed dashboards, which provide performance metrics and health status information. You can use the interface to customize how workloads are monitored by setting thresholds for the performance metrics.

Additionally, VDX Monitoring can send alert notifications based on performance thresholds. You can choose how you want to receive alert notifications, and who should receive those notifications.

The menu options that are available in VDX Monitoring depend on the permissions assigned to you by your administrator. This document describes features that may not be available to all users.

The following sections describe each of the menu options and the functionality they provide:

- ["Dashboards" on page 12](#)
- ["Settings" on page 16](#)
- ["Authentication" on page 19](#)

Dashboards

Dashboards provide detailed information about performance metrics and statuses that allow you to monitor the health of workloads and the various processes associated with the workloads.

Two types of dashboards are available in VDX Monitoring:

- ["System Dashboards" on page 12](#)
- ["Custom Dashboards" on page 13](#)

System Dashboards

System dashboards are dashboards that are available by default in the VDX Monitoring Web UI. You cannot delete or rename a system dashboard; however, you

can duplicate a system dashboard and edit it to create a custom dashboard. You can also disable system dashboards. The system dashboards are:

- AAD Connect
- ADFS
- Exchange
- Exchange Advanced Free/Busy
- Exchange DAG
- Exchange Edge
- Exchange Mailbox Servers
- Exchange MAPI
- MS Service Health
- Mail Routing
- Mail Routing Hybrid
- Network
- Office 365 Operations
- OneDrive
- Teams
- Teams Advanced
- URL

Custom Dashboards

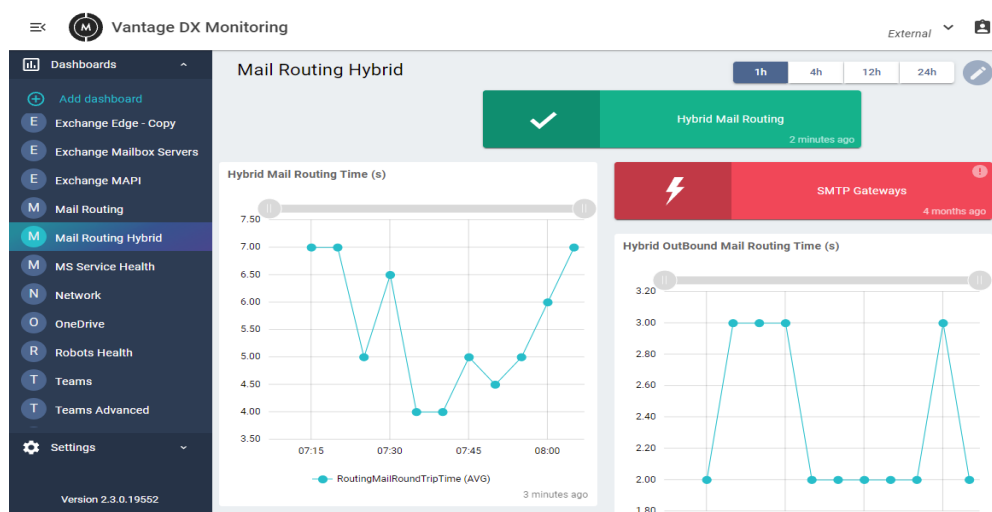
You can create a custom dashboard so that VDX Monitoring best fits your needs. You can create a new blank custom dashboard from scratch, or you can duplicate a system dashboard to create an editable copy. You can perform the following actions on a custom dashboard:

- Add or remove dashboard components.
- Resize and move dashboard components.
- Customize the dashboard name.

Dashboard Components

The components that display on a dashboard depend on the workload being monitored.

The following image shows an example of a dashboard with its different components.

Figure 1: Dashboard Example—Exchange

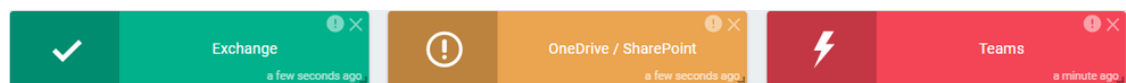
The following types of data are displayed within a dashboard:

- "Status Cards" on page 14
- "Graphs" on page 15
- "Tables" on page 16
- "Time Period" on page 16

Status Cards

Status cards provide a visual indication about the current health of workloads, based on the tests that robots perform. Status cards are colour-coded to provide a real-time indication about the health status of a particular workload.



The following image shows the different statuses that a workload can have.

Figure 2: Status Examples

Each status is indicated by one of the following colors:

- **Green**—The robots perform the tests successfully and the results are better than the performance threshold.
- **Orange**—Warning. The tests have breached the performance threshold but have not reached the critical threshold.
- **Red**—The critical threshold has been reached. This status indicates a possible outage.

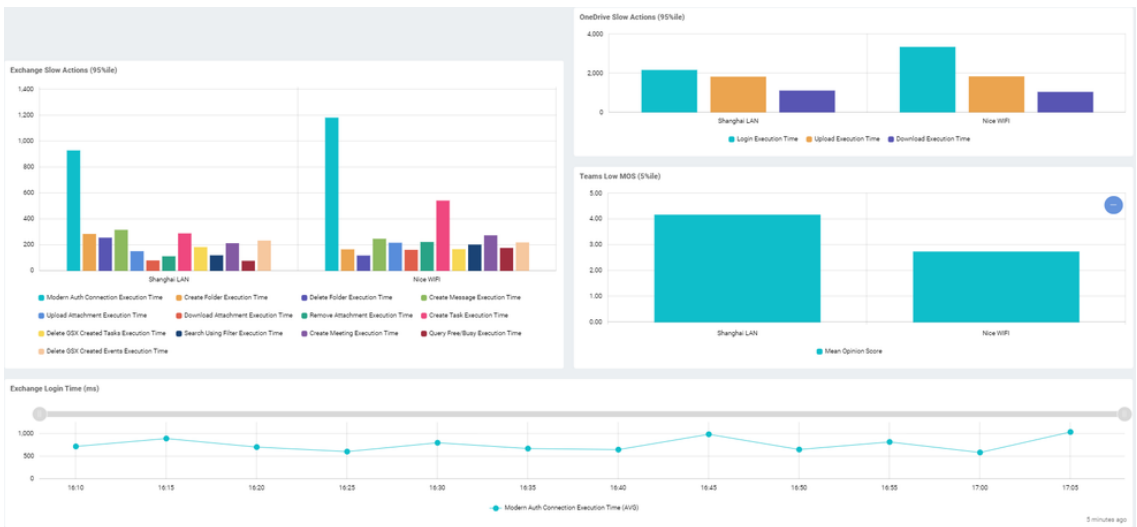
The following functions are available within a status card:

| Button | Function | Description |
|---|-------------------|--|
|  | View details | This button shows information about the status in a pop-up window. |
|  | Copy to clipboard | This button allows you to copy the detailed status information to the clipboard. |

Graphs

The following image shows several types of graphs displayed in a dashboard.

Figure 3: Graphs Example



The number of graphs, the data in the graphs, and the graph types vary, depending on the selected dashboard. Not all dashboards have graphical data to display.

The dashboard displays up to 12 Robot Managers per graph, prioritizing those with the most critical status.

VDX Monitoring aggregates data in each graph for up to five minutes.

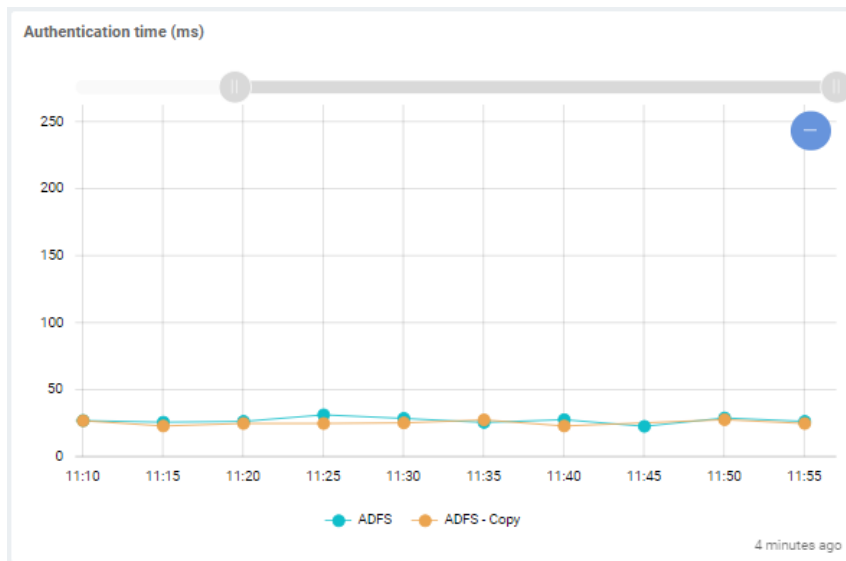
The types of graphs displayed include:

- **Line graphs**—Illustrate trends in data over a period of time.
- **Bar graphs**—Compare numbers across categories.
- **Gauge graphs**—Display the value of a key indicator against the colored data range or chart axis.
- **Pie chart graphs**—Show a percentage or proportional data represented by a category.

Within a line graph you can zoom in and out on a time period using the slider bar at the top of the graph. You can also use the mouse to draw a selection area on the graph to zoom into a specific time period. Doing so changes the view of the data in all of the graphs and tables in the dashboard to the selected time period.

The following image shows a slider bar at the top of a graph.

Figure 4: Graph Slider Bar



You can click on an item in the graph legend to enable or disable the specific metric in the graph. When a metric is disabled in the graph, it also appears in grayed-out in the legend. Click it again to enable it.

Tables

The number of tables, and the data displayed within each table, varies depending on the selected dashboard. Not all dashboards have data to display in tables.

Time Period

The Time Period selector allows you to display the data in 1 hour, 4 hour, 12 hour, and 24 hour increments. For example, select 12h to display the data from the last 12 hours.

Dashboard data is refreshed every five minutes.



Note: Status information is always based on the real-time status, even when you select a different time period.

Settings

The Settings menu is available from the left navigation pane and contains the following options:

- ["Credentials" on page 17](#)
- ["Notification Systems" on page 17](#)
- ["Configurations" on page 17](#)

- ["Robots" on page 18](#)
- ["Statuses & Notifications" on page 18](#)
- ["Dashboards" on page 19](#)

Credentials

The Credentials page is where you configure the credentials that robots can use to log into workloads and perform tests.

During the installation process, a list of credentials is created by default and displayed on the Credentials page. These default credentials are placeholders that indicate the correct format to use for each workload. You can edit these placeholders to set up your initial monitoring credentials and add more if needed. If you need to remove credentials, contact vdx-support@martellotech.com.

These credentials are configured by your administrator as part of the installation process. If you need to configure additional credentials, refer to the *VDX Monitoring Installation Guide—On-Premises Deployments* and the *VDX Monitoring Installation Guide Cloud Deployment Guide*, available on the Martello website at the following URL:

<https://martellotech.com/documentation/monitoring/>

Notification Systems

The Notification systems page allows you to specify the notification method that you want VDX Monitoring to use when it sends an alert notification, and who should receive the notification. For example, you can choose to have notifications delivered by email, recorded in an event log, recorded in ServiceNow, or in another application using a webhook.

During the installation process, a list of notification systems is created by default and displayed on the Notification systems page. These default notification systems are placeholders that you need to edit.

Configurations

The Configurations Management page allows you to create monitoring configurations for the workloads that VDX Monitoring supports. Use this page to choose the workloads that you want to monitor and configure their parameters. Parameters include information such as credentials, addresses, port numbers, and other information specific to your network.

From the Configurations Management page you can perform the following actions:

- Add a configuration.
- Edit a configuration.
- Duplicate a configuration.
- Remove a configuration.

Robots

The Robots management page displays all the installed Robot Managers with the following information for each robot:

- The Robot Manager name and the machine where it is installed.
- Any location tags or filter tags that have been added.
- The configured workloads.
- The enabled or disabled notifications.
- The notification systems.

VDX Monitoring displays up to 25 Robot Managers per page. If you have more than 25 Robot Managers, use the previous and next buttons to navigate through the pages.

From the Robots management page you can perform the following actions:

- Select the workloads for each Robot Manager to monitor.
- Manage notification systems for each Robot Manager.
- Manage location and filter tags for each Robot Manager.
- Activate and deactivate notifications for each Robot Manager.

Statuses & Notifications

Statuses provide a real-time visual indication about the current health of workloads by displaying color-coded health status cards on dashboards. The health of the workload is based on the tests that robots perform on that workload. Status notifications are tied to statuses and are triggered when a potentially negative service-affecting change to a health status is detected.

The Statuses & Notifications page lists the available statuses and allows you to perform the following actions:

- Show or hide health status cards on dashboards.
- Enable or disable alert notifications for the status.
- Define which notification system to use for alert notifications, if enabled.
- Configure system-wide default performance thresholds for a status.
- Duplicate a system status to create a custom status

The health status of a workload is based on the tests that the robots perform. When you enable the status of a workload, the dashboard for the workload includes a status card that uses the following colors to indicate the health of the workload:

- **Green**—The robots complete the tests successfully and the results are better than the performance threshold.
- **Orange**—Warning. The robots complete the tests. The test results breach the performance threshold but do not breach the critical threshold.
- **Red**—The critical threshold has been breached. This status indicates a possible outage.

Like the status information, the alert notifications are based on the tests that the robots perform. For example, VDX Monitoring raises a notification if a connectivity test fails, or if a security certificate has expired.

When you enable an alert notification for a workload, VDX Monitoring sends a notification if the threshold is breached. For example, a Teams notification can be triggered for a low MOS score or for a delay in logging in.

Statuses that are based on performance metrics have performance thresholds that determine the current health state of the status, based on robot tests. These thresholds are set to default values that are based on industry standards. Some workload tests have configurable thresholds. For a list of the configurable thresholds for each workload, see "[Default Thresholds](#)" on page 80.

Dashboards

The Dashboards management page displays all of the dashboards available in the application. The dashboards must be set to Active on this page before you can access them from the Dashboards list.

From the Dashboards management page you can do the following:

- Activate or deactivate dashboards.
- Duplicate a dashboard to create a custom dashboard.
- Remove a custom dashboard.



Tip: System dashboards display a lock icon in the Name column, indicating that you cannot edit system dashboards. Custom dashboards can be edited, and do not display a lock icon.

