

MARTELLO



GSX is a subsidiary of
Martello Technologies

Martello Gizmo

INSTALLATION GUIDE — ON-PREMISES DEPLOYMENTS

RELEASE 2.2

DOCUMENT DATE: JULY 16, 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

Installation Guide — On-Premises Deployments
Release 2.2 - July 16, 2021

Contents

CHAPTER 1

Introduction	7
Document Purpose and Intended Audience	7
Revision History	7

CHAPTER 2

About Gizmo	8
Components	8
Gizmo Web UI	8
Gizmo Server	9
Robot Manager Service	9
Robots	9
Workloads	9
Security	11

CHAPTER 3

Deployment Planning	12
Data Comparisons	12
Deployment Examples	14
Monitor Office 365 Workloads at Critical Locations	15
Monitor the Route from Sites to the Cloud	16
Monitor the Full Route to the Cloud	17
Monitor Performance in an Office Building	18
Monitor Cloud Performance	19

CHAPTER 4

Requirements	21
Gizmo Application Requirements	21
Server	21
IIS Roles	22
Antivirus Exclusions	22
Network	23
Supported Browsers	23
SQL Database Requirements	23
RabbitMQ	23
Robot Manager Requirements	24

Machine	24
Antivirus Exclusions	25
Network	25
Accounts	25
Workload Requirements	27
Exchange and Exchange Edge Server Requirements	27
Mail Routing Requirements	28
Security Requirements	28
Power BI Desktop Requirements	28

CHAPTER 5

Installation Process	29
----------------------------	----

CHAPTER 6

Install the Gizmo Application	30
Request a License Code	30
Install Gizmo—Online	31
Install Gizmo—Offline	33
Validate the Installation	35

CHAPTER 7

Configure User Authentication	36
Submit Your Domain	36
Enable HTTPS	37
Configure Single Sign-On	37
Configure Role-Based Access	38

CHAPTER 8

Install the Robot Manager Service	39
Verify Robot Manager Prerequisites	39
Verify Exchange Server and PowerShell Endpoints	40
Install Robot Manager	41

CHAPTER 9

Configure Robot Credentials	42
Edit Monitoring Credentials	43
Add Monitoring Credentials	43

CHAPTER 10

Configure Workloads	44
Create Monitoring Configurations	44
Assign Configurations to Robots	45
Add a Location Tag	46

CHAPTER 11

Deploy Power BI	47
Import the Power BI Template	47
Share a Report Using Power BI Service	48

CHAPTER 12

Upgrade Process	50
Time Requirements	50
Supported Upgrade Paths	50

CHAPTER 13

Upgrade the Gizmo Web UI	51
Migrate Data	51
Retrieve Account and Service Information	52
Upgrade the Application	53
Validate the Upgrade	54
Upgrade the Power BI Template	55

CHAPTER 14

Upgrade the Robot Manager Service	56
Upgrade the Robot Manager Service	56
Validate the Upgrade on the Robot Manager Host	57
Validate the Upgrade on the Gizmo Server	57

CHAPTER 15

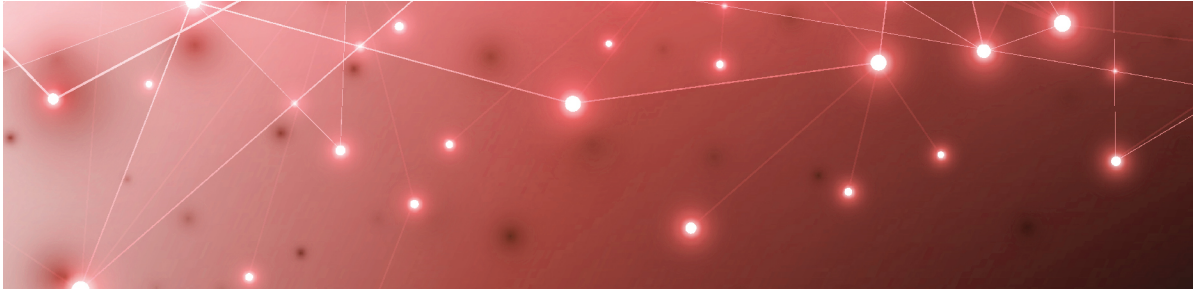
Backup and Restore	59
Back up the Gizmo Environment	59
Restore the Gizmo Web UI	59

CHAPTER 16

Troubleshooting	62
Respond to Error Messages	62
Repair an Installation	64
Submit a Support Ticket	64

