

MARTELLO



GSX is a subsidiary of
Martello Technologies

Martello Gizmo

USER GUIDE

RELEASE 2.1

DOCUMENT DATE: MARCH 24, 2021

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 2021, Martello Technologies Corporation

All rights reserved

User Guide
Release 2.1 - March 24, 2021

Contents

CHAPTER 1

Introduction	6
Document Purpose	6
Intended Audience	6
Revision History	6

CHAPTER 2

About Gizmo	7
Components	7
Gizmo Web UI	7
Robots	8
Workloads	8
Security	8

CHAPTER 3

About the Interface	10
Dashboards	10
System Dashboards	10
Custom Dashboards	11
Dashboard Components	11
Status Cards	12
Graphs	12
Tables	13
Time Period	14
Settings	14
Credentials	14
Delivery Systems	14
Robots	15
Statuses & Alerts	15
Dashboards	16
Authentication	16

CHAPTER 4

Configure Workloads	17
Select Applications to Monitor	17
Add a Location Tag	18

CHAPTER 5

Configure Alerts	19
Configure a Delivery System	19
Add a Delivery System to Status Alerts	21
Add a Delivery System to Robot Managers	22
Edit Alert Thresholds	23
Create Custom Statuses and Alerts	23
Add Filters	24
Apply Filters	24

CHAPTER 6

Configure Dashboards	26
Create a New Custom Dashboard	26
Create a Custom Dashboard from a System Dashboard	27
Enable or Disable Dashboards	28

CHAPTER 7

Power BI Reports	29
Gizmo Power BI Report Pages	29

CHAPTER 8

Metrics Collected	33
ADFS	34
AAD Connect	34
Exchange	35
Exchange DAG	36
Exchange Edge	37
Exchange Mailbox Servers	37
Mail Routing	39
Mail Routing Hybrid	40
MS Service Health	41
Network	41
Office 365 Operations	43
Office 365 Web Apps	44
OneDrive	46

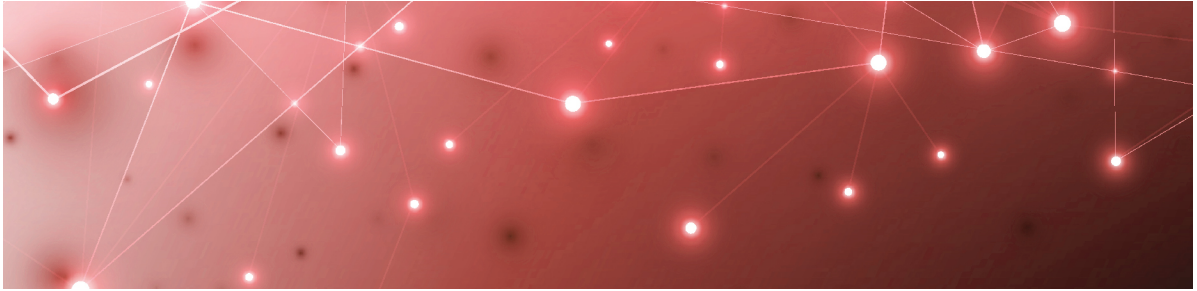
SharePoint	46
Skype for Business	47
Teams	48
Teams Advanced	51
Teams Video	53
URL	57

CHAPTER 9

Default Thresholds	58
ADFS Thresholds	58
Exchange Thresholds	58
Exchange Mailbox Thresholds	59
Exchange Online Thresholds	61
Mail Routing Thresholds	61
OneDrive Thresholds	62
Teams Thresholds	62
URL Thresholds	62

CHAPTER 10

Contact	64
---------------	----



Introduction

Document Purpose

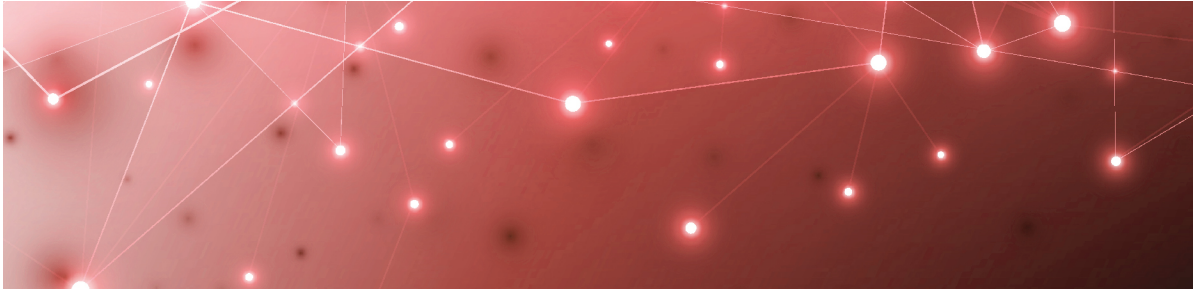
This document provides information about how to use Gizmo to access real-time information in dashboards, manage alerts, understand metrics, and generate reports.

Intended Audience

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

Revision History

Document Date	Description
March 24, 2021	Gizmo User Guide Release 2.1



About Gizmo

Gizmo 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, Gizmo provides you with proactive alerts 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 Gizmo, as well as the security measures that Gizmo uses:

- ["Components" on page 7](#)
- ["Security" on page 8](#)

Components

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

- ["Gizmo Web UI" on page 7](#)
- ["Robots" on page 8](#)
- ["Workloads" on page 8](#)

Gizmo Web UI

The Gizmo Web UI is an application that displays detailed dashboards, metrics, and alerts for the Microsoft workloads that you monitor. The data it provides helps you measure the experience of your end-users. You can use the Gizmo Web UI to customize how workloads are monitored. For example, you can choose which workloads to monitor, set thresholds for alerts, and configure how you receive notifications about alerts.