Authentication

The VDX Monitoring Web UI provides an Authentication menu for customers who are using VDX Monitoring in a standalone deployment with Windows authentication.

You can access the Authentication menu from the icon in the top right corner of the interface. This page allows you to configure the following authentication features:

- **SSO**—Single Sign-On activation
- **RBAC**—Role-Based Access Control activation

Authentication credentials are configured by your administrator as part of the installation process. For more information, refer to the *VDX Monitoring Installation Guide—On-Premises Deployments* or the *VDX Monitoring Cloud Deployment Guide*, available on the Martello website at the following URL:

<https://martellotech.com/documentation/monitoring/>

**Tip:**

VDX Monitoring is now available as part of the Martello Vantage DX solution. The Vantage DX solution has a portal that provides single sign-on capabilities for all of the Vantage DX modules. If you are using VDX Monitoring as part of the Vantage DX solution, you must configure user authentication in the Vantage DX portal. For more information, see the *Vantage DX Deployment Guide*. It is available on the Martello website at:

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



Configure Workloads

Complete the tasks in the following table.

| Task | Description |
|---|---|
| "Create Monitoring Configurations" on page 21 | For each workload that you want to monitor, create a configuration that specifies the parameters for your environment. Parameters include information such as credentials, addresses, port numbers, and other information specific to your network. |
| "Assign Configurations to Robots" on page 22 | Specify the applications that you want the robots to monitor at each site. |
| "Add Location Tags to Robots" on page 23 | Configure location tags to display robots on a map in Power BI. |

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 22](#)

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 21](#)
- 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 23](#)

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 VDX Monitoring as part of the Vantage DX solution, location tags are needed to show location data in Vantage DX 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**.

Configure Statuses and Alert Notifications

VDX Monitoring provides you with performance metrics and health status information on dashboards, and proactive alert notifications so that you can work directly on issues before they become a problem for your business.

For alert notifications, administrators can choose who receives the notifications and how they are notified.

Performance-based health status information and alert notifications are based on default performance thresholds, but some workloads allow you to configure the thresholds to suit your business needs. You can change configurable thresholds for all robots that monitor a workload, or you can create custom statuses and notifications with customized thresholds and apply them to specific robots. For more details about thresholds, see ["Default Thresholds" on page 80](#).

Use the information in this section to configure alert notifications, to change default workload performance thresholds, and to create a custom status and apply it to specific robots.

| Task | Description |
|---|--|
| "Configure Vantage DX Monitoring Alert Notification Systems" on page 25 | Use this procedure to configure how VDX Monitoring sends alert notifications. You can configure multiple notification systems. |
| "Apply Alert Notification Systems to Workloads" on page 28 | Use this procedure to specify which notification systems your various workloads use. |
| "Apply Alert Notification Systems to Robots" on page 29 | Use this procedure to specify which notification systems your individual robots use. You can specify multiple notification systems for each robot. |

| Task | Description |
|---|--|
| "Edit Performance Thresholds" on page 29 | Use this procedure to edit the performance thresholds that trigger health status card changes or alert notifications for a workload. |
| "Add a Filter to Robots for a Custom Status" on page 30 | Add a status and notification filter tag to one or more robots. These are the robots that will use a custom status that you create. |
| "Create a Custom Status" on page 30 | Use this procedure to duplicate and edit a system workload status to create a custom status for the same workload. |
| "Apply Robot Filters to the Custom Status" on page 31 | Associate the custom status with all robots with the status and notification filter tag that you previously applied. |

Configure Vantage DX Monitoring Alert Notification Systems

VDX Monitoring notification systems specify how to send alert notifications, and who to send the notifications to. VDX Monitoring provides default notification systems that you can edit to help you get started, and you can also configure your own notification systems. You can configure multiple notification systems. After you configure all of the notification systems you need for your business, you can apply them to specific robots and specific workloads as needed.



Note: Do not remove the default notification systems. Doing so may cause issues when you upgrade the VDX Monitoring application.

Before you Begin

Ensure you have information about how to access the notification system. Settings vary depending on the notification system type. For example, you may need login, password and addresses of the notification recipients.

1. Select **Settings > Notification systems** and click the **Add** button.
2. From the **Add a new notification system** panel, select the type of notification system to use, then click **Next**.
 - **Email - EWS**—Select this option if you use an EWS email. Ensure that you use a dedicated email account for this option. Using an account that is also used for other purposes may cause errors.

- **Email - SMTP**—Select this option if you use an SMTP email. This connector does not support anonymous or non-secured SMTP.
- **Event Log**—Select this option if you need to capture notification information in Windows Event Log.
- **ServiceNow**—Select this option to manage your incidents directly in the ServiceNow Incident table and take actions to solve issues.
- **Webhook**—Select this option to manage your incidents or automated tasks with other applications or services. You can use MS Power Automate to create a webhook and then trigger a notification based on a Power Automate rule. For information, see the following article in our Knowledge Base: <https://help.gizmo.gsx.com/knowledge-base/how-to/how-to-configure-a-webhook-with-ms-power-automate/>.

3. Provide the settings for the selected notification system type, then click **Next**.

| Notification System Type | Settings |
|--------------------------|---|
| Email - EWS | <ul style="list-style-type: none"> • Login—The login for the dedicated account (user@domain.com). • Password—The password associated with the account. • Recipients—Provide the email addresses of the notification recipients. You must provide at least one recipient. • OrgType—Select the organization type from the available options in the drop-down list. |

| Notification System Type | Settings |
|--------------------------|--|
| Email-SMTP | <ul style="list-style-type: none"> • Server—Provide the server name to use for sending messages. • Port—Specify the port number to use. • User—Provide the user name or email address for the account login. • Password—Provide the password associated with the account. • Sender—Provide an email address as follows: <ul style="list-style-type: none"> • If you entered only a user name in the User field, provide an email address for the notification sender. • Optionally, if you entered an email address in the User field but want to use a different email address for the notification sender, provide the email address. In most cases, this email address should be the address associated with the account user name and password. • If you entered an email address in the User field and want to use that address for the notification sender, leave blank. • Recipients—Provide the email addresses of the notification recipients. You must provide at least one recipient. |
| Event Log | <ul style="list-style-type: none"> • Level—Select the event log level from the available options in the drop-down list. • ID—Provide an ID. |
| ServiceNow | <ul style="list-style-type: none"> • Username—The login account for the ServiceNow instance. • Password—The password for the ServiceNow instance. • Base Url—The base URL for the ServiceNow instance. • Use Proxy—Select if needed, and provide the following: <ul style="list-style-type: none"> • Proxy Address—The address for the proxy. • Proxy Login—The login for the proxy. • Proxy Password—The password for the proxy. |
| Webhook | <ul style="list-style-type: none"> • URL—Fill in the URL to communicate with the service to use with Webhook. |

4. Provide a name for the notification system, then click **Add**.
The page displays the new notification system in the list.
5. If you need to edit a notification system:
 - Click the **Actions** button for the notification system that you want to edit.
 - Click **Edit**.
 - Edit the settings.
 - Click **Save** to confirm your changes.

Next Steps

After you configure the notification systems for VDX Monitoring, perform the following tasks:

- ["Apply Alert Notification Systems to Workloads" on page 28](#)
- ["Apply Alert Notification Systems to Robots" on page 29](#).

Apply Alert Notification Systems to Workloads

Use this procedure to add or change the notification systems associated with workloads.

Before you Begin

You must have configured at least one notification system for VDX Monitoring. See ["Configure Vantage DX Monitoring Alert Notification Systems" on page 25](#).

1. Select **Settings > Statuses & Notifications** and select the workload that you want to receive notifications about. You can select several workloads at once.
2. Click the **Set Notification Systems** button.
The Set Notification Systems panel appears.



Tip: You can also access the Set Notification Systems panel from the Actions menu for each status.

3. From the drop-down list, select the notification system to add to the status.
You can add multiple notification systems if required.
4. Click **Add**.
The added notification systems appear in the dedicated Notification Systems column.



Tip: To remove a notification system from the status, click the **X** icon in the notification system label.

Apply Alert Notification Systems to Robots

Use this procedure to specify which notification systems your robots will use to deliver alert notifications about the workloads those robots monitor. You can add multiple notification systems to robots for multiple workloads.

Before you Begin

You must have configured at least one notification system for VDX Monitoring. See ["Configure Vantage DX Monitoring Alert Notification Systems" on page 25](#).

1. Select **Settings > Robots** and select the Robot Manager you want to configure. You can select several Robot Managers at once or use the **Select all in page** option to select all the Robot Managers displayed on the current page.
2. Click the **Set Notification Systems** button.
The Set notification systems panel opens.
3. Select the notification systems to add from the drop-down list. You can add as many notification systems as you need.
4. Click the **Set Notification Systems** button to confirm.
The added notification systems appear in the dedicated Notification Systems column.



Tip: To remove a notification system from the Robot Manager, click the **X** icon in the notification system label.

Edit Performance Thresholds

VDX Monitoring performance-based health statuses and alert notifications are based on default performance thresholds. The thresholds are based on industry standards but you can edit some workload thresholds, depending on your needs and your environment.

Use this procedure to change the performance thresholds for a workload.

For a list of configurable thresholds and their default values, see ["Default Thresholds" on page 80](#).

1. Select **Settings > Statuses & Notifications**.
2. In the **Status Name** column, click the **Actions** button for the workload you want to edit.
3. Click **Edit Status**.
The Edit Status panel opens.
4. Edit the thresholds for the workload as required.
5. Click **Save** to confirm your changes.

Add a Filter to Robots for a Custom Status

Use this procedure to add a filter tag to robots. After you add the tag to your robots, you will create a custom status, and apply the same tag to that custom status to create an association between the required robots and the custom status. Ensure that you add the same filter tag to each robot.

1. Select **Settings > Robots** and select the Robot Manager that you want to configure.
You can select several Robot Managers at once. Use 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, enter a category for this filter.
4. In the **Value** field, enter the value or select from a list of existing tags.
5. Click the **+** button to confirm the tag and then click **Add**.

Next Steps

- Create a custom status. See ["Create a Custom Status" on page 30](#)

Create a Custom Status

Use this procedure to create a custom status (and the associated alert notifications) by duplicating an existing status and editing its details. This procedure includes multiple tasks to associate the custom status to the robots that will use it.

Before you Begin

- Add a filter tag to each robot that will use this custom status.

To create a custom status, complete the following steps:

1. Select **Settings > Statuses & Notifications**.
2. In the **Status Name** column, click the **Actions** button for the workload you want to edit.
3. Click **Duplicate**.
VDX Monitoring duplicates the workload in the Status Name column and displays it at the bottom of the list. The word "-Copy" is appended to the status.
4. Edit the workload as required by clicking the **Actions** button and selecting **Edit Status**. You can:
 - Change the name of the status.
 - Edit the notification system.
 - Edit the performance thresholds. See ["Edit Performance Thresholds" on page 29](#)
 - Apply the robot filter tag to your custom status. See ["Apply Robot Filters to the Custom Status" on page 31](#)
5. Click **Save** to confirm your changes.

6. Make the custom status available to be used in custom dashboards by toggling the **Enable Status** option to **On**.
7. To activate alert notifications related to the status, click the **bell** icon.

Apply Robot Filters to the Custom Status

Use this procedure to complete the association between the robots and the custom status. When this procedure is completed, the custom status is used by all robots that share the same filter tag with this custom status.

Before you Begin

- Add a tag to use as a filter for each robot that will use the custom status. See ["Add a Filter to Robots for a Custom Status" on page 30](#)
- Create a custom status by duplicating an existing status. See ["Create a Custom Status" on page 30](#).
- Edit the custom status performance thresholds. See ["Edit Performance Thresholds" on page 29](#).

1. Select **Settings > Statuses & Notifications** and click the **Actions** button for the workload to which you want to apply the filter.
2. Click **Edit Status**.
The Edit Status panel opens.
3. In the **Status Filters** section, add the tag you created for the robots by selecting the tag Key and Value from the drop-down lists.
4. Click the **+** button to add the tag.
5. Click **Save**.
The tag now appears in the filter column for the custom status.
6. Repeat these steps if you need additional filters.

Next Steps

- Add the custom status to a custom dashboard. See ["Create a New Custom Dashboard" on page 32](#).



Configure Dashboards

VDX Monitoring provides default dashboards, called system dashboards, which correspond to the applications that VDX Monitoring monitors. These dashboards are indicated by a lock icon on the Web UI. You cannot edit or delete system dashboards; however, you can create custom dashboards.

Use the information in this section to create custom dashboards:

| Task | Description |
|--|--|
| "Create a New Custom Dashboard" on page 32 | Create your own custom dashboards from a blank page. |
| "Create a Custom Dashboard from a System Dashboard" on page 33 | Create a custom dashboard that is based on a system dashboard. |
| "Enable or Disable Dashboards " on page 34 | Specify whether a dashboard is visible in the Dashboards list. |

Create a New Custom Dashboard

Use this procedure to create a custom dashboard.

1. Expand the **Dashboards** list and click **Add dashboard**.
2. Click the **Edit** icon.
3. Click the **Edit** icon next to the name of the dashboard and enter a new name. Click the **check mark** icon to save it.
4. Click the **Add** icon to select the type of component you want to add and click **Next**. The options are:
 - Line chart
 - Bar chart
 - Status
 - Table
 - Gauge
 - Pie Chart

5. Enter the settings for the component and click **Add**. The settings vary depending on the type of component you are adding.
 - Title—Enter the name of the component to display on the dashboard.
 - View name—Select the performance metric that you want to display.
 - Status—Select the application or infrastructure component that you want to display the health status for.
6. Click **Save**.

**Tip:**

You can resize components, move them, or delete them.

To resize a component:

- Hover the mouse over the bottom right corner of the component until the cursor changes to a diagonal arrow.
- Click and drag the corner of the component to resize it horizontally, vertically, or diagonally to best display the data in the component.

To move a component:

- Hover the mouse over the top of the component until the cursor changes to a hand.
- Click and drag the component to the desired position on the layout.

To remove a component, click the **x** icon in the top right corner.

Create a Custom Dashboard from a System Dashboard

Use this procedure to create a custom dashboard that is based on a system dashboard.