CHAPTER 17

Contact	66
---------------	----



Introduction

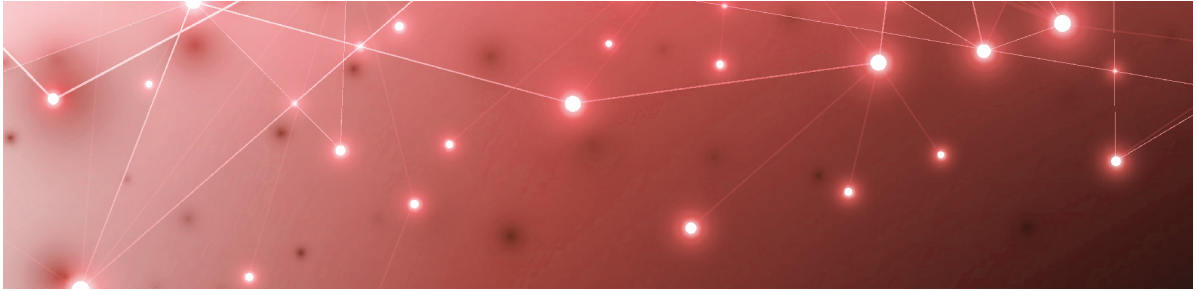
Document Purpose and Intended Audience

This document provides information that enables you to install or upgrade Gizmo. It contains system requirements, installation and upgrade procedures, and steps to configure the system so that it can retrieve data from your Microsoft workloads.

This document is intended for IT system administrators and anyone responsible for installing and configuring Gizmo software. You must have administrator privileges to perform the procedures in this guide.

Revision History

Document Date	Description
July 16, 2021	Martello Gizmo Installation Guide — On-Premises Deployments, Release 2.2



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

Components

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

- ["Gizmo Web UI" on page 8](#)
- ["Gizmo Server" on page 9](#)
- ["Robot Manager Service" on page 9](#)
- ["Robots" on page 9](#)
- ["Workloads" on page 9](#)

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.

Gizmo Server

For on-premises deployments, a Windows server hosts the Gizmo Web UI. In this document, the server is referred to as the Gizmo server, to differentiate it from the machines where the Robot Manager service is running.

When you install the Gizmo Web UI on the server, the executable file also installs RabbitMQ. RabbitMQ is a message-queueing software. Gizmo uses RabbitMQ to receive the results of the tests performed by robots located at your critical business sites. The Gizmo server stores the data it collects in a SQL database.

Robot Manager Service

Robot Manager is a Windows service that you install on machines located at your critical business sites. It manages the robots that perform synthetic transactions at that site. The Robot Manager service sends the results of the synthetic transactions to the Gizmo server using encrypted communication.

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 allows you to create monitoring configurations for the following workloads:

- Active Directory Federation Services (ADFS)
- Azure AD Connect (AAD Connect)
- Exchange DAG
- Exchange Edge Server
- Exchange Free/Busy
- Exchange Mailbox Server
- Exchange MAPI
- Exchange Online
- Exchange Online Network
- Hybrid Mail Routing
- Internal Mail Routing
- Office 365 Health
 - 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
- Office 365 Web Apps
 - 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
- Skype for Business Voice
- SMTP Gateways
- Teams
- Teams Advanced
- Teams Network
- Teams Video
- URL

Security

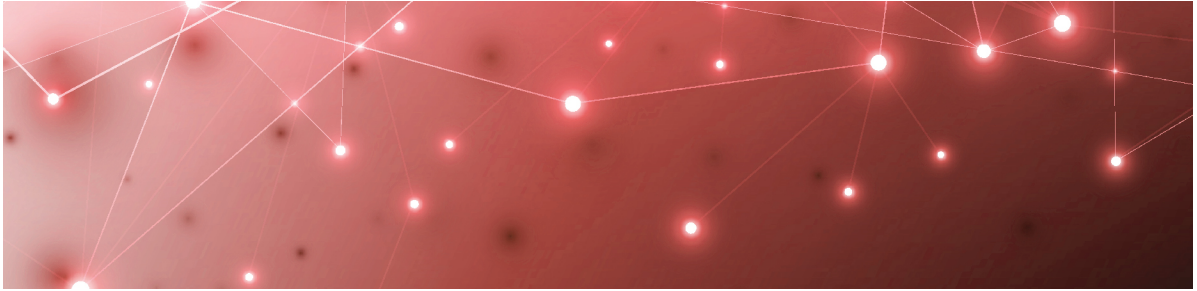
When you configure robots in the Gizmo Web UI, you provide credentials that the robots can use to log into various workloads and perform synthetic transactions. Passwords are stored on disk to persist after a system restart and are encrypted and decrypted on-demand using industry standard encryption.

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.



Deployment Planning

Use the information in the following sections to understand some of the ways that you can use the data that Gizmo collects to measure end-user experience and plan IT projects:

- ["Data Comparisons" on page 12](#)
- ["Deployment Examples" on page 14](#)

Data Comparisons

You can use the data that Gizmo collects to perform A/B comparisons, or to identify trends by comparing data over time.