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

Workloads

A workload is an application or a resource that you can monitor. Gizmo includes pre-installed monitoring configurations for the following workloads:

- ADFS
- Azure AD Connect
- Exchange DAG
- Exchange Edge Server
- Exchange Mailbox Server
- Exchange Online
- Exchange Online Network
- Hybrid Mail Routing
- Internal Mail Routing
- Office 365 Health
- Office 365 Web Apps
- OneDrive
- Roundtrip Mail Routing
- SharePoint Network
- SharePoint Page
- Skype for Business Voice
- SMTP Gateways
- Teams
- Teams Advanced
- Teams Network
- Teams Video
- URL

Security

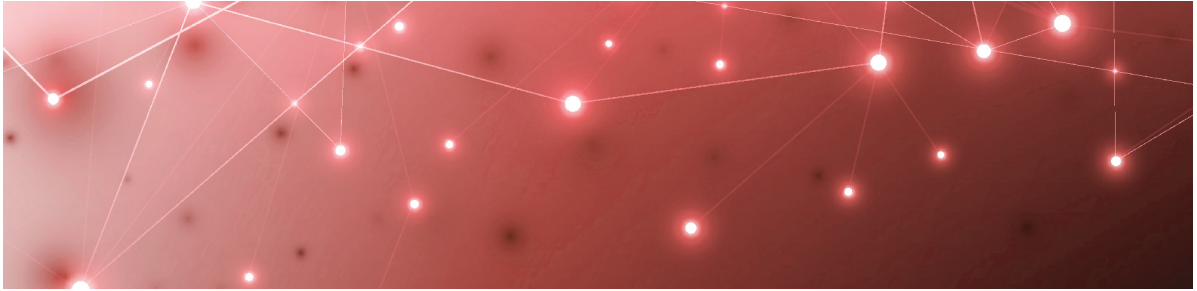
When you configure robots in the Gizmo Web UI, you provide credentials that the robots can use to log into various workloads and perform synthetic transactions. Passwords are stored on disk to persist after a system restart and are encrypted and decrypted on-demand using industry standard encryption.

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

Gizmo 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 Gizmo 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 Gizmo 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 status information. You can use the interface to customize how workloads are monitored by setting thresholds for the performance metrics. Gizmo notifies you when a threshold is met or exceeded. You can choose how you want to receive notifications when the system raises alerts.

The menu options that are available in Gizmo 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 10](#)
- ["Settings" on page 14](#)
- ["Authentication" on page 16](#)

Dashboards

Dashboards provide detailed information such as metrics in order to monitor the health of a specific process. Each dashboard is related to a workload.

Two types of dashboard are available in Gizmo:

- ["System Dashboards" on page 10](#)
- ["Custom Dashboards" on page 11](#)

System Dashboards

System dashboards are dashboards that are available by default in the Gizmo 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

- ## Custom Dashboards
- Create your own custom dashboard so that Gizmo best fits your needs. You can edit custom dashboard when you need to add, resize, move, remove a component, or name the dashboard.

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

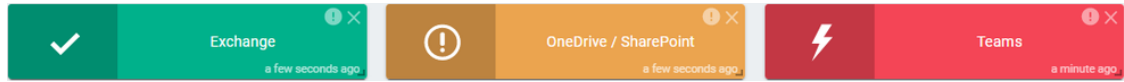
The following image shows an example of a dashboard with its different components.

The screenshot displays the GSX GIZM2 dashboard with a dark blue header and a sidebar on the left. The main content area is divided into several sections:

- Exchange Section:** A green header with a checkmark icon and the text "Exchange" and "a few seconds ago". Below it is a semi-circular gauge chart showing "Performance" at 99.91%.
- 95% of AutoDiscover Execution Time (ms) by Robot:** A bar chart showing execution times for 12 robots. The first robot, "Shanghai-LAN", has a significantly higher execution time (around 600 ms) compared to the others (around 400 ms).
- Average Time per Action (ms):** A line chart showing the average time per action for 12 robots over a period from 10:35 to 11:30. The chart includes a legend with 12 actions: Modern Auth Connection Execution Time (AVG), Create Folder Execution Time (AVG), Delete Folder Execution Time (AVG), Create Message Execution Time (AVG), Upload Attachment Execution Time (AVG), Download Attachment Execution Time (AVG), Remove Attachment Execution Time (AVG), Create Task Execution Time (AVG), Delete GSX Created Tasks Execution Time (AVG), Search Using Filter Execution Time (AVG), Create Meeting Execution Time (AVG), and Query Free/Busy Execution Time (AVG).
- 95% of Exchange actions (ms) by Robot:** A bar chart showing the 95th percentile of exchange actions for 12 robots. The chart shows a distribution of execution times, with some robots having higher values (up to 4000 ms) than others.

- "Status Cards" on page 12
- "Graphs" on page 12
- "Tables" on page 13
- "Time Period" on page 14



Status Cards



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.

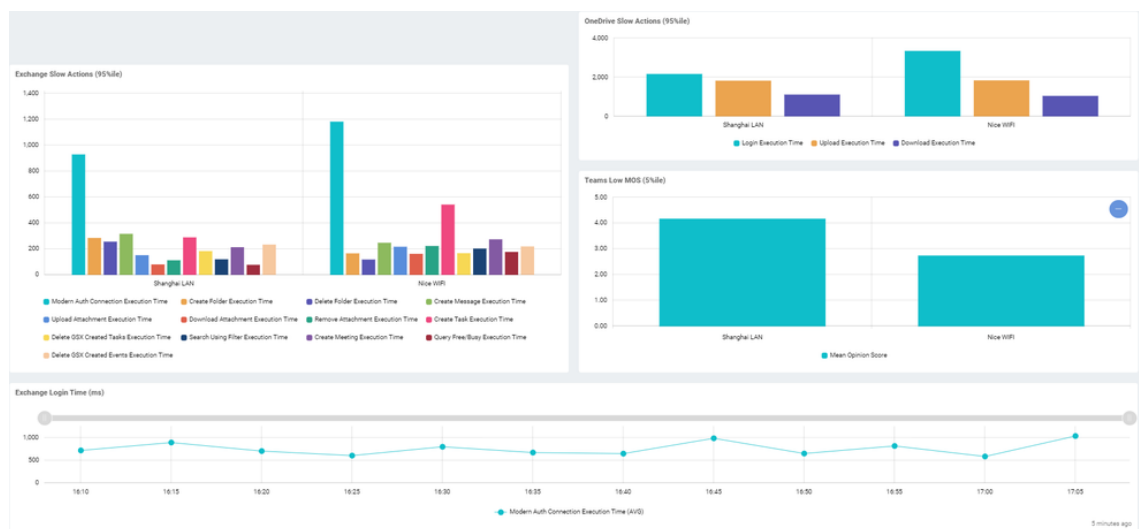
The following functions are available within a status card:

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 clipboard.

Graphs

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

Figure 2: 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.

Gizmo aggregates data in each graph for up to five minutes.