1. From the navigation panel, select **Settings > Dashboards**.
2. Click the **Actions** icon for the dashboard that you want to copy and click **Duplicate**.
3. Activate the dashboard by toggling the **Active** option to on (green). After you activate the dashboard, it displays in alphabetical order in the Dashboards list. The word "-Copy" is appended to the dashboard name.
4. In the navigation panel, click **Dashboards** to expand the Dashboards list. This option is located above the **Settings** menu.
5. Select the dashboard that you copied and click the **Edit** icon.
6. Click the **Edit** icon next to the name of the dashboard and enter a new name. Click the **check mark** icon to save it.

7. Click the **Add** icon to select the type of component you want to add and click **Next**. The options are:
 - Line chart
 - Bar chart
 - Status
 - Table
 - Gauge
 - Pie Chart
8. Enter the settings for the component and click **Add**. The settings vary depending on the type of component you are adding.
 - Title—Enter the name of the component to display on the dashboard.
 - View name—Select the performance metric that you want to display.
 - Status—Select the application or infrastructure component that you want to display the health status for.
9. Click **Save**.

**Tip:**

You can resize components, move them, or delete them.

To resize a component:

- Hover the mouse over the bottom right corner of the component until the cursor changes to a diagonal arrow.
- Click and drag the corner of the component to resize it horizontally, vertically, or diagonally to best display the data in the component.

To move a component:

- Hover the mouse over the top of the component until the cursor changes to a hand.
- Click and drag the component to the desired position on the layout.

To remove a component, click the **x** icon in the top right corner.

Enable or Disable Dashboards

When a dashboard is active, it is available to view in the dashboards list. If you do not want a dashboard to be visible in the dashboards list, disable the dashboard.

Use this procedure to enable or disable a dashboard:

1. From the navigation panel, select **Settings > Dashboards**.

2. Toggle the **Active** button for the dashboard to **on** (green) or **off** (gray).



Power BI Reports

VDX Monitoring data can be viewed and shared as a Power BI report. Your administrator imports your data into the VDX Monitoring Power BI template and publishes the data as a report to a workspace using the Power BI Service. To view the report, you need the following:

- A Power BI license.
- The link to the published report provided by your administrator.

If you have a Power BI Pro license, you can share a report with others.

Use the information in this section to share Power BI reports, and to understand the types of data that the report contains:

| Task | Description |
|--|---|
| "Share a Report Using Power BI Service" on page 36 | Share a report by email, or to embed the report in SharePoint or to a website or portal. |
| "VDX Monitoring Power BI Report Pages" on page 37 | This section provides an overview of the pages that are available in the Power BI report. |

Share a Report Using Power BI Service

You can publish reports and dashboards created in Power BI Desktop directly to a workspace using Power BI Service. If you have a free Power BI account, you can publish a report to your own workspace. If you have a Power BI Pro license, you can share a report with others.

Before you Begin

To publish and share reports you must have:

- A workspace created in Power BI. See <https://docs.microsoft.com/en-us/power-bi/collaborate-share/service-create-the-new-workspaces>.
- A Power BI license or a Power BI Pro license.

1. In Power BI Desktop, open the VDX Monitoring report template.
2. From Power BI Desktop Home menu, click **Publish**.
3. Save the report when prompted.
4. Supply your Power BI credentials if prompted.
5. On the **Publish to Power BI** page, click the workspace where you want to share the report, then click **Select**.
6. After the report is generated, click the link to open the report in Power BI. Power BI opens in a browser window and the report is displayed.
7. Click **Share** to send the report by email, or to embed the report in SharePoint or to a website or portal.


Tip:

To ensure that the data in your Power BI report is refreshed regularly, use the scheduling feature described in the following article:

<https://docs.microsoft.com/en-us/power-bi/connect-data/refresh-scheduled-refresh>

We recommend that you schedule a daily backup, before business hours.

VDX Monitoring Power BI Report Pages

The following table lists the pages that are available in the Power BI report.

Table 1: Power BI Reports

| Report Page | Description |
|---------------------|---|
| Top Level Dashboard | <p>An at-a-glance view of overall performance for the monitored workloads by robot location.</p> <p>For detailed information about the metrics displayed on this page, see "Top Level Dashboard" on page 66</p> |
| Exchange UX | <p>An overview of the Exchange end user experience by location. The panels in this report page display information about user actions within Exchange.</p> <p>For detailed information about the metrics displayed on this page, see "Exchange UX" on page 67</p> |

| Report Page | Description |
|------------------------|---|
| OneDrive/SharePoint UX | <p>An overview of the SharePoint and OneDrive end user experience by location. The panels in this report page display information about user actions within SharePoint and OneDrive, such as the time it takes to log in, upload and download a file, and total execution time.</p> <p>For detailed information about the metrics displayed on this page, see "OneDrive and SharePoint UX" on page 68</p> |
| Teams Voice | <p>An overview of the Teams voice call end user experience by location. Robots place 15 second calls every five minutes to determine the mean opinion score (MOS) at each location where Teams is installed.</p> <p>For detailed information about the metrics displayed on this page, see "Teams Voice" on page 70</p> |
| Teams Login | <p>An overview of the Teams end user authentication experience by location. Various metrics related to user login are displayed, including connection time, OAuth time, AuthZ time, endpoint discovery, and property time.</p> <p>For detailed information about the metrics displayed on this page, see "Teams Login" on page 69</p> |
| Teams (for export) | <p>Detailed call data in tabular format that you can export to share with your networking team for further analysis of call performance. You can also filter this data by MOS score and location. For example, you can filter by MOS to display all calls that had a MOS of three or less at a specific robot location.</p> <p>For detailed information about the metrics displayed on this page, see "Teams for Export" on page 70</p> |
| UX Analysis | <p>An overview analysis of the end user performance issues according to service type and location. Key metrics for each service type are tracked where poor performance is experienced. A table lists the top 100 issues encountered.</p> <p>For detailed information about the metrics displayed on this page, see "UX Analysis" on page 72</p> |

| Report Page | Description |
|-----------------------------|--|
| Metric Analysis | <p>An overview of the health for each service type. This report displays the performance of key metrics collected for each of the service types.</p> <p>For detailed information about the metrics displayed on this page, see "Metric Analysis" on page 73.</p> |
| Mail Routing | <p>An overview of the time it takes, along with the average number of hops, to send an email. Two mail routing configurations are supported by default:</p> <ul style="list-style-type: none"> • Internal mail routing—the time it takes to send an internal email from one mailbox to another. • Roundtrip mail routing—the time it takes an email to leave the sender's outbox until it comes back from the echo service. This measures the full outbound and inbound routing of an email. <p>You can filter these metrics by location.</p> <p>For detailed information about the metrics displayed on this page, see "Mail Routing" on page 76.</p> |
| Cross Analysis | <p>This report page allows you to compare metrics across different platforms. For example, you can view metrics about Exchange Mailbox Server performance next to metrics about Exchange Edge. You can compare Exchange login times with SharePoint login times, or see how long it takes to download a file in Teams versus SharePoint. Use Ctrl-Click to select the metrics to compare.</p> <p>For detailed information about the metrics displayed on this page, see "Cross Analysis" on page 76.</p> |
| Exchange Server Performance | <p>Performance metrics specific to Exchange Servers.</p> <p>For information about the metrics displayed on this page, see "Exchange Server Performance" on page 77.</p> |
| Exchange Free/Busy | <p>An overview of the Exchange Advanced Free/Busy end user experience by location. The panels in this report page track user actions such as the time it takes to log in or to perform a free/busy query.</p> <p>This report page is hidden by default.</p> <p>For detailed information about the metrics displayed on this page, see "Exchange Advanced Free/Busy" on page 78.</p> |

| Report Page | Description |
|------------------|--|
| Exchange MAPI UX | <p>Information about the quality of the connection to Exchange or to Exchange Online from an Outlook client that uses MAPI over HTTP.</p> <p>For detailed information about the metrics displayed on this page, see "Exchange MAPI UX" on page 78.</p> |



Metrics Collected

The following table lists the metrics that are collected for each workload and indicates whether they are available on a VDX Monitoring dashboard or through Power BI.

Table 2: Metrics Available on Dashboards and in Power BI

| Workload or Configuration | Dashboard | Power BI Report |
|---------------------------|--|--|
| AAD Connect | "AAD Connect" on page 46 | "Cross Analysis" on page 76 |
| ADFS | "ADFS" on page 46 | — |
| Exchange DAG | "Exchange DAG" on page 48 | — |
| Exchange Edge Server | "Exchange Edge" on page 49 | "Exchange Server Performance" on page 77 |
| | | "Cross Analysis" on page 76 |
| Exchange Free/Busy | "Exchange Advanced Free/Busy" on page 48 | "Exchange Advanced Free/Busy" on page 78 |
| | | "Cross Analysis" on page 76 |
| Exchange Mailbox Server | "Exchange Mailbox Servers" on page 50 | "Exchange Server Performance" on page 77 |
| | | "Cross Analysis" on page 76 |

| Workload or Configuration | Dashboard | Power BI Report |
|---------------------------|------------------------------------|--|
| Exchange MAPI | "Exchange MAPI" on page 52 | "Exchange MAPI UX" on page 78 |
| Exchange Online | "Exchange" on page 47 | "Exchange UX" on page 67 |
| | | "Cross Analysis" on page 76 |
| | | "UX Analysis" on page 72 |
| | | "Metric Analysis" on page 73 |
| Exchange Online Network | "Network" on page 56 | "Exchange UX" on page 67 "Metric Analysis" on page 73 |
| Exchange OWA | — | "Cross Analysis" on page 76 |
| Hybrid Mail Routing | "Mail Routing Hybrid" on page 54 | "Cross Analysis" on page 76 |
| Internal Mail Routing | "Mail Routing" on page 53 | "Mail Routing" on page 76 "Cross Analysis" on page 76 |
| — | "Office 365 Operations" on page 57 | — |
| Office 365 Health | "MS Service Health" on page 55 | — |
| Office 365 Web App | — | "Cross Analysis" on page 76 |

| Workload or Configuration | Dashboard | Power BI Report |
|---------------------------|----------------------------------|---|
| OneDrive | "OneDrive" on page 58 | "OneDrive and SharePoint UX" on page 68 |
| | | "UX Analysis" on page 72 |
| | | "Power BI Metrics" on page 64 |
| | | "Cross Analysis" on page 76 |
| Roundtrip Mail Routing | "Mail Routing" on page 53 | "Mail Routing" on page 76 |
| | | "Cross Analysis" on page 76 |
| SharePoint Network | "Network" on page 56 | "OneDrive and SharePoint UX" on page 68 |
| | | "Metric Analysis" on page 73 |
| | | "Cross Analysis" on page 76 |
| SharePoint Page | — | "Cross Analysis" on page 76 |
| SMTP Gateways | "Mail Routing Hybrid" on page 54 | "Cross Analysis" on page 76 |

| Workload or Configuration | Dashboard | Power BI Report |
|---------------------------|-----------------------------|-------------------------------|
| Teams | "Teams" on page 59 | "Teams Voice" on page 70 |
| | | "Teams for Export" on page 70 |
| | | "Teams for Export" on page 70 |
| | | "UX Analysis" on page 72 |
| | | "Metric Analysis" on page 73 |
| | | "Cross Analysis" on page 76 |
| Teams Advanced | "Teams Advanced" on page 61 | "Teams Voice" on page 70 |
| | | "Teams Login" on page 69 |
| | | "Teams for Export" on page 70 |
| | | "UX Analysis" on page 72 |
| | | "Metric Analysis" on page 73 |
| | | "Cross Analysis" on page 76 |
| Teams Network | "Network" on page 56 | "Teams Voice" on page 70 |
| | | "Teams Login" on page 69 |
| | | "Cross Analysis" on page 76 |
| Teams Video | — | "Cross Analysis" on page 76 |
| URL | "URL" on page 63 | "Cross Analysis" on page 76 |

Dashboard Metrics

The following table lists the metrics that VDX Monitoring collects for each workload and the dashboard where they are displayed. Click the links to see more information about metrics available on each dashboard. For information about the metrics available in Power BI, see ["Power BI Metrics" on page 64](#)

Table 3: Metrics Available on Dashboards

| Workload or Configuration | Dashboard |
|---------------------------|--|
| AAD Connect | "AAD Connect" on page 46 |
| ADFS | "ADFS" on page 46 |
| Exchange DAG | "Exchange DAG" on page 48 |
| Exchange Edge Server | "Exchange Edge" on page 49 |
| Exchange Free/Busy | "Exchange Advanced Free/Busy" on page 48 |
| Exchange Mailbox Server | "Exchange Mailbox Servers" on page 50 |
| Exchange MAPI | "Exchange MAPI" on page 52 |
| Exchange Online | "Exchange" on page 47 |
| Exchange Online Network | "Network" on page 56 |
| Hybrid Mail Routing | "Mail Routing Hybrid" on page 54 |
| Internal Mail Routing | "Mail Routing" on page 53 |
| — | "Office 365 Operations" on page 57 |
| Office 365 Web App | — |
| OneDrive | "OneDrive" on page 58 |
| Roundtrip Mail Routing | "Mail Routing" on page 53 |
| SharePoint Network | "Network" on page 56 |
| SharePoint Page | — |
| SMTP Gateways | "Mail Routing Hybrid" on page 54 |

| Workload or Configuration | Dashboard |
|---------------------------|--|
| Teams | "Teams" on page 59 |
| Teams Advanced | "Teams Advanced" on page 61 |
| Teams Network | "Network" on page 56 |
| Teams Video | — |
| URL | "URL" on page 63 |
| Office 365 Health | "MS Service Health" on page 55 |

AAD Connect

For the Azure Active Directory Connect (AAD Connect) workload, VDX Monitoring robots retrieve the last active directory synchronization date and time along with any potential provisioning errors.

The following table lists the metrics that the robots collect.

Table 4: Metrics Collected for AAD Connect

| Metric | Description |
|---------------------------|--|
| Last Synchronization Date | The last date that user information in your on-premises Active Directory was synchronized with the Azure AD tenant of your Microsoft 365 subscription. |

ADFS

For the Active Directory Federation Services (ADFS) workload, VDX Monitoring robots log into ADFS endpoints and authenticate.

The following table lists the metrics that the robots collect.