A/B comparisons are a test method where you compare two versions of something to determine which one performs better. For example, you can compare two routes to the same endpoint in your network to see which route is the most efficient. You can use Gizmo to collect metrics for each network path, and then compare the data. You can compare performance at different sites in your network, or you can compare network performance at remote sites to the performance at the head office.

This comparative approach allows you to understand how your network impacts the end-user experience. It also helps you assess how changes to your infrastructure will affect performance, so that you can plan IT projects with an understanding of how those changes will impact your end users.

The following table lists some examples of how you can deploy robots to make A/B comparisons.

Table 1: Examples of A/B Comparisons

Workload	User Experience	Example Deployments
Exchange Mailbox	Outlook disconnects Mail is delayed	<p>Use Gizmo to test the connectivity to the Exchange server, check the protocols, and check the status of the services and the transport queue.</p> <p>Robots should be deployed as close as possible to the Exchange server so that the server monitoring the workload is not impacted by the network.</p>
Exchange Online	Outlook is slow	<p>Use Gizmo to test the connection between the Exchange Online service and the end user.</p> <p>In this scenario, you could deploy a pair of robots in any of the following locations:</p> <ul style="list-style-type: none">• LAN/WiFi —Compare the connection time for LAN users and WiFi users.• VPN/no-VPN—Compare the connection time for users who connect through a VPN to those who do not use a VPN.• MPLS/direct internet— Compare the connection time for users who connect to the service through your MPLS to those who connect directly through the internet.

Workload	User Experience	Example Deployments
OneDrive	Login in slow	<p>OneDrive performance depends on many network factors, such as the distance between the end user and the host, DNS resolution, and proxy connections.</p> <p>In this scenario, you could deploy a pair of robots to make the following comparisons:</p> <ul style="list-style-type: none"> • ISP1/ISP2—Compare the experience of users who connect through one ISP to the experience of users who connect through a different ISP. • Bandwidth/upgraded bandwidth—Compare the experience of users who connect to the OneDrive host through different service levels.

Time-lapse comparisons allow you to identify trends by comparing data over time. This approach allows you to determine a baseline for performance. You can use this information in several ways. For example, time-lapse information helps you to:

- Identify the root cause of recurring incidents.
- Compare the current performance to your performance targets.
- Understand when the demands on your network are at their peak, and whether your current network performance meets the requirements for new applications.
- Identify bottlenecks and to compare the effects of the bottleneck on each site.

Deployment Examples

The following sections describe some example deployments. Use the information in these sections to help you identify the best locations to deploy robots.

- ["Monitor Office 365 Workloads at Critical Locations" on page 15](#)
- ["Monitor the Route from Sites to the Cloud" on page 16](#)
- ["Monitor the Full Route to the Cloud " on page 17](#)
- ["Monitor Performance in an Office Building " on page 18](#)
- ["Monitor Cloud Performance" on page 19](#)

Monitor Office 365 Workloads at Critical Locations

If you have multiple sites that rely on Office 365, you can deploy robots at critical locations to monitor end-user experience.

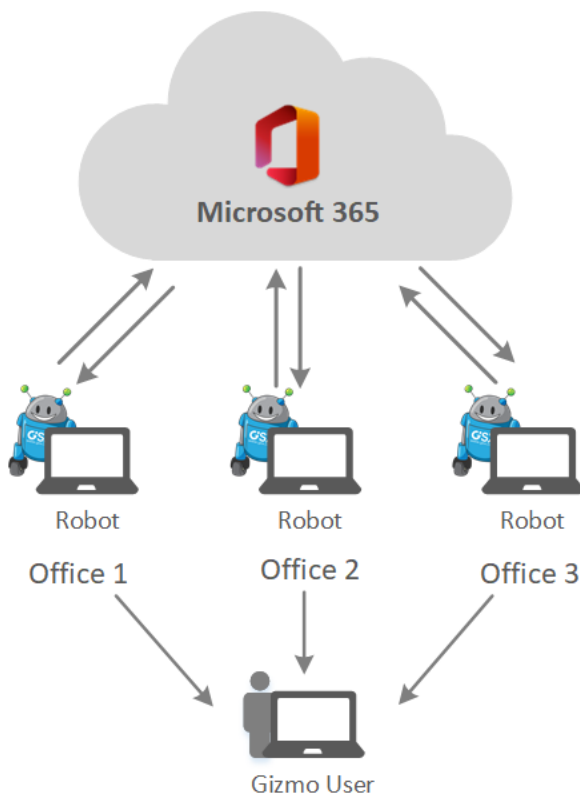
We recommend that you select sites that meet one or more of the following criteria:

- There are a high number of users.
- There are recurring issues.
- There are major IT projects at the site that will improve or affect the user experience.
- You need to measure the user experience to evaluate the return on investment for an IT project.