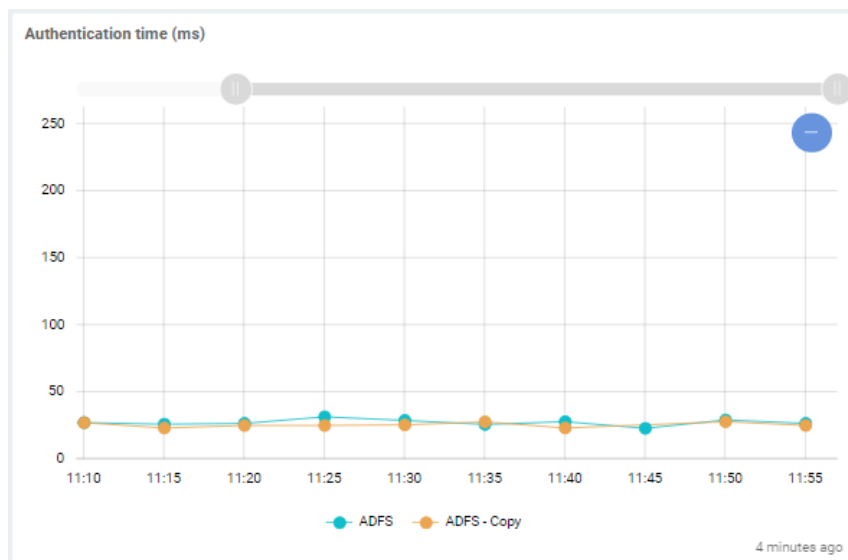
The types of graphs displayed include:

- **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 3: 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 14
- "Delivery Systems" on page 14
- "Robots" on page 15
- "Statuses & Alerts" on page 15
- "Dashboards" on page 16

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 gsx-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 *Gizmo Installation Guide—On-Premises Deployments* and the *Gizmo Installation Guide—Cloud Deployments*, available on the Martello website at the following URL:

<https://martellotech.com/documentation/martello-gizmo/>

Delivery Systems

The Delivery systems page allows you to specify the delivery method that you want Gizmo to use when it sends an alert, and who should receive the alert. For example, you can choose to have alerts 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 delivery systems is created by default and displayed on the Delivery systems page. These default delivery systems are placeholders that you need to edit.

Robots

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

- The robot name and the machine where it is installed.
- The tags related to the robot.
- The configured workloads.
- The enabled or disabled alerts.
- The selected delivery systems.

Gizmo 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 applications (configurations) for each Robot Manager to monitor.
- Manage delivery systems for each Robot Manager.
- Manage tags for each Robot Manager.
- Activate and deactivate alerts for each Robot Manager.

Statuses & Alerts

The Statuses & Alerts page lists the workloads that Gizmo monitors and allows you to configure the following options:

- Whether the health status of the workload is displayed on a dashboard.
- Whether alerts are enabled for the workload.
- Which delivery system to use for alerts.

You can also use this page to create custom statuses and alerts for workloads.

The health status of an application 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 alerts are based on performance metrics. Each metric has a threshold. These thresholds are set to default values that are based on industry standards, but you can configure them based on your needs.

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

From this page, you can perform the following actions on a status:

- Set a delivery system for a workload.
- Activate or deactivate a status to determine whether it displays on a dashboard.
- Activate or deactivate alerts for a workload.
- Add or manage thresholds.
- Add or manage filters.
- Create a custom status with your own configured delivery systems, thresholds, and filters.

Dashboards

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

From the Dashboards management page you can do the following:

- Enable or disable a dashboard.
- Duplicate a system dashboard.
- Remove a custom dashboard.

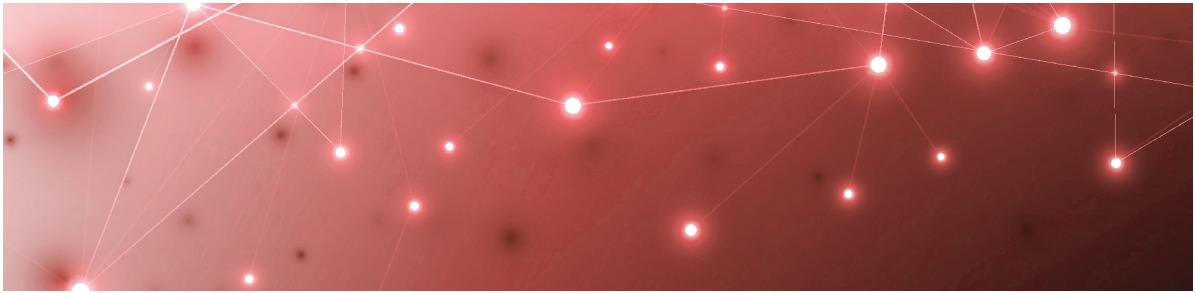
Authentication

You can access the Authentication menu from the gear icon in the top 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 *Gizmo Installation Guide—On-Premises Deployments* and the *Gizmo Installation Guide—Cloud Deployments*, available on the Martello website at the following URL:

<https://martellotech.com/documentation/martello-gizmo/>



Configure Workloads

For each Robot Manager, you need to specify the applications that you want the robots to monitor. Complete the tasks in the following table.

Task	Description
"Select Applications to Monitor" on page 17.	Select the applications that you want each robot to monitor.
"Add a Location Tag" on page 18	Configure location tags to display robots on a map in Power BI.

Select Applications to Monitor

Use this procedure to select the applications that you want the robots at each site to monitor. Perform this procedure on the Gizmo Web UI.

Before you Begin

- This procedure uses local system credentials. If there is a proxy server installed between the Robot Manager machine and Office 365, 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. 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 Office 365, 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.

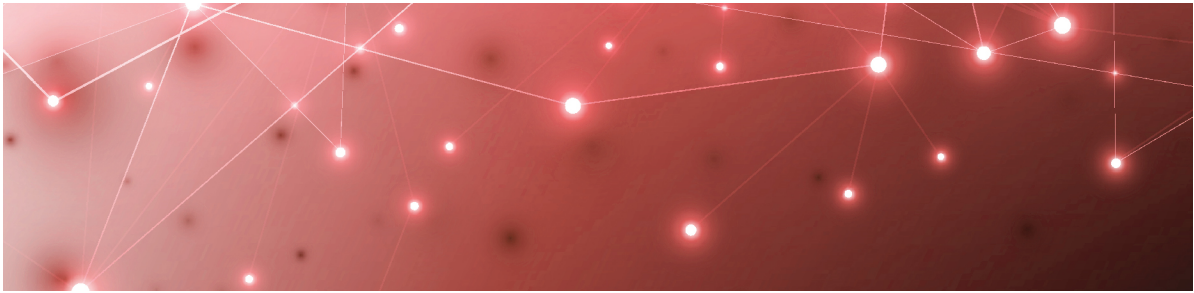
Next Steps

- ["Add a Location Tag" on page 18](#)

Add a Location Tag

Use this procedure to add a tag that indicates the location of your robots. Location tags are required for Power BI to display robots on a map.