Table 5: Metrics Collected for ADFS

| Metric | Description |
|---------------------------------|--|
| Authentication Time (ms) | The amount of time, in milliseconds that it takes a user to authenticate against the ADFS. |
| 95%ile Authentication Time (ms) | 95% of the time, the authentication occurs in this amount of time or less. |
| Certificate Information | |

| Metric | Description |
|-------------------------------|---|
| • Scan Configuration Alias | The alias of the scan configuration, as displayed in the "Configurations" page. |
| • Certificate Name | The name of the token-signing certificate used by ADFS. |
| • Certificate Expiration Date | The expiration date of the token-signing certificate used by ADFS. |
| • Certificate Errors | Error messages related to the certificate, such as validation errors. |

Exchange

VDX Monitoring robots perform the following tests for the Exchange Online workload using EWS (Exchange Web Services) to connect to an Exchange mailbox:

- Create a folder.
- Delete a folder.
- Create a message.
- Upload an attachment.
- Download an attachment.
- Delete an attachment.
- Create a task.
- Delete a task.
- Search for an item using filters.
- Create a meeting.
- Query free/busy state.
- Delete an event.

The following table lists the metrics that the robots collect.

Table 6: Metrics Collected for Exchange Online

| Metric | Description |
|------------------------------|--|
| % Warning by app | The percentage of warnings related to Exchange at each site. |
| Top 25 Actions Degraded (ms) | The top 25 user actions that caused the status of the service to be "degraded." The table lists the actions and the number of milliseconds required to perform each one. |

| Metric | Description |
|--|---|
| Performance | Indicates the overall health of the Exchange service. |
| AutoDiscover Execution Time (ms) | The amount of time it takes to find the Exchange Web Service endpoint URL. If auto discover takes a long time, initial connections to Exchange user mailboxes are also impacted. |
| Average Time per Action (ms) | The average time required for robots to perform the test actions. |
| 95%ile per Action by App (ms) | The time that it takes to perform the test actions at each site. The graph shows that 95% of the time, the actions are performed faster than the average. The remaining 5% of the time, the actions take longer than average. |
| 95%ile AutoDiscover Execution Time by App (ms) | The time that it takes to auto discover the Exchange Web Service endpoint URL at each site. The graph shows that 95% of the time, the auto discovery is performed faster than the average. The remaining 5% of the time, the auto discovery take longer than average. |

Exchange Advanced Free/Busy

For the Exchange Free/Busy workload, VDX Monitoring robots perform free/busy requests to a target attendee to retrieve the free/busy status.

The following table lists the metrics that the robots collect.

Table 7: Metrics Collected for Exchange Free/Busy

| Metric | Description |
|----------------------------------|---|
| Performance | Indicates the overall health of the Exchange Advanced Free / Busy service. |
| 95%ile Free/Busy Query Time (ms) | The graph shows that 95% of the time, the server query is faster than the average. The remaining 5% of the time, the server query is longer than the average. |

Exchange DAG

VDX Monitoring robots perform replication health checks for the Exchange Database Availability Group (DAG) workload.

The following table lists the information that the robots collect.

Table 8: Metrics Collected for Exchange DAG

| Metric | Description |
|-------------------------------|---|
| Status | The status of the health check. Each health check is either passed or failed. |
| Replication Health Check Name | The name of the health check performed by the robot. The replication health checks include several tests, such as monitoring database replication and checking the health of the underlying cluster service and network components. |
| Server Name (in error) | For failed tests, the name of the server where errors occurred. |
| Error Message | The message associated with the failure. |

Exchange Edge

VDX Monitoring robots perform the following actions for the Exchange Edge Server workload:

- Retrieve a set of performance counters.
- Retrieve the state of a list of Windows services.
- Retrieve disk information.

The following table lists the metrics that the robots collect.

Table 9: Metrics Collected for Exchange Edge Server

| Metric | Description |
|---|--|
| Current Number of Messages in Submission Queue | The number of messages that are either waiting to be processed, or are actively being processed. |
| Current Number of Messages in Unreachable Queue | The number of messages that cannot be routed to their destinations. This number should not exceed 100. |
| Current Number of Messages in Poison Queue | The number of messages that are isolated in the poison queue. The poison queue isolates messages that contain errors and are determined to be harmful to Exchange after a server or service failure. |
| Top 25 lowest disk space available (%) | The 25 Exchange Edge servers that have the lowest amount of available disk space. |

| Metric | Description |
|--------------|--|
| CPU% Average | The average CPU percentage across all the Exchange Edge Servers calculated per server. |
| RAM% Average | The average RAM percentage across all the Exchange Edge Servers calculated per server. |

Exchange Mailbox Servers

VDX Monitoring robots perform the following actions for the Exchange Mailbox Server workload:

- Retrieve a set of performance counters.
- Retrieve the state of a list of Windows services.
- Retrieve disk information.
- Retrieve Exchange queues information
- Retrieve Exchange components state information
- Retrieve Exchange database information.

The following table lists the metrics that the robots collect.

Table 10: Metrics Collected for Exchange Mailbox Server

| Metric | Description |
|--|--|
| Top Servers with highest CPU Average (%) | The top ten servers that have the highest average CPU usage. |
| Top Servers with highest RAM Average (%) | The servers that have the highest average RAM usage. |
| 50 Mailbox Database Copy Queue Length | <p>The top 50 mailbox databases, sorted by copy queue length.</p> <p>The copy queue length indicates the number of logs waiting to be copied. The recommended queue length is 10 logs or less.</p> |

| Metric | Description |
|---|--|
| Mailbox database status | <p>The mailbox database status provides status information about mailbox database copies.</p> <p>The mailbox database status should either be “mounted” or “healthy.” In Exchange, the mailbox databases are duplicated through the DAG. The primary copy is “mounted” the other copies are “healthy.” The pie chart should show one quarter mounted and three quarters “healthy.” If other statuses appear in this chart, it is an indication that there is an issue.</p> <p>For details on the possible statuses, refer to: https://docs.microsoft.com/en-us/exchange/high-availability/manage-ha/monitor-dags?view=exchserver-2019.</p> |
| 50 Mailbox Database Replay Queue Length | The number of log files waiting to be replayed into the copy of the database. |
| RPC user count | The number of users connected to the service. RPC (Remote Procedure Call over HTTP) is the protocol that allows users to connect securely to an Exchange server. |
| Top Servers with highest RPC Latency average (ms) | The average latency, in milliseconds, of RPC requests. The graph shows the latency for each database. |
| OWA current user | The number of unique users currently logged on to Outlook Web App. The graph shows the number for each database. |
| Top Queues with highest message count | The Exchange server has several queues that hold messages while they are waiting for the next stage of processing. This graph shows the queues that contain the highest number of messages. |
| Top Disks with lowest disk space available (%) | The servers that have the lowest amount of available disk space. |

| Metric | Description |
|---------------------------------------|---|
| 50 Mailbox Database Replay Lag Status | The top 50 mailbox databases, sorted by the percent of completion of log file replay from an active database into its passive lagged database copy. |
| 50 Mailbox Database Seed Status | The top 50 mailbox databases, sorted by the percent of completion of database seeding from an active database into its passive database copy. |

Exchange MAPI

The Exchange MAPI workload provides information about the quality of the connection to Exchange or to Exchange Online from an Outlook client that uses MAPI over HTTP. VDX Monitoring robots perform the following tests for the Exchange MAPI workload:

- Open a mailbox.
- Create an email message.
- Create a meeting.

The following table lists the metrics that the robots collect.

Table 11: Metrics Collected for Exchange MAPI

| Metric | Description |
|---|---|
| % Warning by App | The percentage of warnings related to the Exchange MAPI service at each site. |
| Performance | Indicates the overall health of the Exchange MAPI service. |
| Average Time per Action (ms) | The average time required for robots to perform the test actions. |
| Top 25 Actions Degraded (ms) | The top 25 user actions that caused the status of the service to be "degraded." The table lists the actions and the number of milliseconds required to perform each one. |
| 95%ile of Open Mailbox Time (ms) by Robot | The time that it takes to open a mailbox at each site. The graph shows that 95% of the time, the actions are performed faster than the average. The remaining 5% of the time, the actions take longer than average. |

| Metric | Description |
|---|--|
| 95%ile of Create Message Time (ms) by Robot | The time that it takes to create an email message at each site. The graph shows that 95% of the time, the actions are performed faster than the average. The remaining 5% of the time, the actions take longer than average. |
| 95%ile of Create Meeting Time (ms) by Robot | The time that it takes to create a meeting at each site. The graph shows that 95% of the time, the actions are performed faster than the average. The remaining 5% of the time, the actions take longer than average. |

Mail Routing

This dashboard provides a consolidated view of internal and roundtrip mail routing test results. VDX Monitoring robots perform the following tests for the Internal Mail Routing and Roundtrip Mail Routing workloads:

- Internal mail routing—The time it takes to send an internal email within the same organization. The message is sent from one mailbox to the same mailbox.
- Roundtrip mail routing—The time it takes an email to leave the sender's outbox until it comes back from the echo service. This measures the full outbound and inbound routing of an email.

The following table lists the metrics that the robots collect.

Table 12: Metrics Collected

| Metric | Description |
|---------------------------------|--|
| Internal Mail Routing Time (s) | The average number of seconds it takes to route internal email. |
| Roundtrip Mail Routing Time (s) | The average number of seconds it takes to route external email. |
| Internal Mail Routing # Hops | The average number of hops required to route internal email. |
| Roundtrip Mail Routing # Hops | The average number of hops required for the full outbound and inbound routing of an email. |

| Metric | Description |
|---|---|
| Internal Mail Routing Hops details (slowest) | Detailed information about the internal email that experienced the longest delays in routing. |
| Roundtrip Mail Routing Hops details (slowest) | Detailed information about the outbound and inbound routing for the email that experienced the longest delays in routing. |

Mail Routing Hybrid

This dashboard provides a consolidated view of hybrid mail routing test results if you have both on-premises Exchange servers and Exchange Online.

For the Hybrid Mail Routing and SMTP Gateways workloads, VDX Monitoring robots test the routing time of an email by connecting to a user's mailbox to send an email, and then connecting to the recipient's mailbox to check the receipt of the email. The recipient sends an auto response. When the response is received, the mail flow is successful and the robots delete the test messages. The email can be sent by either EWS or SMTP.

The following table lists the metrics that the robots collect.

Table 13: Metrics Collected

| Metric | Description |
|---------------------------------------|--|
| Hybrid Mail Routing Time (s) | The average round-trip routing time, in seconds, for all mail in a hybrid deployment. |
| Hybrid OutBound Mail Routing Time (s) | The average routing time, in seconds, for outgoing mail in a hybrid deployment. This metric measures the elapsed time from the sending mailbox to the receiving mailbox. |
| Hybrid InBound Mail Routing Time (s) | The average routing time, in seconds, for incoming mail in a hybrid deployment. |
| SMTP Gateways Mail Routing Time (s) | The average routing time, in seconds, for all mail that flows through an SMTP gateway. |
| Hybrid Mail Routing # InBound Hops | The average number of hops required to route email received from external sources. |
| Hybrid Mail Routing # OutBound Hops | The average number of hops required to route email sent to external sources. |
| SMTP Gateways Mail Routing # Hops | The number of hops required to route mail through SMTP gateways. |

| Metric | Description |
|---|--|
| Hybrid Mail Routing InBound Hops details (slowest) | A summary of the sending and receiving endpoints that have the slowest routing time for incoming mail. |
| Hybrid Mail Routing OutBound Hops details (slowest) | A summary of the sending and receiving endpoints that have the slowest routing time for outgoing mail. |
| SMTP Gateways Mail Routing Hops details (slowest) | A summary of the sending and receiving SMTP that have the slowest routing time. |

MS Service Health

Use this dashboard to view the health of your Microsoft Services. The possible health states are:

- Green—The service is operating and is healthy.
- Yellow—The service is degraded.
- Red—The service is not operating.

The Microsoft services for the Office 365 Health workload are auto-discovered and include all Microsoft 365 services that are provisioned for use by an administrator for an organization. The services may include the following:

- Azure Information Protection
- Dynamics 365
- Exchange Online
- Identity Service
- Microsoft Forms
- Flow in Microsoft 365
- Microsoft StaffHub
- Microsoft Teams
- Microsoft Intune
- Office Client Applications
- Office for the Web
- Planner
- PowerApps in Microsoft 365
- Mobile Device Management for Office 365
- Yammer Enterprise
- Office 365 Portal
- OneDrive for Business
- Power BI
- SharePoint Online

Network

This dashboard provides a consolidated view of network test results. VDX Monitoring robots perform the following tests for the Exchange Online Network, SharePoint Network, and Teams Network workloads:

- TCP ping test
- DNS resolution test

The following table lists the metrics that the robots collect.

Table 14: Metrics Collected

| Metric | Description |
|-----------------------------------|--|
| Teams: Average TCP Time (ms) | The amount of time, in milliseconds, that it takes to reach the Teams service. A TCP ping tests the reachability of a service on a host and measures the time it takes to connect to the specified port. |
| Exchange: Average TCP Time (ms) | The amount of time, in milliseconds, that it takes to reach the Exchange service. |
| SharePoint: Average TCP Time (ms) | The amount of time, in milliseconds, that it takes to reach the SharePoint service. |
| Teams: 95%ile TCP Time | The average time that it takes to reach the Teams service each site. The graph shows that 95% of the time, the ping time is faster than the average. The remaining 5% of the time, the TCP ping time is slower. |
| Exchange: 95%ile TCP Time | The average time that it takes to reach the Exchange service each site. The graph shows that 95% of the time, the ping time is faster than the average. The remaining 5% of the time, the TCP ping time is slower. |
| SharePoint: 95%ile TCP Time | The average time that it takes to reach the SharePoint service each site. The graph shows that 95% of the time, the ping time is faster than the average. The remaining 5% of the time, the TCP ping time is slower. |
| Teams: Average Packet Loss (%) | The average percentage of Teams packets lost in a 15-second interval. |
| Exchange: Average Packet Loss (%) | The average percentage of Exchange packets lost in a 15-second interval. |

| Metric | Description |
|--|--|
| SharePoint: Average Packet Loss (%) | The average percentage of SharePoint packets lost in a 15-second interval. |
| Teams: 95%ile Packet Loss | The average amount of packet loss for the Teams service at each site, in comparison to the 95 percentile. The graph shows that 95% of the time, the loss is below this average. The remaining 5% of the time, the loss is above this average. |
| Exchange: 95%ile Packet Loss | The average amount of packet loss for the Exchange service at each site, in comparison to the 95 percentile. The graph shows that 95% of the time, the loss is below this average. The remaining 5% of the time, the loss is above this average. |
| SharePoint: 95%ile Packet Loss | The average amount of packet loss for the Exchange service at each site, in comparison to the 95 percentile. The graph shows that 95% of the time, the loss is below this average. The remaining 5% of the time, the loss is above this average. |
| Teams: Average Packet Loss by App (%) | The average amount of packet loss, shown for the Teams service at each site. |
| Exchange: Average Packet Loss by App (%) | The average amount of packet loss, shown for the Exchange service at each site. |
| SharePoint: Average Packet Loss by App (%) | The average amount of packet loss, shown for the SharePoint service at each site. |

Office 365 Operations

The Office 365 Operations dashboard is created automatically by VDX Monitoring; no configuration is necessary. The dashboard provides a consolidated view of the following Microsoft 365 services test results:

- Exchange
- Teams
- OneDrive

The following table lists the metrics that the robots collect.