After you have identified critical locations, deploy one or two Robot Manager services at each site. If you deploy two Robot Manager services, use one to monitor the LAN connection and one to monitor the WIFI connection. This approach allows you to compare the performance of your LAN to the performance of your WIFI connection. If you have a single robot, we recommend that you monitor the LAN connection.

The following image shows an example of this deployment option.

Figure 1: Robot Deployment to Monitor Office 365 at Critical Locations



Monitor the Route from Sites to the Cloud

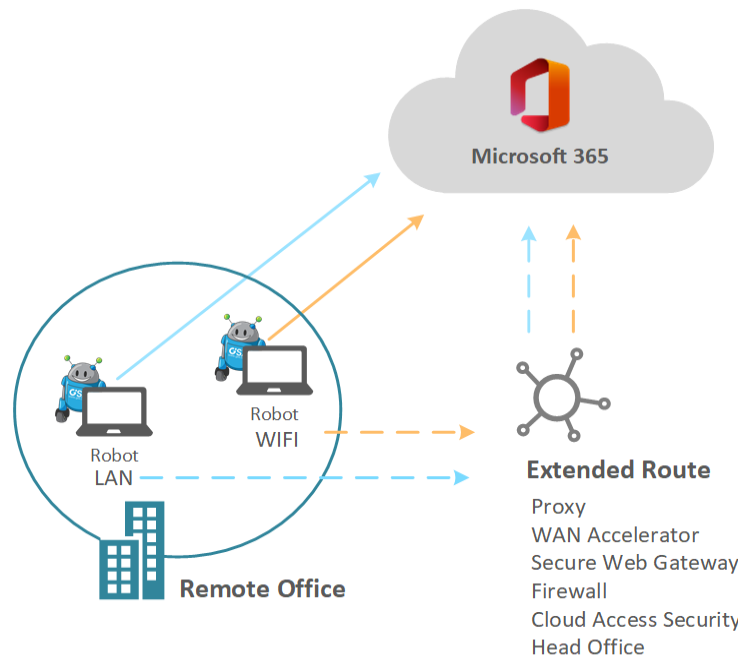
You can use Gizmo to monitor the route between your cloud-based infrastructure and your sites. This type of deployment allows you to analyze remote office connectivity and end-user experience.

To set up this type of deployment, you need to:

- Identify the sites that you want to monitor, and for those sites, identify the components that are part of the local route to the cloud, such as routers, proxy servers, or security gateways.
- Deploy the following robots at the sites:
 - Two robots to monitor the LAN connection: one robot monitors the egress directly to internet, and one robot monitors the route through the components.
 - Two robots to monitor the WIFI connection: one robot monitors the egress directly to internet, and one robot monitors the route through the components.
- Deploy a robot on a virtual machine in your cloud infrastructure.

The following image shows an example of this deployment option.

Figure 2: Robot Deployment to Monitor Routes from Sites to the Cloud



This approach allows you to use the data collected by the robots to compare the performance of your LAN to the performance of your WIFI connection. Comparing the direct egress to the route through the components allows you to understand how your network components impact the end-user experience. This information also helps you assess how changes to your infrastructure will affect users.

After the assessment is complete and you have optimized the route, we recommend that you use only two Robot Manager services at each site: one to monitor the LAN, and one to monitor the WIFI connection. This approach provides basic service quality monitoring at each location.



Note: This option allows you to assess the full route to the cloud; it does not provide information about specific parts of the route. To monitor the full route to the cloud, see ["Monitor the Full Route to the Cloud "](#) on page 17.