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.
5. Click the **+** button to confirm the tag and then click **Add**.



Configure Alerts

Gizmo provides you with proactive alerts so that you can work directly on issues before they become a problem for your business. Administrators can choose who receives alerts and how they are notified.

Alerts are based on default thresholds, but you can configure the thresholds to suit your business needs. For more details on thresholds, see ["Default Thresholds" on page 58](#).

Use the information in this section to complete the following tasks:

Task	Description
"Configure a Delivery System" on page 19	Follow this procedure to configure how Gizmo sends alerts.
"Add a Delivery System to Status Alerts" on page 21	Use this procedure to link an alert to a delivery system.
"Add a Delivery System to Robot Managers" on page 22	Use this procedure to receive health alerts from robot managers.
"Edit Alert Thresholds" on page 23	Follow this procedure to edit the thresholds that trigger an alert.
"Create Custom Statuses and Alerts" on page 23	Duplicate an existing status to create custom status and alert.
"Add Filters" on page 24	Create a filter.
"Apply Filters" on page 24	Apply a filter that groups robots by status.

Configure a Delivery System

Gizmo allows you to configure how to send an alert, and who to send the alert to.

Before you Begin

- Ensure you have the information to fill in the different required fields. Settings vary depending on the delivery system type. For example, you may need login, password and addresses of the alert recipient.

1. Select **Settings > Delivery systems** and click the **Add** button.
2. From the **Add a new delivery system** panel, select the type of delivery system to use, then click **Next**.
 - **Email - EWS**—Select this option if you use an EWS email.
 - **Email - SMTP**—Select this option if you use an SMTP email. This connector does not support anonymous nor non-secured SMTP.
 - **Event Log**—Select this option if you need to capture alert 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. Select Webhook if you need to use another table.
 - **Webhook**—Select this option to manage your incidents or automated tasks with other applications or services. In this example, MS Power Automate is used.
3. Provide the settings for the selected delivery system type, then click **Next**.

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

Delivery System Type	Settings
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.
Service Now	<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 delivery system, then click **Add**.

The page displays the new delivery system in the list.

5. If you need to edit a delivery system:

- Click the **Actions** button for the delivery system that you want to edit.
- Click **Edit**.
- Edit the settings.
- Click **Save** to confirm your changes.

Next Steps

After you create a delivery system, you can perform any of the following tasks:

- ["Add a Delivery System to Status Alerts" on page 21](#)
- ["Add a Delivery System to Robot Managers" on page 22.](#)

Add a Delivery System to Status Alerts

Delivery systems determine how your users receive notifications about alerts. Alerts must be associated with a delivery system. When you install Gizmo, the alerts are configured to work with the default delivery systems. Use this procedure to add or change the delivery systems.

Use this procedure to receive alerts based on status changes.

Before you Begin

You must have configured a delivery system. See ["Configure a Delivery System" on page 19](#).

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



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

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



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

Add a Delivery System to Robot Managers

This procedure allows you to receive health alerts from robot managers.

Before you Begin

You must have configured a delivery system. See ["Configure a Delivery System" on page 19](#).

1. Select **Settings > Robots management** 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 Delivery Systems** button.
The Set delivery systems panel opens.
3. Select the delivery systems to add from the drop-down list. You can add as many delivery systems as you need.
4. Click the **Set Delivery Systems** button to confirm.
The added delivery systems appears in the dedicated Delivery Systems column.



Tip: To remove a delivery system from the robot manager, click the **X** icon in the delivery system label.

Edit Alert Thresholds

Gizmo defines thresholds by default that you can edit, depending on your needs and your environment. Alerts are triggered when a threshold is reached.

Thresholds are defined for each workload. For a list of the default threshold values see ["Default Thresholds" on page 58](#).

1. Select **Settings > Statuses & Alerts Management**.
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.

Create Custom Statuses and Alerts

You can create custom statuses and alerts in Gizmo by duplicating an existing status, editing its details, and adding filters.

To create a custom status, complete the following steps:

1. Select **Settings > Statuses & Alerts Management**.
2. In the **Status Name** column, click the **Actions** button for the workload you want to edit.
3. Click **Duplicate**.
Gizmo 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 thresholds for the workload as required by clicking the **Actions** button and selecting **Edit Status**. You can:
 - Change the name of the status.
 - Edit the delivery system.
 - Edit the thresholds. See ["Edit Alert Thresholds" on page 23](#)
 - Add filters. See ["Apply Filters" on page 24](#)
5. Click **Save** to confirm your changes.
6. Make the custom status available to be used in custom dashboard by toggling the **Enable Status** option to **On**.
7. To activate an alert and send a notification related to the status, click the **bell** icon.

Next Steps

- After you enable the custom status, you can use it to add status data to custom dashboards. See ["Create a New Custom Dashboard" on page 26](#).

Add Filters

You can add tags to Robot Managers and use them as filters to sort and display your configurations.

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

- Apply the filter; see ["Apply Filters" on page 24](#)

Apply Filters

Use this procedure to create filters that group robots by status. You can then receive alerts based on the status of this group.

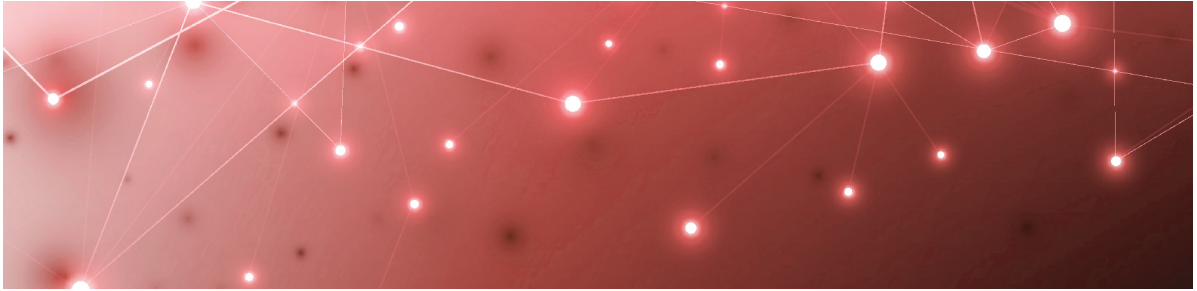
Before you Begin

- Create a tag to use as a filter for the Robot Manager. See ["Add Filters" on page 24](#)
- Create a custom status by duplicating an existing status. See ["Create Custom Statuses and Alerts" on page 23](#).

1. Select **Settings > Statuses & Alerts Management** 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 to use for the filter 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 26](#).