Table 15: Metrics Collected

| Metric | Description |
|--------------------------------|---|
| OneDrive Slow Actions (95%ile) | A comparison of the time required for a user to perform the following tasks: login, upload a file, and download a file. Data is provided for each site. |
| Exchange Slow Actions (95%ile) | <p>A comparison of the time required for a user to perform the following tasks:</p> <ul style="list-style-type: none"> • Authenticate the connection. • Create a message. • Search using a filter. • Create a folder. • Delete a folder. • Upload an attachment. • Download an attachment. • Remove an attachment. • Create a task. • Create a meeting. • Delete a task. • Delete an event. • Query free/busy availability for meeting invitations. <p>Data is provided for each site.</p> |
| Teams Low MOS (5%ile) | Indicates that 5% of the time, the Mean Opinion Score (MOS) for teams is lower than the score indicated by the graphs. Data is provided for each site. |
| Exchange Login Time (ms) | The average time it takes a user to login into Exchange and authenticate. |

OneDrive

VDX Monitoring robots perform the following tests for the OneDrive workload:

- Log in.
- Upload a file.
- Download a file.
- Create a OneDrive folder.

The following table lists the metrics that the robots collect.

Table 16: Metrics Collected for OneDrive

| Metric | Description |
|-------------------------------|---|
| % Warning by App | The percentage of warnings related to OneDrive at each site. |
| Top 25 Actions Degraded (ms) | The top 25 user actions that caused the status of the service to be "degraded." The table lists the actions and the number of milliseconds required to perform each one. |
| Performance | Indicates the overall health of the OneDrive service. |
| Average Time per Action (ms) | The average time required for robots to perform the test actions. |
| 95%ile per Action by App (ms) | The time that it takes to perform the test actions at each site. The graph shows that 95% of the time, the actions are performed faster than the average. The remaining 5% of the time, the actions take longer than average. |

Teams

VDX Monitoring robots perform the following tests for the Teams workload:

- Log in.
- Make a voice call.

The following table lists the metrics that the robots collect.

Table 17: Metrics Collected for Teams

| Metric | Description |
|-----------------------------------|---|
| Average Mean Opinion Score Global | The average Mean Opinion Score (MOS). A prediction of end-user audio quality experience. It is based on latency, the packet loss, jitter, and the codec used. |
| % Warning by App | The percentage of warnings related to Teams at each site. |
| Performance | Indicates the overall health of the Teams service. |
| Lowest MOS Overall | Displays the lowest MOS score at any site. |

| Metric | Description |
|--|---|
| 95%ile PacketLoss, PacketReorder by App | |
| <ul style="list-style-type: none"> • Packet Loss Rate | <p>The number of packets lost in a 15-second interval. For example, if 1000 packets are sent in a 15-second interval and 50 are lost, the packet loss rate is 5%.</p> <p>Microsoft recommends a packet loss rate of 1% during a 15-second interval. A packet loss rate between 3% and 7% causes a noticeable impact to call quality. A rate of more than 7% severely impacts the call quality.</p> <p>The graph shows that 95% of the time, the packet loss is better than the average. The remaining 5% of the time, packet loss is below the average.</p> |
| <ul style="list-style-type: none"> • Packet Reorder Ratio | <p>The packet reorder ratio is the number of packets that should be reordered over the total number of packets.</p> <p>Packets need to be reconstructed when they arrive in a different order than they were sent. Packet reordering severely degrades the call quality.</p> <p>The graph shows that 95% of the time, the number of packets re-ordered was lower than the average. The remaining 5% of the time, the number of packets re-ordered was above the average.</p> |
| 95%ile RTT, Jitter by App | |
| <ul style="list-style-type: none"> • Round Trip Latency | <p>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.</p> |

| Metric | Description |
|--|--|
| <ul style="list-style-type: none"> Average Jitter | <p>The size of the buffer that is needed to store packets before they are reconstructed in the correct order. The value is calculated over a 15-second period.</p> <p>A low jitter number means that the call connection is good. A large jitter value can cause delay in calls and indicates congestion of the network.</p> |
| 5%ile MOS by App | A prediction of end-user audio quality experience. It is based on latency, the packet loss, jitter, and the codec used. The graph shows that 5% of the time, MOS is below the average. |
| 10%ile Bandwidth Average by App (Mbit/s) | The graph shows that 10% of the time, bandwidth usage is above the average. |
| 95%ile Login Time by App (ms) | The time in milliseconds to log into Teams. The graph shows that 95% of the time, the amount of time required to log in was better than the average. The remaining 5% of the time, the amount of time required to log in was slower than the average. |
| Login Time (ms) | The average time in milliseconds to log into Teams. |

Teams Advanced

VDX Monitoring robots perform the following tests for the Teams Advanced workload:

- Log in.
- Voice call.
- Create a channel.
- Post a message to a channel.
- Upload file to a channel.
- Download file from a channel.
- Search for a user.
- Check presence.
- Send an instant message.

The following table lists the metrics that the robots collect.

Table 18: Metrics Collected for Teams Advanced

| Metric | Description |
|--|--|
| Average Mean Opinion Score Global | The average Mean Opinion Score (MOS). A prediction of end-user audio quality experience. It is based on latency, the packet loss, jitter, and the codec used. |
| % Warning by App | The percentage of warnings related to Teams at each site. |
| Performance | Indicates the overall health of the Teams service. |
| 95%ile per Action by App (ms) | The time that it takes to perform the test actions at each site. The graph shows that 95% of the time, the actions are performed faster than the average. The remaining 5% of the time, the actions take longer than average. |
| Average Time per Action (ms) | The average time required for robots to perform the test actions. |
| Lowest MOS Overall | Displays the lowest MOS score at any site. |
| 95%ile PacketLoss, PacketReorder by App: | |
| <ul style="list-style-type: none"> Packet Loss Rate | <p>The number of packets lost in a 15-second interval. For example, if 1000 packets are sent in a 15-second interval and 50 are lost, the packet loss rate is 5%.</p> <p>Microsoft recommends a packet loss rate of 1% during a 15-second interval. A packet loss rate between 3% and 7% causes a noticeable impact to call quality. A rate of more than 7% severely impacts the call quality.</p> |
| <ul style="list-style-type: none"> Packet Reorder Ratio | <p>The packet reorder ratio is the number of packets that should be reordered over the total number of packets.</p> <p>Packets need to be reconstructed when they arrive in a different order than they were sent. Packet reordering severely degrades the call quality.</p> |

| Metric | Description |
|--|--|
| 95%ile RTT, Jitter by App | |
| <ul style="list-style-type: none"> Round Trip Latency | 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. |
| <ul style="list-style-type: none"> Average Jitter | <p>The size of the buffer that is needed to store packets before they are reconstructed in the correct order. The value is calculated over a 15-second period.</p> <p>A low jitter number means that the call connection is good. A large jitter value can cause delay in calls and indicates congestion of the network.</p> |
| 5%ile MOS by App | A prediction of end-user audio quality experience. It is based on latency, the packet loss, jitter, and the codec used. The graph shows that 5% of the time, MOS is below the average. |
| 10%ile Bandwidth Average by App (Mbit/s) | The graph shows that 10% of the time, bandwidth usage is above the average. |
| 95%ile Login Time by App (ms) | The time in milliseconds to log into Teams. The graph shows that 95% of the time, the amount of time required to log in was better than the average. The remaining 5% of the time, the amount of time required to log in was slower than the average. |
| Login Time (ms) | The average time in milliseconds to log into Teams. |

URL

For the URL workload, VDX Monitoring robots connect to a specified URL and retrieve the HTTPS certificate information.

The following table lists the metrics that the robots collect.

Table 19: Metrics Collected for URL

| Metric | Description |
|--------------------------------|---|
| Average URL Response Time (ms) | The average time, in milliseconds, that it takes for request from a user to receive a response from the server. |
| 95%ile Response Time (ms) | The graph shows that 95% of the time, the server response is faster than the average. The remaining 5% of the time, the server response is longer than the average. |
| URL Detailed Information | A summary of information about the URL, including the certificate name, certificate expiry date, and any certificate errors. |

Power BI Metrics

The following table lists the metrics that VDX Monitoring collects for each workload and the Power BI report page where they are displayed. Click the links to see more information about metrics available on each report page. For information about the metrics available on dashboards, see ["Dashboard Metrics" on page 45](#).

Table 20: Metrics Available in Power BI

| Workload or Configuration | Power BI Report |
|---------------------------|---|
| AAD Connect | "Cross Analysis" on page 76 |
| ADFS | — |
| Exchange DAG | — |
| Exchange Edge Server | "Exchange Server Performance" on page 77 "Cross Analysis" on page 76 |
| Exchange Free/Busy | "Exchange Advanced Free/Busy" on page 78 "Cross Analysis" on page 76 |
| Exchange Mailbox Server | "Exchange Server Performance" on page 77 "Cross Analysis" on page 76 |
| Exchange MAPI | "Exchange MAPI UX" on page 78 |

| Workload or Configuration | Power BI Report |
|---------------------------|---|
| Exchange Online | "Exchange UX" on page 67 |
| | "Cross Analysis" on page 76 |
| | "UX Analysis" on page 72 |
| | "Metric Analysis" on page 73 |
| Exchange Online Network | "Exchange UX" on page 67 |
| | "Metric Analysis" on page 73 |
| Exchange OWA | "Cross Analysis" on page 76 |
| Hybrid Mail Routing | "Cross Analysis" on page 76 |
| Internal Mail Routing | "Mail Routing" on page 76 |
| | "Cross Analysis" on page 76 |
| Office 365 Health | — |
| Office 365 Web App | "Cross Analysis" on page 76 |
| OneDrive | "OneDrive and SharePoint UX" on page 68 |
| | "UX Analysis" on page 72 |
| | "Cross Analysis" on page 76 |
| Roundtrip Mail Routing | "Mail Routing" on page 76 |
| | "Cross Analysis" on page 76 |
| SharePoint Network | "OneDrive and SharePoint UX" on page 68 |
| | "Metric Analysis" on page 73 |
| | "Cross Analysis" on page 76 |
| SharePoint Page | "Cross Analysis" on page 76 |
| SMTP Gateways | "Cross Analysis" on page 76 |

| Workload or Configuration | Power BI Report |
|---------------------------|---|
| Teams | "Teams Voice" on page 70 |
| | "Teams for Export" on page 70 |
| | "Teams for Export" on page 70 |
| | "UX Analysis" on page 72 |
| | "Metric Analysis" on page 73 |
| | "Cross Analysis" on page 76 |
| Teams Advanced | "Teams Voice" on page 70 |
| | "Teams Login" on page 69 |
| | "Teams for Export" on page 70 |
| | "UX Analysis" on page 72 |
| | "Metric Analysis" on page 73 |
| | "Cross Analysis" on page 76 |
| Teams Network | "Teams Voice" on page 70 |
| | "Teams Login" on page 69 |
| | "Cross Analysis" on page 76 |
| Teams Video | "Cross Analysis" on page 76 |
| Teams Voice | "Teams Voice" on page 70 |
| | "Metric Analysis" on page 73 |
| | "Cross Analysis" on page 76 |
| URL | "Cross Analysis" on page 76 |

Top Level Dashboard

The following table lists the metrics that are available in Power BI on the Top Level Dashboard page.

Table 21: Metrics Collected for the Top Level Report

| Metric | Description |
|--------------------------------------|---|
| Performance delivered to end users | The percentage of time when users were able to access the service and perform actions within the performance thresholds for each location. |
| Performance degradations by location | A geographical map that allows you to compare the amount of performance degradation at each location. |
| Top critical locations | For each location, a comparison of the proportion of warnings for each of the following applications: Exchange Online (Exco), SharePoint Online (Spo), and Teams. |

Exchange UX

The following table lists the metrics that are available in Power BI on the Exchange UX page.

Table 22: Metrics Collected for the Exchange UX Report

| Metric | Description |
|--------------------------------------|--|
| Performance delivered to end users | The percentage of time when users were able to access the service and perform actions within the performance thresholds for each location. |
| AutoDiscover (ms) | The amount of time it takes to find the Exchange Web Service endpoint URL. If auto discover takes a long time, initial connections to Exchange user mailboxes are also impacted. |
| Open Mailbox (ms) | The average time required for robots to open a mailbox. |
| Performance degradations by location | A geographical map that allows you to compare the amount of performance degradation at each location. |
| Create Email (ms) | The average time required for robots to create an email message. |
| Create Meeting (ms) | The average time required for robots to create a meeting. |

| Metric | Description |
|--------------------------|--|
| Free/Busy check (ms) | The average time required for robots to check the free/busy status of user's calendar. |
| Search (ms) | The average time required for robots to search for an email message. |
| Download Attachment (ms) | The average time required for robots to download an email attachment. |
| TCP Connect Time (ms) | The average time that it takes to connect to the Exchange service at each site. |
| DNS Resolution time (ms) | The average time it takes to resolve DNS requests for outlook.office365.com. |
| Total Packet Loss (%) | The total percentage of Exchange packets lost during a ping. |

OneDrive and SharePoint UX

The following table lists the metrics that are available in Power BI on the OneDrive and SharePoint UX page.