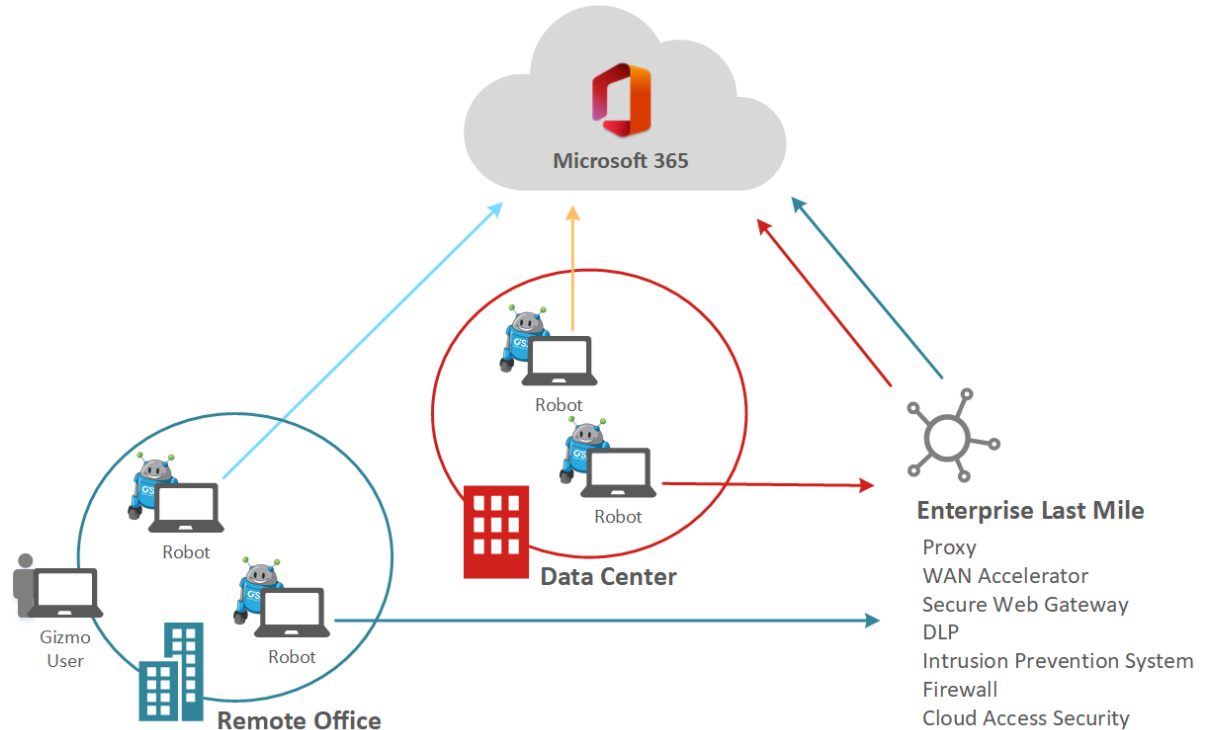
Monitor the Full Route to the Cloud

You can use Gizmo to monitor the route between your cloud-based infrastructure, your head office, and your remote sites. This type of deployment is beneficial if performance improvement is a higher priority than monitoring services geographically.

To set up this type of deployment, you need to:

- Identify the remote sites that you want to monitor, and for those sites, identify the components that are part of the local route to the cloud. For example, identify any routers, proxy servers, or security gateways at each site.
- Identify the components that are part of the route to the cloud at the head office. These components are typically last mile security components, such as proxy servers, WAN accelerators, secure web gateways, data loss prevention, intrusion prevention systems, firewalls, and cloud access security.
- Deploy a robot on a virtual machine in your cloud infrastructure.
- Deploy the following robots at your remotes sites:
 - Two robots to monitor the LAN connection: one robot monitors the egress directly to internet, and one robot monitors the route through the components.
 - Two robots to monitor the WIFI connection: one robot monitors the egress directly to internet, and one robot monitors the route through the components.
- Deploy the following robots at the head office:
 - One robot that accesses Office 365 through your last mile security.
 - One robot that bypasses your last mile security, and instead relies on Office 365 security.

The following image shows an example of this deployment option.

Figure 3: Robot Deployment to Monitor the Full Route to the Cloud

This approach allows you to use the data collected by the robots to make the following assessments:

- **Remote sites**—You can compare the performance of your LAN to the performance of your WIFI connection. You can also compare the direct egress route to the route through your network components. Comparing the direct egress to the route through the components allows you to understand how your network components impact the end-user experience. This information also helps you assess how changes to your infrastructure will affect users.
- **Head office**—Compare the direct egress route to the route through the last mile components. This comparison helps you understand how different layers of security affect the end-user experience.
- **Connectivity between sites**—Compare the routes from your remote sites to the routes from your head office to understand how the MPLS connection affects the end-user experience.

After you have completed the assessment and optimized the routes, we recommend that you use only two robots at each of your remote sites: one to monitor the LAN, and one to monitor the WIFI connection. This approach provides basic service quality monitoring at each location.

Monitor Performance in an Office Building

You can use Gizmo to monitor the performance of workloads on each floor of an office building. This option allows you to analyze how the network on each floor affects the end-user experience. It also simplifies troubleshooting, since the data