Configure Dashboards

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

Use the information in this section to create custom dashboards:

Task	Description
"Create a New Custom Dashboard" on page 26	Create your own custom dashboards from a blank page.
"Create a Custom Dashboard from a System Dashboard" on page 27	Create a custom dashboard that is based on a system dashboard.
"Enable or Disable Dashboards " on page 28	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.

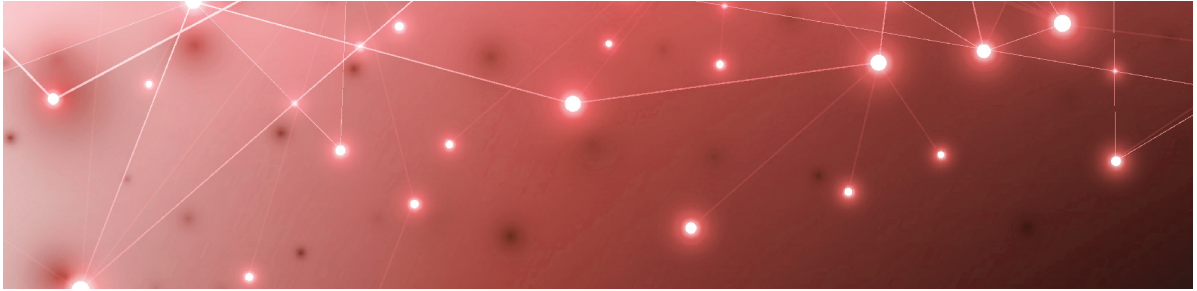
Enable or Disable Dashboards

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.

System dashboards are enabled by default.

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

Gizmo data can be viewed and shared as a Power BI report. Your administrator imports your data into the Gizmo 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:

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

From Power BI you can export the report to the following formats:

- PDF
- PowerPoint
- Excel

If you have a Power BI Pro license and appropriate permissions you can share the report in the following ways:


- As an email.
- In SharePoint Online.
- Embedded in a website or portal.

Gizmo Power BI Report Pages

The Gizmo Power BI report displays Gizmo data in the following report pages.

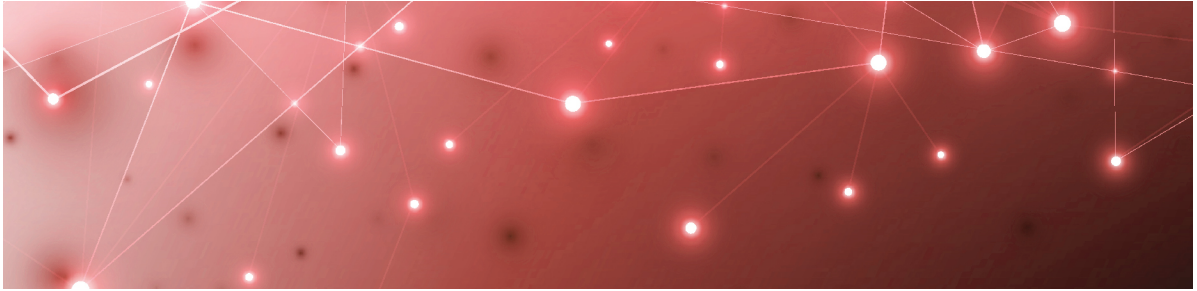
Report Page	Description
Top Level Dashboard	Provides an at-a-glance view of overall performance for the monitored platforms and services by robot location. The performance gauge indicates the percentage of good performance across all of the monitored applications during the selected time period.

Report Page	Description
Exchange UX	<p>An overview of the Exchange end user experience by location. The panels in this report page track user actions within Exchange, such as the time it takes (in milliseconds) to open a mailbox, create an email, download an attachment, or create a meeting.</p> <p>This report page also includes the following basic network metrics: TCP Connect Time, DNS Resolution Time, and Total Packet Loss. These metrics can help determine if performance degradation is related to network issues.</p>
OneDrive/SharePoint UX	<p>An overview of the SharePoint and OneDrive end user experience by location. The panels in this report page track user actions within SharePoint and OneDrive, such as the time it takes (in milliseconds) to log in, upload and download a file, and total execution time.</p> <p>This report page also includes the following basic network metrics: TCP Connect Time, DNS Resolution Time, and Total Packet Loss. These metrics can help determine if performance degradation is related to network issues.</p>
Teams/Skype Voice	<p>An overview of the Teams and/or Skype 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 or Skype is installed.</p> <p>Network metrics, including Packet Loss Rate, Jitter, and Bandwidth Average are included in this report tab to help determine if low MOS metrics are related to network degradation.</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>This report page also includes the following basic network metrics: TCP Connect Time, DNS Resolution Time, and Total Packet Loss. These metrics can help determine if performance degradation is related to network issues.</p>

Report Page	Description
Teams (for export)	<p>Provides detailed call data in tabular format that can easily be exported to share with your networking team for further analysis of call performance. This data can also be filtered by MOS metrics 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>The call data includes the date and time of the calls, the robot location and address, the IP address the robot connected to, packet loss, latency, jitter, bandwidth (estimated, average, max, and min), the protocol used, and MOS, among others.</p>
UX Analysis	An overview analysis of the end user performance issues per service type per location. Key metrics per service type are tracked where poor performance is experienced, and provides a table of the top 100 issues encountered.
Metric Analysis	An overview of the overall health for each service type that displays the performance of key metrics collected for each of the service types.
Mail Routing	<p>An overview of the time it takes in milliseconds, 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>These metrics can also be filtered by location.</p> <div>  <p>Note: Additional mail routing configurations can be supported, but must be customized. Contact support at gsx-support@martellotech.com.</p> </div>

Report Page	Description
Cross Analysis	An extensive list of metrics, grouped by platform, that you can select to report on. This report page also allows you to compare metrics across the different platforms that don't show up together in the other report pages. Use Ctrl-Click to select the metrics to compare. For example, you can compare Exchange login times with SharePoint login time, or how long it takes to download a file in Teams versus SharePoint.
Exchange Server Performance	<p>Provides reporting capabilities across a number performance counter metrics specific to Exchange Servers.</p> <p>This report page is only available in the Full version of the Gizmo Analytics Power BI template.</p>

For additional details about the metrics displayed in the report pages, see ["Metrics Collected" on page 33](#).