Table 23: Metrics Collected for the OneDrive/SharePoint Report

| Metric | Description |
|--------------------------------------|--|
| Performance delivered to end users | The percentage of time when users were able to access the service and perform actions within the performance thresholds for each location. |
| Total Execution Time (ms) | The average time required for robots to perform all of the test actions at each site. |
| Login (ms) | The average time it takes to log in at each site. |
| Performance degradations by location | A geographical map that allows you to compare the amount of performance degradation at each location. |
| Total Packet Loss (%) | The total percentage of SharePoint or OneDrive packets lost during a ping. |
| Upload (ms) | The average time it takes to upload a file at each site. |

| Metric | Description |
|--------------------------|--|
| TCP Connect Time (ms) | The average time that it takes to connect to the service at each site. |
| Download (ms) | The average time it takes to download a file at each site. |
| DNS Resolution time (ms) | The average time it takes to resolve DNS requests for the SharePoint or OneDrive domain. |
| Create Folder (ms) | The average time it takes to create a OneDrive folder at each site. |

Teams Login

The following table lists the metrics that are available in Power BI on the Teams Login page.

Table 24: Metrics Collected for the Teams Login Report

| Metric | Description |
|--------------------------------------|--|
| Performance delivered to end users | The percentage of time when users could access the service and perform actions within the performance thresholds configured for each location. |
| Connection time (ms) | The time it takes to connect to the Teams endpoint. |
| Teams Connection Time breakdown (ms) | A comparison of the amount of time required by each authentication method to connect to the Teams endpoint. |
| OAuth time (ms) | The time required to authenticate the user on either Azure AD or ADFS and to get an authentication token. |
| AuthZ time (ms) | The time required to authenticate Teams users. |
| Property time (ms) | The time it takes to make API requests to access user properties. |
| Endpoint Discovery time (ms) | The time required to find global endpoints for Teams. |
| TCP Connect Time (ms) | The average time that it takes to connect to the Teams service at each site. |

| Metric | Description |
|--------------------------|--|
| DNS Resolution time (ms) | The average time it takes to resolve DNS requests for the Teams service. |
| Total Packet Loss (%) | The number of packets lost in a 15-second interval. For example, if 1000 packets are sent in a 15-second interval and 50 are lost, the packet loss rate is 5%. |

Teams for Export

The following table lists the metrics that are available in Power BI on the Teams for Export page. This report page provides raw data about the connection between the machine where the Robot Manager is installed and the Teams endpoint. You can use this data to understand where packet loss and latency are occurring.

Table 25: Metrics Collected for the Teams Export Report

| Metric | Description |
|-----------------------|---|
| Call Data Table | <p>This table lists details of test calls, such as:</p> <ul style="list-style-type: none"> The date and time of robot tests. The host name, IP address, and location of the machine that hosts the robot. Call quality metrics such as packet loss, latency, jitter, and more. |
| Mean Opinion Score | The average Mean Opinion Score (MOS). A prediction of end-user audio quality experience. It is based on latency, the packet loss, jitter, and the codec used. |
| Remote Port Breakdown | This graph shows the percentage of usage for each remote port. |
| Count by Remote IP | The number of connections or sessions for each IP address. |
| Source | For each host where a Robot Manager is installed, this table lists the average packet loss rate and average latency. |

Teams Voice

The following table lists the metrics that are available in Power BI on the Teams Voice page.

Table 26: Metrics Collected for Teams Voice Report

| Metric | Description |
|------------------------------------|--|
| Performance delivered to end users | The percentage of time when users were able to access the service and perform actions within the performance thresholds for each location. |
| Mean Opinion Score | The average Mean Opinion Score (MOS). A prediction of end-user audio quality experience. It is based on latency, the packet loss, jitter, and the codec used. |
| Protocol | The percentage of connections that used TCP and UDP at each site. |
| Packet Loss Rate | The number of packets lost in a 15-second interval. For example, if 1000 packets are sent in a 15-second interval and 50 are lost, the packet loss rate is 5%. |
| Packet Reorder Ratio | Packets need to be reconstructed when they arrive in a different order than they were sent. Packet reordering severely degrades the call quality. The packet reorder ratio is the number of packets that need to be reordered compared to the total number of packets. |
| Jitter (ms) | The size of the buffer that is needed to store packets before they are reconstructed in the correct order. The value is calculated over a 15-second period. |
| Healed Ratio | The percentage of audio samples that had to be concealed due to packet loss. A value higher than 2% causes a degradation in audio quality. |
| Degradation Average | The amount of network jitter and packet loss, as it relates to an audio stream. If the average audio degradation is found to be above 1.0, then the stream is classified as being of poor quality. |

| Metric | Description |
|--------------------------------------|--|
| RTT (ms) | Round trip time (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. |
| Performance degradations by location | A geographical map that allows you to compare the amount of performance degradation at each location. |
| Bandwidth Average | The average bandwidth usage at each site. |

UX Analysis

The following table lists the metrics that are available in Power BI on the UX Analysis page.

Table 27: Metrics Collected for the UX Analysis Report

| Metric | Description |
|---|--|
| Warning per location and service | The proportion of warnings for each of the following services, shown by the locations where the Robot Manager is installed: Exchange Online (Exco), SharePoint Online (Spo), and Teams. |
| Exchange - Bad user experience counts | This graph shows the tasks that caused a poor experience for end users, and the number of times the experience was poor. |
| Top 100 Actions degraded (Exchange / SharePoint / OneDrive) | The information displayed in this table depends on the selections you make on the page. If you select a location from the Warning per Location and Service list, this table lists the 100 actions for that location that had the worst performance degradations. If you select one of the actions from the Exchange or SharePoint Bad user Experience Counts panels, this table lists details about performance degradation for the selected action. |

| Metric | Description |
|--|---|
| SharePoint - Bad user experience counts | This graph shows the the number of times that the user experience was poor. |
| Voice - Bad user experience counts (including dropped calls) | This graph shows the the number of times that the user experience was poor. |

Metric Analysis

The following table lists the metrics that are available in Power BI on the Metric Analysis page.

Table 28: Metrics Collected for the Metric Analysis Report

| Metric | Description |
|------------------------------|---|
| Exchange | |
| AutoDiscover (ms) | The time required to perform an autodiscover operation, which finds the URL for the EWS endpoint. |
| Open Mailbox (ms) | The average time required for robots to open a mailbox. |
| Create Meeting (ms) | The average time required for robots to create a meeting. |
| Free/Busy check (ms) | The average time required for robots to check the free/busy status of user's calendar. |
| Search (ms) | The average time required for robots to search for an email message. |
| Download Attachment | The average time required for robots to download an email attachment. |
| Create Email with Attachment | The time required to create an email and add an attachment. |
| SharePoint/OneDrive | |
| Login (ms) | The time it takes to log in at each site. |
| Upload (ms) | The time it takes to upload a file at each site. |

| Metric | Description |
|-----------------------|---|
| Download (ms) | The time it takes to download a file at each site. |
| Teams | |
| Mean Opinion Score | The average Mean Opinion Score (MOS). A prediction of end-user audio quality experience. It is based on latency, the packet loss, jitter, and the codec used. |
| Healed Ratio | The percentage of audio samples that had to be concealed due to packet loss. A value higher than 2% causes a degradation in audio quality. |
| Degradation Average | The amount of network jitter and packet loss, as it relates to an audio stream. If the average audio degradation is found to be above 1.0, then the stream is classified as being of poor quality. |
| Bandwidth Average | The average bandwidth usage at each site. |
| Low Bandwidth (<2.5K) | The number of tests where the results showed that the available bandwidth was less than 2500 Mbps. |
| MOS 5th %ile | Shows your average MOS in comparison to the ideal MOS. MOS is a prediction of end-user audio quality experience. It is based on latency, the packet loss, jitter, and the codec used. For 5% of the time, MOS is below the average shown in this graph. |
| Protocol | The percentage of connections that used TCP and UDP at each site. |
| Bandwidth 5th %ile | For 5% of the time, the available bandwidth is below the average shown in this graph. |
| Network | |

| Metric | Description |
|----------------------|--|
| RTT (ms) | Round trip time (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. |
| Jitter (ms) | The size of the buffer that is needed to store packets before they are reconstructed in the correct order. The value is calculated over a 15-second period. |
| Packet Loss Rate (%) | The number of packets lost in a 15-second interval. For example, if 1000 packets are sent in a 15-second interval and 50 are lost, the packet loss rate is 5%. |
| Packet Reorder Ratio | Packets need to be reconstructed when they arrive in a different order than they were sent. Packet reordering severely degrades the call quality. The packet reorder ratio is the number of packets that need to be reordered compared to the total number of packets. |
| DNS (ms) | The average time to resolve DNS requests. The optimal threshold is 750 ms or less, is also indicated on the graph. |
| DNS (ms) | The time to resolve DNS requests, shown by robot. The optimal threshold is 750 ms or less, is also indicated on the graph. |
| RTT 95th %ile (ms) | <p>Round trip time (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.</p> <p>The graph shows that 95% of the time, the RTT is better than the performance threshold (100 ms) shown on the graph.</p> |

| Metric | Description |
|------------------------------------|---|
| Packet Loss Rate 95th %ile (ms) | The average amount of packet loss for the network , in comparison to the 95 percentile. The graph shows that 95% of the time, the loss is below this average. The remaining 5% of the time, the loss is above this average. |
| DNS 95th %ile (ms) | The average amount of time to resolve DNS requests. The graph shows that 95% of the time, the resolution time is better than the performance threshold (750 ms) shown on the graph. |

Mail Routing

The following table lists the metrics that are available in Power BI on the Mail Routing report page.

Table 29: Metrics Collected for Mail Routing Report

| Metric | Description |
|--|--|
| Configuration Name | Select the mail routing configuration that you want to display information about. |
| Choose a Mail Routing Configuration | Click to select an option. |
| Avg Routing Time (ms) | The average number of milliseconds it takes to route email for the selected configuration. |
| Avg # Hops | The average number of hops required to route email. |
| Internal Mail Routing Time (ms) and #Hops by Scan Date | The average number of milliseconds it takes to route email and the average number of hops required, shown on a timeline. The scan date is the date of the test performed by the robot. |

Cross Analysis

This report page allows you to compare metrics across different platforms. For example, you can view metrics about Exchange Mailbox Server performance next to metrics about Exchange Edge. You can compare Exchange login times with SharePoint login times, or see how long it takes to download a file in Teams versus SharePoint. Use Ctrl-Click to select the metrics to compare.

The following table lists the metrics that are available in Power BI on the Cross Analysis page.

Table 30: Metrics Collected for the Cross-Analysis Report

| Metric | Description |
|----------------------------|---|
| Platform and Property Name | <p>Select a platform, or expand the platform and select a specific metric. Use Ctrl-click to select multiple metrics. The data in the report updates, based on the selection you make in this panel.</p> <p>To see a definition of each metric, click to expand it. A definition displays below the name of the metric.</p> |
| Platform | This panel displays the selected metric, and provides the minimum, average, and maximum value for each. |
| Average Value by Property | This graph shows a comparison of the selected metrics. |
| Average Value by Property | Displays the selected metrics in the format of your choice. You can view the metrics on a time line, on a map, as a waterfall graph, or as a radar graph. |

Exchange Server Performance

The following table lists the metrics that are available in Power BI on the Exchange Server Performance page.

Table 31: Metrics Collected for the Exchange Server Performance Report

| Metric | Description |
|----------------------------|--|
| Platform and Property Name | <p>Select a platform, or expand the platform and select a specific metric. The data in the report updates, based on the selection you make in this panel.</p> <p>To see a definition of each metric, click to expand it. A definition displays below the name of the metric.</p> |
| Platform | This panel displays the selected metric, and provides the minimum, average, and maximum value for each. |

| Metric | Description |
|--|---|
| Average property value by Configuration | This graph shows the average for each performance metric for the selected platform. |
| Average property value by Configuration, by Date | Select one or more metrics from the Platform and Property Name panel to view the average value for the metrics over time. |

Exchange Advanced Free/Busy

The following table lists the metrics that are available in Power BI on the Exchange Advanced Free/Busy page.

Table 32: Metrics Collected for the Exchange Advanced Free/Busy Report

| Metric | Description |
|--|--|
| Performance delivered to end users | The percentage of time when users were able to access the service and perform actions within the performance thresholds for each location. |
| Connection Time by Robot (ms) | The time it takes to connect to the endpoint. You can filter the times by robot. |
| Free / Busy Query Time by Robot (ms) | The average time required for robots to check the free/busy status of user's calendar. You can filter the times by robot. |
| Performance degradations by location | A geographical map that allows you to compare the amount of performance degradation at each location. |
| Connection Time by Configuration (ms) | The time it takes to connect to the endpoint. You can filter the times by monitoring configuration. |
| Free/Busy Query Time by Configuration (ms) | The average time required for robots to check the free/busy status of user's calendar. You can filter the times by monitoring configuration. |

Exchange MAPI UX

The following table lists the metrics that are available in Power BI on the Exchange MAPI UX page. The page is hidden by default. To make the page available to viewers, unhide the page in Power BI Desktop before you share the report.

Table 33: Metrics Collected for the Exchange MAPI UX Report

| Metric | Description |
|-------------------------------------|--|
| Performance delivered to end users | The percentage of time when users were able to access the service and perform actions within the performance thresholds for each location. |
| Performance degradation by location | A geographical map that allows you to compare the amount of performance degradation at each location. |
| Open Mailbox (ms) | The average time required for robots to open a mailbox. |
| Create Message (ms) | The average time required for robots to create an email message. |
| Create Meeting (ms) | The average time required for robots to create a meeting. |

Default Thresholds

VDX Monitoring raises alert notifications based on the tests that the robots perform. For example, VDX Monitoring raises a notification if a connectivity test fails, or if a security certificate has expired. Some notifications are based on performance metrics that have configurable thresholds. These thresholds are set to default values that are based on industry standards, but you can configure them based on your needs. The following table lists each workload that VDX Monitoring supports, and indicates which ones have configurable thresholds. Click the links in the table to see information about the thresholds, their default values, and the type of alert notification raised if the threshold is breached.