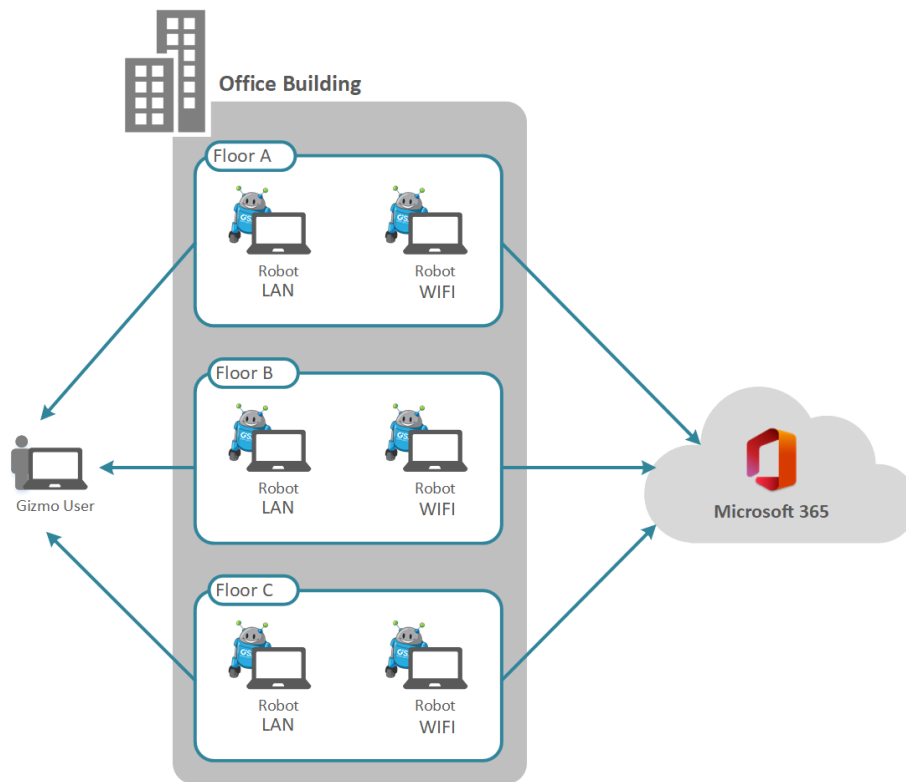
collected by the robots is specific to each floor. You can extend this deployment to include last mile connectivity checks.

To set up this type of deployment, you need to:

- Identify the office site that you want to monitor, and the floors that you consider critical.
- Identify the workloads that you want to monitor.
- Deploy at least one robot for each floor. We recommend that you deploy two robots for each floor. If you deploy two robots, use one to monitor the LAN connection and one to monitor the WIFI connection. This approach allows you to compare the performance of your LAN to the performance of your WIFI connection.

The following image shows an example of this deployment option.

Figure 4: Robot Deployment in an Office Building



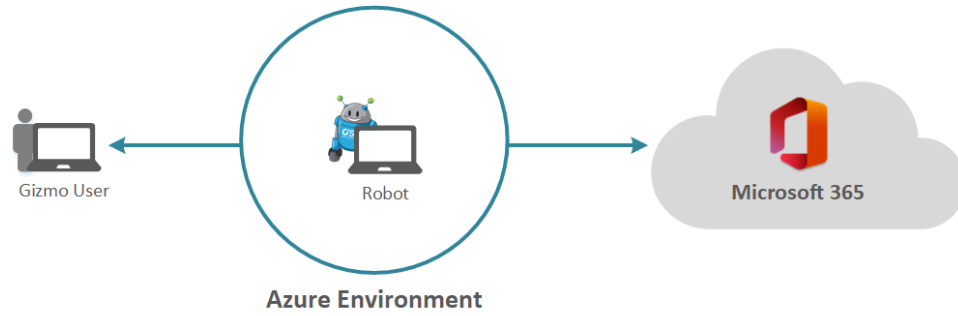
Monitor Cloud Performance

You can use Gizmo to monitor the Microsoft services that are delivered to your sites. This type of deployment allows you to be aware of service degradation immediately, before receiving an alert from Microsoft. It also allows you to understand typical quality of service that you receive.

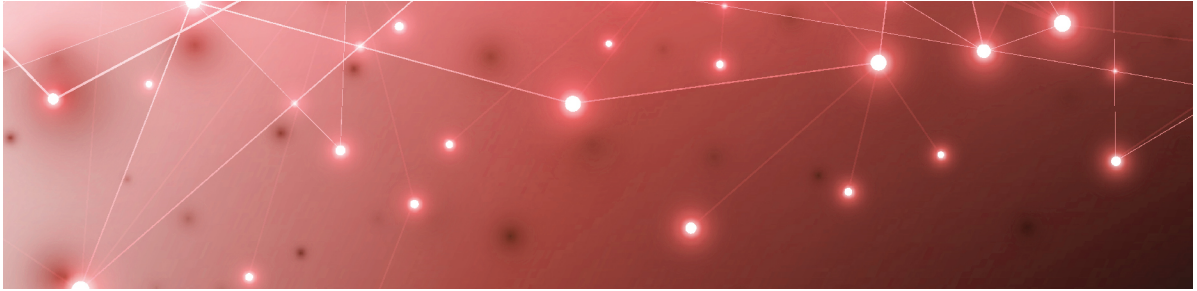
To set up this type of deployment, you need to deploy a robot on a virtual machine in your cloud-based infrastructure.

The following image shows an example of this deployment option.