Metrics Collected

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

Table 1: Metrics Collected in Dashboards and in Power BI

Workload	Metrics Available	
	Gizmo Dashboard	Power BI
"ADFS" on page 34	•	
"AAD Connect" on page 34	•	•
"Exchange" on page 35	•	•
"Exchange DAG" on page 36	•	
"Exchange Edge" on page 37	•	•
"Exchange Mailbox Servers" on page 37	•	•
"Mail Routing" on page 39	•	•
"Mail Routing Hybrid" on page 40	•	
"MS Service Health" on page 41	•	
"Network" on page 41	•	•
"Office 365 Operations" on page 43	•	•
"Office 365 Web Apps" on page 44		•
"OneDrive" on page 46	•	•
"SharePoint" on page 46		•

Workload	Metrics Available	
	Gizmo Dashboard	Power BI
"Skype for Business" on page 47	•	•
"Teams" on page 48	•	•
"Teams Advanced" on page 51	•	•
"Teams Video" on page 53		•
"URL" on page 57	•	•

ADFS

For the Active Directory Federation Services (ADFS) workload, Gizmo robots pass login parameters to specified ADFS endpoints using HTTP calls to retrieve valid authentication tokens.

The following table lists the metrics that the robots collect.

Table 2: 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	
• 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.

AAD Connect

For the Azure Active Directory Connect (AAD Connect) workload, Gizmo 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 3: 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.

Exchange

Gizmo robots perform the following tests for the Exchange workload using EWS (Exchange Web Services) to connect to an Exchange mailbox to perform the following actions:

- 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 4: Metrics Collected for Exchange

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.
Performance	Indicates the overall health of the Exchange service.

Metric	Description
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 DAG

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

The following table lists the information that the robots collect.

Table 5: 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

Gizmo robots perform the following actions for the Exchange Edge 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 6: Metrics Collected for Exchange Edge

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.
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

Gizmo robots perform the following actions for the Exchange Mailbox Servers 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 7: Metrics Collected for Exchange Mailbox Servers

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>
Mailbox database status	<p>The mailbox database status provides status information about mailbox database copies. 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> <p>At any time the mailbox database status should 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>
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.

Metric	Description
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.

Mail Routing

Gizmo robots perform the following tests for the Mail Routing workload:

- Internal mail routing—the time it takes to send an internal email from one mailbox to another within the same organization (tenant).
- 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 8: Metrics Collected for Mail Routing

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.
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

Use the Mail Routing Hybrid workload if you have both an on-premises Exchange organization and Exchange Online.

For this workload, Gizmo 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 email can be sent by either EWS or SMTP.

The following table lists the metrics that the robots collect.

Table 9: Metrics Collected for Mail Routing Hybrid

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.
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 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
- Microsoft Kaizala
- Planner
- PowerApps in Microsoft 365
- Mobile Device Management for Office 365
- Skype for Business
- Yammer Enterprise
- Office 365 Portal
- Office Subscription
- OneDrive for Business
- Power BI
- SharePoint Online

Network

For the Network workload, Gizmo robots perform the following tests for the Network workload:

- DNS resolution test.
- TCP ping test.






These tests are performed on the following Microsoft 365 services:

- Exchange Online

- SharePoint
- Teams

The following table lists the metrics that the robots collect.

Table 10: 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.
SharePoint: Average Packet Loss (%)	The average percentage of SharePoint packets lost in a 15-second interval.

Metric	Description
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 workload 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 11: Metrics Collected for Office 365 Operations

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.

Office 365 Web Apps

For the Office 365 Web Apps workload, the Gizmo robots simulate an end user's authentication through the Microsoft Login Portal to the Office 365 Web App page using web automation technology.

The following table lists the metrics that the robots collect.

Table 12: Metrics Collected for Office 365 Web Apps

Metric	Description
Connect Time	The time (in milliseconds) it takes to connect to the server to retrieve content and upload files.
DNS Lookup Time	The time (in milliseconds) it takes to resolve the host name. The resolution is measured for each part of the SharePoint page that is built on content from different servers and CDNs.
DOM Content Load Time	The time (in milliseconds) between the initial request and the point when the response is parsed and the DOM/page content is completely loaded.
DOM Interactive Time	The time (in milliseconds) between the initial request and the point when the response is parsed and the DOM/page becomes interactive.
Login Time	The time (in milliseconds) it takes to login to the Microsoft 365 portal.
Page Initial Layout Time	The time (in milliseconds) between the initial request and the point when the response is parsed and displayed, but before any DOM manipulations.
Page Initial Load Time	The initial page loading time (in milliseconds), including all redirects through front-end authorization.
Page Load Time	The time (in milliseconds) it takes to fully load the page.
Page Rendering Time	The time (in milliseconds) between the point when the DOM loading starts and the point when the DOM is completely processed.
Proxy Time	The time (in milliseconds) it takes to connect to the organization proxy server.
SSL Negotiate Time	The time (in milliseconds) it takes to handshake and perform the Secure Sockets Layer negotiation for the connection.

Metric	Description
Time To First Byte	The time (in milliseconds) it takes to get the response first byte. TTFB is a critical measure of how overloaded IIS and SharePoint servers may be in processing and serving up content from Microsoft 365.

OneDrive

Gizmo robots perform the following tests for the OneDrive workload:

- Log in.
- Upload a file.
- Download a file.

The following table lists the metrics that the robots collect.

Table 13: 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.

SharePoint

Gizmo robots perform the following tests for the SharePoint workload:

- Log in.
- Upload a file.
- Download a file.

The following table lists the metrics that the robots collect.

Table 14: Metrics Collected for SharePoint

Metric	Description
Login Time (ms)	The time it takes to log in at each site.
Upload Time (ms)	The time it takes to upload a file at each site.
Download Time (ms)	The time it takes to download a file at each site.
Total Execution Time (ms)	The total time required for robots to perform the test actions at each site.

Skype for Business

Gizmo robots perform test voice calls to collect metrics about the call quality for the Skype for Business workload:

The following table lists the metrics that the robots collect.

Table 15: Metrics Collected for Skype for Business

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

Metric	Description
95%ile PacketLoss, PacketReorder by App	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%.
	The amount of packets that needed to be re-ordered. The packet order needs to be reconstructed when packets arrive in a different order than they were sent. Packet reordering severely degrades the call quality.
	The graph shows that 95% of the time, the packet loss and packet re-ordering were better than the average. The remaining 5% of the time, packet loss and packet re-ordering were worse than the average.
95%ile RTT, Jitter by App	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 indicates 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.
	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.
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.

Teams

Gizmo robots perform the following tests for the Teams workload:

- Log in.

- Voice call.

The following table lists the metrics that the robots collect.

Table 16: 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.
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>

Metric	Description
<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>
<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	<p>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.</p>
10%ile Bandwidth Average by App (Mbit/s)	<p>The graph shows that 10% of the time, bandwidth usage is above the average.</p>

Metric	Description
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

Gizmo 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 17: 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.