Table 34: Workloads with Configurable Thresholds

| Workload or Configuration | Configurable Thresholds |
|---------------------------|---|
| AAD Connect | — |
| ADFS | "ADFS Thresholds" on page 82 |
| Exchange DAG | — |
| Exchange Edge Server | "Exchange Edge Thresholds" on page 83 |
| Exchange Free/Busy | "Exchange Advanced Free/Busy Thresholds" on page 82 |
| Exchange Mailbox Server | "Exchange Mailbox Server Thresholds" on page 83 |
| Exchange MAPI | "Exchange MAPI Thresholds" on page 88 |

| Workload or Configuration | Configurable Thresholds |
|---------------------------|--|
| Exchange Online | "Microsoft Exchange Thresholds" on page 88 |
| Exchange Online Network | — |
| Exchange OWA | "Exchange OWA Thresholds" on page 90 |
| Hybrid Mail Routing | "Hybrid Mail Routing Thresholds" on page 91 |
| Internal Mail Routing | "Internal Mail Routing Thresholds" on page 92 |
| Office 365 Health | — |
| Office 365 Web App | "Office 365 Web App Thresholds" on page 92 |
| OneDrive | "OneDrive Thresholds" on page 92 |
| Roundtrip Mail Routing | "Roundtrip Mail Routing Thresholds" on page 93 |
| SharePoint Network | — |
| SharePoint Page | "SharePoint Page Thresholds" on page 94 |
| SMTP Gateways | "SMTP Gateways Thresholds" on page 94 |
| Teams | "Teams Thresholds" on page 95 |
| Teams Advanced | "Teams Advanced Thresholds" on page 95 |
| Teams Network | — |
| Teams Video | "Teams Video Thresholds" on page 96 |
| URL | "URL Thresholds" on page 97 |

ADFS Thresholds

For the Active Directory Federation Services (ADFS) workload, the robots log into an ADFS endpoint and receive authentication tokens.

The following table lists the thresholds that you can configure for the ADFS workload.

Table 35: Default Thresholds for ADFS

| Threshold Name and Description | Type of Alert | Default Value |
|---|---------------|---------------|
| ADFS Performance Threshold An alert is raised when the robot does not receive an authentication token within the time specified. | Warning | 3000 ms |
| ADFS Critical Threshold An alert is raised when authentication fails. | Critical | 5000 ms |

Exchange Advanced Free/Busy Thresholds

The following table lists the thresholds that you can configure for the Exchange Advanced Free/Busy workload, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 36: Default Thresholds for Exchange Advanced Free/ Busy

| Threshold Name and Description | Type of Alert | Default Value |
|--|---------------|---------------|
| Free/Busy Performance Status Threshold for Open Mailbox action An alert is raised based on the time required to open a mailbox. | Warning | 6000 ms |
| Free/Busy Performance Status Threshold An alert is raised based on the time required to query the availability of the user. | Warning | 4000 ms |
| Free/Busy Critical Status Threshold | Critical | 6000 ms |
| Free/Busy Critical Status Threshold for Open Mailbox action An alert is raised based on the time required to open a mailbox. | Critical | 9000 ms |

Exchange Edge Thresholds

The following table lists the thresholds that you can configure for the Exchange Edge server, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 37: Default Thresholds for Exchange Edge

| Threshold Name and Description | Type of Alert | Default Value |
|---|---------------|---------------|
| Exchange Edge Unreachable Queue Length Threshold An alert is raised based on the number of messages that cannot be routed to their destinations. | Warning | 100 messages |
| Exchange Edge RAM Threshold An alert is raised based on the amount of memory in use compared to the amount of committed memory. | Warning | 90% |
| Exchange Edge Messaged Queued for Delivery Threshold VDX Monitoring raises a notification based on the number of messages that are in the processing queue for delivery. | Warning | 300 messages |
| Exchange Edge Processor Time Threshold An alert is raised when the server is executing processes for more then 75% of the time. | Warning | 75 % |
| Exchange Edge Poison Queue Length Threshold An alert is raised based on the number of messages in the poison queue. The poison queue isolates messages that contain errors and are determined to be harmful to Exchange after a server or service failure. | Warning | 5 messages |
| Exchange Edge Disk Threshold An alert is raised when less than 10% of the disk is free space. | Warning | 10 % |

Exchange Mailbox Server Thresholds

You can configure the following thresholds for the Exchange Mailbox server:

- ["Client Access Thresholds" on page 84](#)
- ["Database Thresholds" on page 84](#)
- ["Lagged Copies Thresholds" on page 85](#)
- ["System Thresholds" on page 85](#)

- ["Transport Thresholds" on page 87](#)

Client Access Thresholds

The following table lists the thresholds that you can configure for the Exchange Mailbox Server Client Access workload, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 38: Default Thresholds for Exchange Mailbox Server Client Access

| Threshold Name and Description | Type of Alert | Default Value |
|---|---------------|---------------|
| RPC Client Access Requests Threshold Alerts are based on the number of requests processed by the RPC Client Access service. | Warning | 40 requests |
| RPC Client Access Averaged Latency Time Threshold Alerts are based on the average latency for the RPC Client Access service. | Warning | 250 ms |

Database Thresholds

The following table lists the thresholds that you can configure for the Exchange Mailbox Server Database workload, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 39: Default Thresholds for Exchange Mailbox Server Databases

| Threshold Name and Description | Type of Alert | Default Value |
|---|---------------|---------------|
| Store RPC Requests Threshold Alerts are based on the number of RPC requests currently executing within the information store. | Warning | 70 requests |
| Database Reads (Attached) Average Latency Time Threshold Alerts are based on the average time of latency to read from the database. | Warning | 20 ms |
| Database Writes (Attached) Average Latency Time Threshold Alerts are based on the average time of latency to write to the database file. | Warning | 50 ms |

| Threshold Name and Description | Type of Alert | Default Value |
|---|---------------|---------------|
| Database Log Writes Average Latency Time Threshold Alerts are based on the average time of latency for each log write operation. | Warning | 10 ms |
| Database Reads Recovery Average Latency Time Threshold Alerts are based on the average time of latency for each passive database read operation. | Warning | 200 ms |
| Store RPC Average Latency Time Threshold Alerts are based on the average time of latency for RPC requests for each database. | Warning | 50 ms |
| Client Type RPC Average Latency Time Threshold Alerts are based on the average time of latency for the RPC server. | Warning | 50 ms |

Lagged Copies Thresholds

The following table lists the thresholds that you can configure for the Exchange Mailbox Server Lagged Copies workload, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 40: Default Thresholds for Exchange Mailbox Server Lagged Copies

| Threshold Name and Description | Type of Alert | Default Value |
|---|---------------|---------------|
| Replay Lag Status Percentage Threshold Alerts are based on the log file replay percentage from an active database into its passive lagged database copy. | Warning | 100 % |

System Thresholds

The following table lists the thresholds that you can configure for the Exchange Mailbox Server System, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 41: Default Thresholds for Exchange Mailbox Server - System

| Threshold Name and Description | Type of Alert | Default Value |
|---|---------------|---------------|
| <p>ASPNet Request Wait Time Threshold</p> <p>Alerts are based on the amount of time that the request waited in the queue for processing.</p> | Warning | 0 ms |
| <p>Exchange Mailbox Disk Threshold</p> <p>An alert is raised when less than 10% of the disk is free space.</p> | Warning | 10 % |
| <p>Domain Controllers LDAP Read Time Threshold</p> <p>Alerts are based on the amount of time it takes to send a message to the domain controller and receive a response.</p> | Warning | 100 ms |
| <p>Processor Percentage Time Threshold</p> <p>Alerts are based on the percentage of time that the processor is executing instructions.</p> | Warning | 75 % |
| <p>Processes LDAP Search Time Threshold</p> <p>Alerts are based on the amount of time it takes to send an LDAP search request and receive a response.</p> | Warning | 100 ms |
| <p>Domain Controllers LDAP Search Time Threshold</p> <p>Alerts are based on the time (in ms) to send an LDAP search request to a domain controller and receive a response.</p> | Warning | 100 ms |
| <p>Processor Privileged Percentage Time Threshold</p> <p>Alerts are based on the amount of elapsed time that the service was running in privileged mode.</p> | Warning | 75 % |
| <p>.Net CLR Memory GC Percentage Time Threshold</p> <p>Alerts are based on the amount of time required to perform garbage collection. This process requires CPU and memory and can cause delays and disconnections if it exceeds the threshold.</p> | Warning | 10 % |
| <p>Processes LDAP Read Time Threshold</p> <p>Alerts are based on the amount of time required to send an LDAP request to a domain controller and receive a response.</p> | Warning | 100 ms |

| Threshold Name and Description | Type of Alert | Default Value |
|---|---------------|---------------|
| ASPNet Application Restarts Threshold Notifications are based on the number of restarts of the ASP.NET application. | Warning | 0 restarts |
| Processor Queue Length Threshold Alerts are based on the number of threads the processor is servicing. A value higher than the threshold can cause high CPU usage and can indicate that processor capacity is not sufficient. | Warning | 6 threads |
| Memory Committed Bytes In Use Percentage Threshold Alerts are based on the amount of committed virtual memory in use, as a percentage of the memory/commit limit. | Warning | 80 % |
| Network Packets Outbound Errors Threshold Alerts are based on the number of outbound packets in error. | Warning | 0 packets |
| ASPNet Requests In Application Queue Threshold Alerts are based on the number of requests waiting for service in the application queue. | Warning | 0 requests |
| Processor User Percentage Time Threshold Alerts are based on the percentage of processor time spent in user mode, which is a processing mode for applications and subsystems. | Warning | 75 % |
| ASPNet Worker Process Restarts Threshold Alerts are based on the number of restarts of the ASP.NET worker process. | Warning | 0 restarts |

Transport Thresholds

The following table lists the thresholds that you can configure for the Exchange Mailbox Server Transport workload, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 42: Default Thresholds for Exchange Mailbox Server—Transport

| Threshold Name and Description | Type of Alert | Default Value |
|---|---------------|---------------|
| Number Of Messages In Queue Threshold Alerts are based on the number of messages waiting for service in the queue. | Warning | 300 messages |

Exchange MAPI Thresholds

The following table lists the thresholds that you can configure for Exchange MAPI, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 43: Default Thresholds for Exchange MAPI

| Threshold Name and Description | Type of Alert | Default Value |
|---|---------------|---------------|
| MAPI Critical Status Threshold Alerts are based on the amount of time required to create an email message and create a meeting. | Critical | 8 s |
| MAPI Performance Status Threshold Alerts are based on the amount of time required to create an email message and create a meeting. | Warning | 5 s |
| MAPI Critical Status Threshold for Open Mailbox action Alerts are based on the amount of time required to open a mailbox. | Critical | 11 s |
| MAPI Performance Status Threshold for Open Mailbox action Alerts are based on the amount of time required to open a mailbox. | Warning | 8 s |

Microsoft Exchange Thresholds

The following table lists the thresholds that you can configure for Exchange, the default values, and the type of type of alert that is raised when the threshold is exceeded. Alerts are based on the amount of time required to perform each task.

These thresholds apply to the Exchange Online workload.

Table 44: Default Thresholds for Exchange

| Threshold Name and Description | Type of Alert | Default Value |
|--|---------------|---------------|
| Exchange Critical Status Threshold for Create Folder action | Critical | 6000 ms |
| Exchange Performance Status Threshold for Create Folder action | Warning | 4000 ms |
| Exchange Critical Status Threshold for Delete Folder action | Critical | 6000 ms |
| Exchange Performance Status Threshold for Delete Folder action | Warning | 4000 ms |
| Exchange Critical Status Threshold for Create Message action | Critical | 6000 ms |
| Exchange Performance Status Threshold for Create Message action | Warning | 4000 ms |
| Exchange Critical Status Threshold for Upload Attachment action | Critical | 6000 ms |
| Exchange Performance Status Threshold for Upload Attachment action | Warning | 4000 ms |
| Exchange Critical Status Threshold for Download Attachment action | Critical | 6000 ms |
| Exchange Performance Status Threshold for Download Attachment action | Warning | 4000 ms |
| Exchange Critical Status Threshold for Remove Attachment action | Critical | 6000 ms |
| Exchange Performance Status Threshold for Remove Attachment action | Warning | 4000 ms |
| Exchange Critical Status Threshold for Create Task action | Critical | 6000 ms |
| Exchange Performance Status Threshold for Create Task action | Warning | 4000 ms |
| Exchange Critical Status Threshold for Delete Task action | Critical | 6000 ms |
| Exchange Performance Status Threshold for Delete Task action | Warning | 4000 ms |

| Threshold Name and Description | Type of Alert | Default Value |
|--|---------------|---------------|
| Exchange Critical Status Threshold for Search Using Filter action | Critical | 6000 ms |
| Exchange Performance Status Threshold for Search Using Filter action | Warning | 4000 ms |
| Exchange Critical Status Threshold for Create Meeting action | Critical | 6000 ms |
| Exchange Performance Status Threshold for Create Meeting action | Warning | 4000 ms |
| Exchange Critical Status Threshold for Query Free/Busy action | Critical | 6000 ms |
| Exchange Performance Status Threshold for Query Free/Busy action | Warning | 4000 ms |
| Exchange Critical Status Threshold for Delete Event action | Critical | 6000 ms |
| Exchange Performance Status Threshold for Delete Event action | Warning | 4000 ms |
| Exchange Critical Status Threshold for Open Mailbox action | Critical | 9000 ms |
| Exchange Performance Status Threshold for Open Mailbox action | Warning | 6000 ms |

Exchange OWA Thresholds

The following table lists the thresholds that you can configure for Exchange MAPI, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 45: Default Thresholds for Exchange MAPI

| Threshold Name and Description | Type of Alert | Default Value |
|--|---------------|---------------|
| OWA Performance Status Threshold for Open Mailbox action. | Warning | 8000 ms |
| Alerts are based on the amount of time required to open a mailbox. | | |

| Threshold Name and Description | Type of Alert | Default Value |
|--|---------------|---------------|
| OWA Critical Status Threshold for Open Mailbox action. Alerts are based on the amount of time required to open a mailbox. | Critical | 11000 ms |
| OWA Critical Status Threshold for Create Email action Alerts are based on the amount of time required to create an email. | Warning | 5000 ms |
| OWA Critical Status Threshold for Create Email action Alerts are based on the amount of time required to create an email. | Critical | 8000 ms |
| OWA Critical Status Threshold for Create Meeting action. Alerts are based on the amount of time required to create a meeting. | Warning | 5000 ms |
| OWA Critical Status Threshold for Create Meeting action. Alerts are based on the amount of time required to create a meeting. | Critical | 8000 ms |