Figure 5: Robot Deployment to Monitor Cloud Performance



This deployment option does not test performance from actual user locations.



Requirements

The following sections provide information about the requirements that your system must meet before you can install or upgrade Gizmo.

- ["Gizmo Application Requirements" on page 21](#)
- ["SQL Database Requirements" on page 23](#)
- ["Robot Manager Requirements" on page 24](#)
- ["Workload Requirements" on page 27](#)
- ["Security Requirements" on page 28](#)
- ["Power BI Desktop Requirements" on page 28](#)

Gizmo Application Requirements

The following sections list the requirements that your system must meet before you install the Gizmo application.

- ["Server" on page 21](#)
- ["IIS Roles" on page 22](#)
- ["Antivirus Exclusions" on page 22](#)
- ["Network " on page 23](#)

Server

The Gizmo application runs on a Windows server. The following table lists the minimum requirements and recommendations for the server.

Table 2: Gizmo Server—Requirements and Recommendations

Component	Minimum Requirement	Recommended
Windows Server	2016	2019
Memory	8 GB	16 GB (if Power BI Desktop will import data from this server)
Processors	4	4
Available Drive Disk Space	150 GB	150 GB
.NET Framework	4.6.2 or higher	4.6.2 or higher

IIS Roles

Ensure that you add the roles listed below to your Gizmo server:

- Websocket Protocol Enable
- IIS .Net Core Runtime 3.1 Module (Hosting Bundle)
- IIS URL Rewrite Module
- IIS Application Request Routing Module

Antivirus Exclusions

We recommend that you exclude the processes, directories, and ports listed below from the items scanned by your antivirus software.

Processes:

- Gsx.Microservice.Alert
- Gsx.Microservice.DataTier
- Gsx.Microservice.Preprocessing
- Gsx.Microservice.ScanConfiguration
- Gsx.Microservice.StatusCalculation

Directories:

- C:\ProgramData\GSX Solutions*
- C:\Program Files\GSX Solutions*

Ports:

- 60000-60005

Network

The Robot Manager must be able to reach Gizmo server on the following ports:

- TCP 5671 (5672) for AMQP protocol and connect to RabbitMQ.
- TCP 80 (443) for HTTP communication in order to download .zip files.

Ensure that the following URLs are accessible from the server:

- Security Token Service (<https://sts.windows.net/{tenant-id}>)
- Azure sign-in page (<https://login.microsoftonline.com/{tenant-id}>)
- Microsoft graph API (<https://graph.microsoft.com/v1.0/me/transitiveMemberOf/>)

Supported Browsers

Users can use any of the following browsers to access the Gizmo application:

- Chrome
- Firefox
- Edge (Chromium based)

SQL Database Requirements

Ensure that the SQL database meets the following requirements:

- The SQL database server is not collocated on the Gizmo server.
- The version is SQL 2017 or 2019—Standard, Enterprise or Azure SQL.
- SQL Authentication and Windows authentication are supported.
- The database password must not start with a hyphen or special characters.
- The Gizmo server must be able to communicate with the SQL database on port 143 (the default port).
- A new database is added for use during the installation.
- The database must have the db_owner role assigned to it.
- Optional, but recommended: SQL Management software, such as Azure Data Studio, or SQL Server Management Studio.

RabbitMQ

When you install the Gizmo application, the installer prompts you to install RabbitMQ. The installer uses the FQDN of this server as the host. The default username is `gizmo` and the password based on letters and numbers is randomly generated.

If you have an existing installation of RabbitMQ that you plan to use with Gizmo, ensure that the password does not start with a hyphen or other special characters.

Robot Manager Requirements

The following sections provide information about the requirements for the machine where the Robot Manager is installed.

- ["Machine" on page 24](#)
- ["Antivirus Exclusions" on page 25](#)
- ["Network " on page 25](#)
- ["Accounts" on page 25](#)

Machine

Robot Manager is a service that runs on Windows. The following table lists the minimum requirements and recommendations for the machine where the Robot Manager service is installed.

We recommend that you install the Robot Manager service on a machine that is as similar as possible to the machines used by your end users. This practice helps ensure that the performance data collected by the robots is realistic and reflects the experience of your end users. It also helps you determine if anything included in your standard deployment is impacting the performance of the service.

Table 3: Robot Manager Server—Requirements and Recommendations

Component	Minimum Requirement	Recommended
Operating System	Windows 10	—
Memory	4 GB	8 GB or higher is recommended for most environment.
Processors	2.5 GHz Dual Core	2.5 GHz Dual Core is acceptable for most workloads, with exception of Web Automation like Teams Video, which may require additional CPU.
PowerShell	4.0	4.0 or higher
.NET Framework	4.7.1	4.7.1 or higher
Power settings	Always On	—

Antivirus Exclusions

We recommend that you exclude the process and directories listed below from the files scanned by your antivirus software.