Metric	Description
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>
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.

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 Video

For the Teams Video workload, Gizmo robots perform test video calls using web automation to simulate an end user's behavior to log in, authenticate, and retrieve metrics about the video call quality.

The following table lists the metrics that the robots collect.

Table 18: Metrics Collected for Teams Video

Metric	Description
Number of Data Points	The number of data points used to capture metrics.

Metric	Description
Video Average Jitter	<p>The average jitter when sending video packets over the network.</p> <p>Jitter indicates 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 video connection is good. A large jitter value can cause delay in calls and indicates congestion of the network.</p>
Video Max Jitter	<p>The maximum jitter when sending video packets over the network.</p> <p>Jitter indicates 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 video connection is good. A large jitter value can cause delay in calls and indicates congestion of the network.</p>
Outbound Video Packets Lost	The number of outbound video packets lost.
Video Round-Trip Time	Round trip time (RTT) is the time in milliseconds that it takes a video packet to travel from point A to B and return.
Connection Available Outgoing Bitrate	Indicates the available outbound capacity of the network connection. The higher the value, the more bandwidth is available for outgoing data.
Outbound Video FIR Count	The total number of outbound Full Intra Request (FIR) packets sent by this sender.
Outbound Video PLI Count	The total number of outbound Picture Loss Indication (PLI) packets sent by this sender.
Outbound Video NACK Count	The total number of outbound Negative ACKnowledgement (NACK) packets sent by this sender.

Metric	Description
Outbound Video QP Sum	The total number of Quantization Parameter (QP) values of outbound frames encoded by this sender.
Outbound Video Packets Sent	The total number of outbound packets sent.
Outbound Video Retransmitted Packets Sent	The total number of retransmitted packets.
Outbound Video Bytes Sent	The total number of bytes sent.
Outbound Video Header Bytes Sent	The total number of header bytes sent.
Outbound Video Frames Encoded	The total number of video frames encoded by this sender.
Outbound Video Total Packet Send Delay	The total number of seconds that packets have spent buffered locally before being transmitted onto the network.
Outbound Video Quality Limitation Reason	The current reason for limiting the resolution and/or frame rate, or "none" if not limited.
Outbound Video Quality Limitation Resolution Changes	The number of times that the resolution has changed because the quality is limited.
Outbound Video Frames Sent	The total number of frames sent on this RTP stream.
Outbound Video Huge Frames Sent	The total number of huge frames sent by this RTP stream. Huge frames, by definition, are frames that have an encoded size of at least 2.5 times the average size of the frames.
Outbound Video Frame Rate	The outbound video frame rate in frame per second (FPS).
Outbound Video Key Frames Encoded	The total number of key frames successfully encoded for this RTP media stream.

Metric	Description
Inbound Video Jitter Buffer Delay	The total amount of time, in seconds, each video frame takes from the time the first packet is received by the jitter buffer to the time it exits the jitter buffer.
Inbound Video Jitter Buffer Emitted Count	The total number of video frames that have exited the jitter buffer.
Inbound Video Bytes Received	The total number of bytes received on this RTCDataChannel, not including headers or padding.
Inbound Video FIR Count	The total number of inbound Full Intra Request (FIR) packets.
Inbound Video PLI Count	The total number of inbound Picture Loss Indication (PLI) packets.
Inbound Video QP Sum	The total number of the Quantization Parameter (QP) values of inbound frames encoded by this receiver.
Inbound Video NACK Count	The total number of inbound Negative ACKnowledgement (NACK) packets received.
Inbound Video Frames Decoded	The total number of frames correctly decoded for this RTP stream.
Inbound Video Packets Lost	The total number of RTP packets lost for this Synchronization Source (SSRC).
Inbound Video Packets Received	The total number of RTP packets received for this Synchronization Source (SSRC).
Inbound Video Total Interframe Delay	The total amount of interframe delays, in seconds, between consecutively decoded frames, recorded just after a frame has been decoded.
Inbound Video Total Squared Interframe Delay	The total number of squared interframe delays, in seconds, between consecutively decoded frames, recorded just after a frame has been decoded.
Inbound Video Total Freezes Duration	The total duration of rendered frames that are considered as frozen, in seconds. This value is updated when a frame is rendered.

Metric	Description
Inbound Video Total Pause Duration	The total duration of pauses, in seconds. This value is updated when a frame is rendered.
Inbound Video Total Frames Duration	The total duration of all rendered video frames, in seconds. This value is updated when a frame is rendered.
Inbound Video Frames Dropped	The total number of frames dropped prior to decode or dropped because the frame missed its display deadline for this receiver track.
Inbound Video Freeze Count	The total number of video freezes experienced by this receiver.
Inbound Video Pause Count	The total number of video pauses experienced by this receiver. Video is considered to be paused if the amount of time passed since last received packet exceeds 5 seconds.
Inbound Video Frames Received	The total number of complete frames received on this RTP stream. This metric is incremented when the complete frame is received.

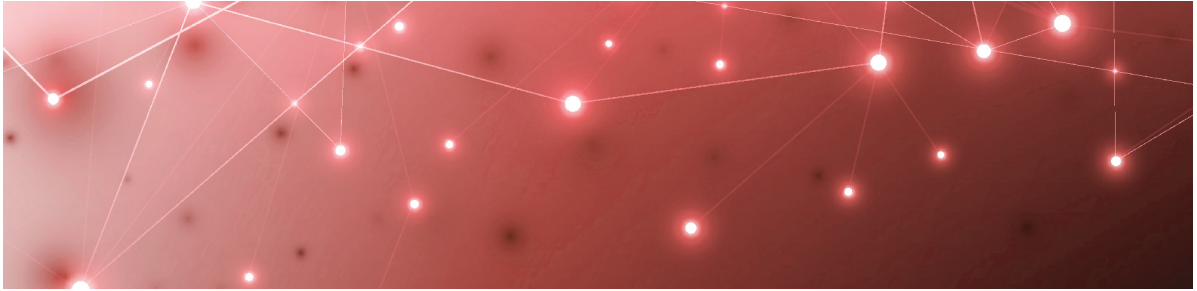
URL

For the URL workload, Gizmo robots perform HTTP calls to a specified URL to retrieve its HTTPS certificate information.

The following table lists the metrics that the robots collect.

Table 19: Metrics Collected for the URL Workload

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.



Default Thresholds

This chapter lists all the thresholds with their value and unit, per workload available in the Web Application.