Hybrid Mail Routing Thresholds

The following table lists the thresholds that you can configure for Hybrid Mail Routing, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 46: Default Thresholds for Hybrid Mail Routing

| Threshold Name and Description | Type of Alert | Default Value |
|--|---------------|---------------|
| Hybrid Mail Routing Performance Status Threshold Alerts are based on the amount of time required to connect to Exchange, as well as mail routing times and roundtrip times (RTT). | Warning | 30000 ms |
| Hybrid Mail Routing Critical Threshold Alerts are based on the amount of time required to connect to Exchange, as well as mail routing times and roundtrip times (RTT). | Critical | 120000 ms |

Internal Mail Routing Thresholds

The following table lists the thresholds that you can configure for Internal Mail Routing, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 47: Default Thresholds for Internal Mail Routing

| Threshold Name and Description | Type of Alert | Default Value |
|--|---------------|---------------|
| Internal Mail Routing Performance Status Threshold Alerts are based on the amount of time required to connect to Exchange and route mail to internal addresses. | Warning | 15000 ms |
| Internal Mail Routing Critical Status Threshold Alerts are based on the amount of time required to connect to Exchange and route mail to internal addresses. | Critical | 60000 ms |

Office 365 Web App Thresholds

The following table lists the thresholds that you can configure for the Office 365 Web App, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 48: Default Thresholds for Office 365 Web App

| Threshold Name and Description | Type of Alert | Default Value |
|---|---------------|---------------|
| Office 365 Web App Performance Status Threshold Alerts are based on the amount of time required for the page to load after logging in. | Warning | 5000 ms |

OneDrive Thresholds

The following table lists the thresholds that you can configure for the OneDrive workload, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 49: Default Thresholds for OneDrive

| Threshold Name and Description | Type of Alert | Default Value |
|--|---------------|---------------|
| OneDrive Performance Status Threshold for Login action Alerts are based on the time required to log into OneDrive. | Warning | 6000 ms |
| OneDrive Critical Status Threshold for Login action Alerts are based on the time required to log into OneDrive. | Critical | 9000 ms |
| OneDrive Performance Status Threshold for Download action Alerts are based on the time required to download a file from OneDrive. | Warning | 3000 ms |
| OneDrive Critical Status Threshold for Download action Alerts are based on the time required to download a file from OneDrive. | Critical | 5000 ms |
| OneDrive Performance Status Threshold for Upload action Alerts are based on the time required to upload a file to OneDrive. | Warning | 6000 ms |
| OneDrive Performance Status Threshold for Upload action Alerts are based on the time required to upload a file to OneDrive. | Critical | 9000 ms |
| OneDrive Performance Status Threshold for Create Folder action Alerts are based on the time required to create a OneDrive folder. | Warning | 6000 ms |
| OneDrive Critical Status Threshold for Create Folder action Alerts are based on the time required to create a OneDrive folder. | Critical | 9000 ms |

Roundtrip Mail Routing Thresholds

The following table lists the thresholds that you can configure for Roundtrip Mail Routing, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 50: Default Thresholds for Roundtrip Mail Routing

| Threshold Name and Description | Type of Alert | Default Value |
|---|---------------|---------------|
| Roundtrip Mail Routing Critical Status Threshold Alerts are based on the amount of time required to route mail to external addresses. | Critical | 300000 ms |
| Roundtrip Mail Routing Performance Status Threshold Alerts are based on the amount of time required to route mail to external addresses. | Warning | 60000 ms |

SharePoint Page Thresholds

The following table lists the thresholds that you can configure for SharePoint pages, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 51: Default Thresholds for SharePoint Pages

| Threshold Name and Description | Type of Alert | Default Value |
|--|---------------|---------------|
| SharePoint Page Performance Status Threshold Alerts are based on the amount of time required for the page to load after logging in. | Warning | 5000 ms |

SMTP Gateways Thresholds

The following table lists the thresholds that you can configure for SMTP Gateways, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 52: Default Thresholds for SMTP Gateways

| Threshold Name and Description | Type of Alert | Default Value |
|---|---------------|---------------|
| SMTP Gateways Performance Status Threshold Alerts are based on the amount of time required to connect to Exchange and route SMTP mail. | Warning | 60000 ms |
| SMTP Gateways Critical Status Threshold Alerts are based on the amount of time required to connect to Exchange and route SMTP mail. | Critical | 300000 ms |

Teams Thresholds

The following table lists the thresholds that you can configure for the Teams workload, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 53: Default Thresholds for Teams

| Threshold Name and Description | Type of Alert | Default Value |
|--|---------------|---------------|
| Teams Performance Status Threshold An alert is raised if the average Mean Opinion Score (MOS) is below this threshold. MOS is a predictor of voice quality. | Warning | 3.8 MOS |
| Teams Critical Status Threshold An alert is raised if the average Mean Opinion Score (MOS) is below this threshold. MOS is a predictor of voice quality. | Critical | 3.5 MOS |

Teams Advanced Thresholds

The following table lists the thresholds that you can configure for the Teams Advanced workload, the default values, and the type of alert that is raised when the threshold is exceeded. Alerts are based on the amount of time required to perform each of the tasks.

Table 54: Default Thresholds for Teams Advanced

| Threshold Name and Description | Type of Alert | Default Value |
|--|---------------|---------------|
| Teams Performance Status Threshold An alert is raised if the average Mean Opinion Score (MOS) is below this threshold. MOS is a predictor of voice quality. | Warning | 3.8 MOS |
| Teams Critical Status Threshold An alert is raised if the average Mean Opinion Score (MOS) is below this threshold. MOS is a predictor of voice quality. | Critical | 3.5 MOS |
| Teams Performance Status Threshold for Connection Time Action | Warning | 6000 ms |
| Teams Critical Status Threshold for Connection Time Action | Critical | 9000 ms |

| Threshold Name and Description | Type of Alert | Default Value |
|--|---------------|---------------|
| Teams Performance Status Threshold for Create a Channel Time Action | Warning | 6000 ms |
| Teams Critical Status Threshold for Create a Channel Time Action | Critical | 9000 ms |
| Teams Performance Status Threshold for Post Message to Channel Time Action | Warning | 6000 ms |
| Teams Critical Status Threshold for Post Message to Channel Time Action | Critical | 9000 ms |
| Teams Performance Status Threshold for Upload File to Channel Time Action | Warning | 6000 ms |
| Teams Critical Status Threshold for Upload File to Channel Time Action | Critical | 9000 ms |
| Teams Performance Status Threshold for Download File Time Action | Warning | 6000 ms |
| Teams Critical Status Threshold for Download File Time Action | Critical | 9000 ms |
| Teams Performance Status Threshold for Search User Time Action | Warning | 6000 ms |
| Teams Critical Status Threshold for Search User Time Action | Critical | 9000 ms |
| Teams Performance Status Threshold for Check Presence Time Action | Warning | 6000 ms |
| Teams Critical Status Threshold for Check Presence Time Action | Critical | 9000 ms |
| Teams Performance Status Threshold for Instant Message Time Action | Warning | 6000 ms |
| Teams Critical Status Threshold for Instant Message Time Action | Critical | 9000 ms |

Teams Video Thresholds

The following table lists the thresholds that you can configure for Teams Videos, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 55: Default Thresholds for Teams Videos

| Threshold Name and Description | Type of Alert | Default Value |
|---|---------------|---------------|
| Teams Video Performance Status Threshold Alerts are based on the frames per second (FPS) for outbound video streams. | Warning | 7.5 FPS |
| Teams Video Critical Status Threshold Alerts are based on the frames per second (FPS) for outbound video streams. | Critical | 7 FPS |



Note: If you expect your users to regularly utilize screen sharing on Teams Video, we recommend that you change the default Teams Video Critical Status Threshold from 7 FPS to 1 FPS.

URL Thresholds

The following table lists the thresholds that you can configure for the URL workload, the default values, and the type of alert that is raised when the threshold is exceeded.

Table 56: Default Thresholds for URL

| Threshold Name and Description | Type of Alert | Default Value |
|--|---------------|-----------------|
| URL Performance Status Threshold An alert is raised if the HTTP response time is slower than time specified for the threshold. | Warning | 3000 ms |
| URL HTTP Min Status Code Success Threshold The minimum status code for the range of status codes to be excluded from Critical alerts. | Critical | 200 status code |
| URL HTTP Max Status Code Success Threshold The maximum status code for the range of status codes to be excluded from Critical alerts. | Critical | 200 status code |



Troubleshooting

Use the information in the following sections to troubleshoot errors that may occur when you are using VDX Monitoring.


- ["Page Loading and Data Display Errors" on page 98](#)
- ["Notification System Errors" on page 100](#)
- ["Power BI Errors" on page 101](#)

Page Loading and Data Display Errors

Use the information in the table below if pages do not load correctly in the VDX Monitoring Web UI, or if data does not display.

Table 57: Error Messages

| Problem Description or Error Message | Possible Cause |
|---|--|
| <p>On the Exchange Edge, Network, and URL dashboards, the following error displays for some performance metrics:</p> <p>"Failed to retrieve the view."</p> | <p>This error occurs if a Robot Manager has not yet been deployed. The message displays for the following performance metrics:</p> <ul style="list-style-type: none"> Exchange Edge <ul style="list-style-type: none"> CPU% Average RAM% Average Current Number of Messages in Submission Queue Current Number of Messages in Unreachable Queue Current Number of Messages in Poison Queue Network <ul style="list-style-type: none"> Teams: Average Packet Loss by App (%) Exchange: Average Packet Loss by App (%) SharePoint: Average Packet Loss by App (%) URL <ul style="list-style-type: none"> Card 95%ile Response Time (ms) <p>The message clears when Robot Manager is deployed and returns results.</p> |
| <p>Dashboard status information is outdated. For example, your scan frequency is five minutes but the status indicates that the last scan was several days ago.</p> | <p>When you view a dashboard, if the last scan date shown on a status card appears to be incorrect, this may mean that:</p> <ul style="list-style-type: none"> All the robots associated with this status have been manually deleted. The dashboard displays the last known status. The license has expired. |

| Problem Description or Error Message | Possible Cause |
|---|--|
| <p>When you navigate to a page for the first time, the following error message displays:</p> <p>"Can't connect to the database."</p> <p>When you return to a page that you have already viewed, error messages display when you try to use the functionality on the page. Examples of error messages are:</p> <p>"Can't add a tag."</p> <p>"Can't duplicate a configuration."</p> | <p>This problem may occur if you are using Firefox and the browser has been open for several consecutive days. Click the Reload icon in the browser to resolve the issue.</p> |
| <p>The Robots Management page displays the following icon in the Enable Notification and Notification Systems columns:</p>  | <p>The VDX Monitoring Web UI may still be synchronizing with the Robot Manager service. To resolve this issue, wait at least 2 minutes after the Robot Manager installation and then click the Refresh or Reload icon in the browser.</p> |
| <p>The list of configurations on the Robots Management page is not updated to show recently added or removed configurations.</p> | <p>If you or another user adds or removes configurations using PowerShell commands while the Robots Management page is in use, the page may not display the changes immediately. To resolve this issue, click the Refresh or Reload icon in your web browser. The Select Configurations list on the Robots management page updates to reflect the changes.</p> |

Notification System Errors

Use the information in the table below if you encounter error messages related to the notification systems that you have configured.

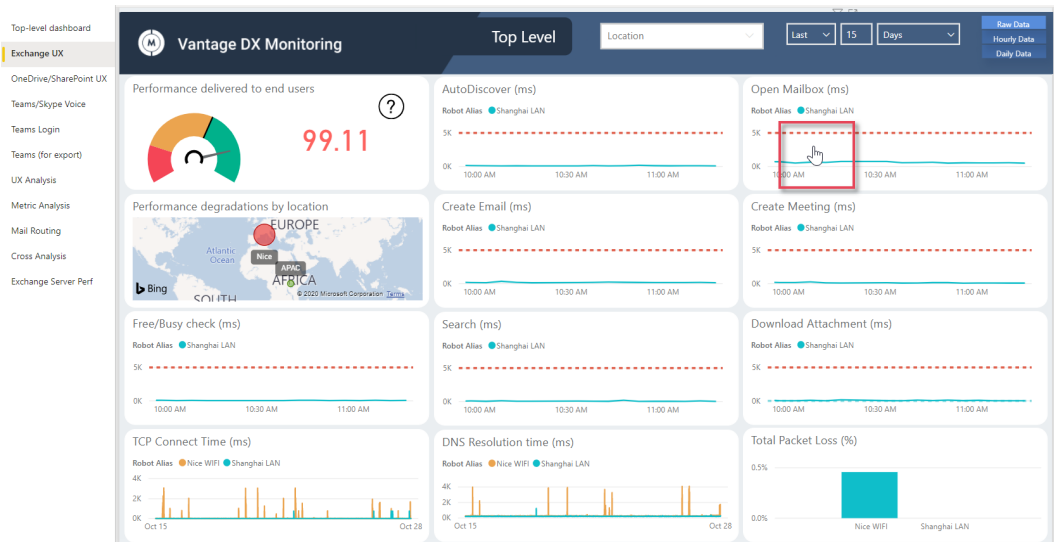
Table 58: Notification System Error Messages

| Problem Description or Error Message | Possible Cause |
|--|--|
| <p>VDX Monitoring does not send alerts to the EWS notification system. The following error message displays:</p> <p>"The server cannot service this request right now. Try again later."</p> | <p>This error may occur if you have not assigned a dedicated account to the notification system. Ensure that you use a dedicated account for each EWS notification system.</p> |
| <p>The Notification Systems page displays the following message:</p> <p>"Error while retrieving delivery systems."</p> | <p>This error may occur if you have used the following PowerShell command to modify a notification system: Set-GsxAlertOutputRoute. Ensure that you use only the VDX Monitoring interface to edit your notification systems.</p> |

Power BI Errors

In Power BI reports, you can view details about the metrics when you hover over them. In some cases, a cursor may display instead, as shown in the following image.

Figure 5: Power BI Display Error



To resolve this issue, perform the following actions:

- **Power BI Desktop**—Click Edit in the report page, resize the component until you see the values correctly, and save the changes.
- **Power BI Service**

Perform these actions on each report page where the error occurs.



Contact

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



© Copyright 2024, Martello Technologies Corporation. All Rights Reserved.

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

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