- ["Exchange Online Thresholds" on page 61](#)
- ["Mail Routing Thresholds" on page 61](#)
- ["OneDrive Thresholds" on page 62](#)
- ["Teams Thresholds" on page 62](#)
- ["URL Thresholds" on page 62](#)

ADFS Thresholds

This table lists all the thresholds available for the ADFS workload.

Table 20: Default Thresholds for ADFS

Threshold Name	Value
ADFSPerformanceThreshold	3000 ms
ADFSCriticalThreshold	5000 ms

Exchange Thresholds

This table lists all the thresholds available for the Exchange workload.

Table 21: Default Thresholds for Exchange

Threshold Name	Value
ExchangeEdgeProcessorTimeThreshold	75 %
ExchangeEdgeRAMThreshold	90 %

Threshold Name	Value
ExchangeEdgePoisonQueueLength-Threshold	5 items
ExchangeEdgeSubmissionQueue-LengthThreshold	300 items
ExchangeEdgeUnreachableQueue-LengthThreshold	100 items
ExchangeEdgeDiskThreshold	10 %

Exchange Mailbox Thresholds

These tables list all the thresholds available for the Exchange Mailbox workload.

Table 22: Default Thresholds for Exchange Mailbox - Client Access

Threshold Name	Value
RPCClientAccessAveragedLatency-TimeThreshold	250 ms
RPCClientAccessRequestsThreshold	40 requests

Table 23: Default Thresholds for Exchange Mailbox - Databases

Threshold Name	Value
DatabaseReadsAttachedAverage-LatencyTimeThreshold	20 ms
DatabaseWritesAttachedAverage-LatencyTimeThreshold	50 ms
DatabaseLogWritesAverageLatency-TimeThreshold	10 ms
DatabaseReadsRecoveryAverage-LatencyTimeThreshold	200 ms
StoreRPCRequestsThreshold	70 requests
ClientTypeRPCAverageLatencyTime-Threshold	50 ms
StoreRPCAverageLatencyTime-Threshold	50 ms

Table 24: Default Thresholds for Exchange Mailbox - System

Threshold Name	Value
DomainControllersLDAPReadTime-Threshold	100 ms
DomainControllersLDAPSearchTime-Threshold	100 ms
ProcessesLDAPReadTimeThreshold	100 ms
ProcessesLDAPSearchTimeThreshold	100 ms
ProcessorPercentageTimeThreshold	75 ms
ProcessorUserPercentageTimeThreshold	75 ms
ProcessorPrivilegedPercentageTime-Threshold	75 ms
ProcessorQueueLengthThreshold	6 items
MemoryCommittedBytesInUse-PercentageThreshold	80 %
NetCLRMemoryGCPercentageTime-Threshold	10 %
NetworkPacketsOutboundErrors-Threshold	0 packet
ASPNetApplicationRestartsThreshold	0 restart
ASPNetWorkerProcessRestarts-Threshold	0 restart
ASPNetRequestWaitTimeThreshold	0 request
ASPNetRequestsInApplicationQueue-Threshold	0 request
ExchangeMailboxDiskThreshold	10 %

Table 25: Default Thresholds for Exchange Mailbox - Transport

Threshold Name	Value
NumberOfMessagesInQueue-Threshold	300 messages

Exchange Online Thresholds

This table lists all the thresholds available for the Exchange Online workload.

Table 26: Default Thresholds for Exchange Online

Threshold Name	Value
ExchangeOnLineCriticalStatus-Threshold	6000 ms
ExchangeOnLinePerformanceStatus-Threshold	4000 ms

Mail Routing Thresholds

These tables list all the thresholds available for the Mail Routing workload.

Table 27: Default Thresholds for Mail Routing - Hybrid

Threshold Name	Value
HybridMailRoutingCriticalThreshold	120000 ms
HybridMailRoutingPerformance-Threshold	30000 ms

Table 28: Default Thresholds for Mail Routing - Internal

Threshold Name	Value
InternalMailRoutingCriticalThreshold	60000 ms
InternalMailRoutingPerformance-Threshold	15000 ms

Table 29: Default Thresholds for Mail Routing - Roundtrip

Threshold Name	Value
RoundtripMailRoutingCriticalThreshold	300000 ms
RoundtripMailRoutingPerformance-Threshold	60000 ms

Table 30: Default Thresholds for Mail Routing - SMTP

Threshold Name	Value
SMTPGatewaysCriticalThreshold	300000 ms
SMTPGatewaysPerformanceThreshold	60000 ms

OneDrive Thresholds

This table lists all the thresholds available for the OneDrive workload.

Table 31: Default Thresholds for OneDrive

Threshold Name	Value
OneDriveCriticalStatusThreshold	9000 ms
OneDrivePerformanceStatusThreshold	6000 ms
OneDriveCriticalStatusDownload-Threshold	5000 ms
OneDrivePerformanceStatusDownload-Threshold	3000 ms

Teams Thresholds

This table lists all the thresholds available for the Teams workload.

Table 32: Default Thresholds for Teams

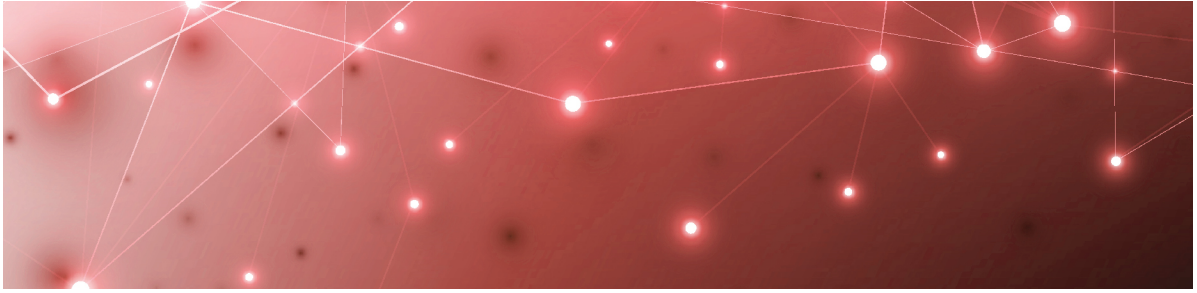
Threshold Name	Value
TeamsCriticalThreshold	3.5 MOS
TeamsPerformanceThreshold	3.8 MOS
TeamsActionTimePerformance-Threshold	6000 ms
TeamsActionTimeCriticalThreshold	9000 ms

URL Thresholds

This table lists all the thresholds available for the URL workload.

Table 33: Default Thresholds for URL

Threshold Name	Value
URLPerformanceThreshold	3000 ms
UrlHttpStatusCodeSuccessThreshold	200 status code



Contact

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



© Copyright 2021, 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.