Processes

- Gsx.Robot
- Gsx.RobotManager

Directory

- C:\Program Files (x86)\GSX Solutions*

Ports

- Ports 51000 to 65535

URLs

- The following URLs must be accessible:
<https://<customername>.ongsx.com/Downloads/>*
- The following URLs must be accessible: <https://<gizmo-server-fqdn>/downloads/>*

Network

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

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


The Robot Manager must be able to reach your the Gizmo server on the following ports:

- TCP 5671/5672
- TCP 80/443

Accounts

The Robot Manager service requires one or more user accounts that are dedicated to monitoring. The account must have a valid Office 365 E3 license in order to monitor the workloads. To avoid interruptions in data collection, we recommend that you disable multi-factor authentication for these accounts, and that you do not set a password expiry. The number of accounts you need depends on the workload that you are monitoring and the number of robots that you deploy:

Workload	Account Information
Exchange Free/Busy	<p>A user account with a provisioned mailbox and a set timezone.</p> <p>An attendee user account with a provisioned mailbox and set timezone.</p> <p>The first user should have the rights to check the free/busy status of the attendee. If the user accounts are in different organizations, the attendee's organization calendars must be accessible from the organizer's organization.</p>
Exchange Online	Up to 30 robots can use one account. You need a user account with a provisioned mailbox and a set timezone.
Exchange Server	The user account that connects to the Exchange server must be a member of the "View-Only Organization Management" security group in the Active Directory.
Exchange MAPI	<p>A user account with a provisioned mailbox and a set timezone.</p> <p>An attendee user account with a provisions mailbox and set timezone.</p> <p>The first user should have the rights to check the free/busy status of the attendee. If the user accounts are in different organizations, the attendee's organization calendars must be accessible from the organizer's organization.</p>
Mail Routing	A user account with a provisioned mailbox and a set timezone.
Office 365 Web Apps	<p>A user account with the intended Office 365 application provisioned.</p> <ul style="list-style-type: none"> • The account must be cloud-only (ADFS is not supported) • The account must be licensed for the intended Office 365 application
One Drive	<p>Up to 30 robots can use one account.</p> <p>A user account with OneDrive provisioned.</p>

Workload	Account Information
Teams/Teams Advanced	<p>Up to five robots can use one account.</p> <p>You need two user accounts.</p> <ul style="list-style-type: none"> • The accounts must be licensed for Teams • The accounts must belong to same tenant • A private team is automatically created at the first scan of a robot. The user accounts must be set as the team admins. <div>  <p>Tip: If you are monitoring Teams Advanced from multiple locations, use separate credentials for the robots at each location.</p> </div>
Teams Video	<p>You need two accounts per robot.</p> <ul style="list-style-type: none"> • The accounts must be cloud only, as ADFS is not supported. • The accounts must be licensed for Teams. • The accounts must belong to the same tenant. • The accounts must have provisioned calendars.

Workload Requirements

The following sections provide information about the requirements that workloads must meet in order to be correctly monitored.

- ["Exchange and Exchange Edge Server Requirements" on page 27](#)
- ["Mail Routing Requirements" on page 28](#)

Exchange and Exchange Edge Server Requirements

This section lists the requirements that your Exchange and Exchange Edge servers must meet so that Gizmo can monitor the workload. These requirements are applicable to on-premises installations.

Ensure that Gizmo can communicate with the Exchange server by meeting at least one of the following conditions:

- The machine where Gizmo is installed and the Exchange server are in the same domain. If the machines are in different domains, ensure that you configure the Exchange server's domain to trust the Gizmo machine's domain.
- The connection relies on SSL authentication.

- The Exchange server is part of the Gizmo station's WinRM trusted hosts:
`Set-Item wsman:\localhost\client\trustedhosts *` where `*` means all servers.

The following requirements apply to the monitored Exchange Server:

- Make sure the port 5985 (5986 if SSL) is open on the monitored server (Microsoft.PowerShell endpoint).
- Configure the server to receive remote commands:
`Enable-PSRemoting -Force`
- Increase the default values of the following throttling policies or set them to unlimited:
 - The `PowerShellMaxRunspaces` policy is closely related to PowerShell sessions initiated on the servers. By default, it is set to 18.
 - The `PowerShellMaxConcurrency` policy defines the maximum number of concurrent PowerShell connections on the server. By default, it is set to 18.

Mail Routing Requirements

The Mail Routing workload is supported on server versions 2016, 2019 and Online.

Security Requirements

The machine where the Robot Manager is installed must have a certificate under the Computer Local Certificates. During the Robot Manager installation, a self-signed certificate is automatically installed in the "Personal" certificate store. This certificate is used to encrypt communication between Gizmo and the Robot Manager using the certificate's Private/Public keys.

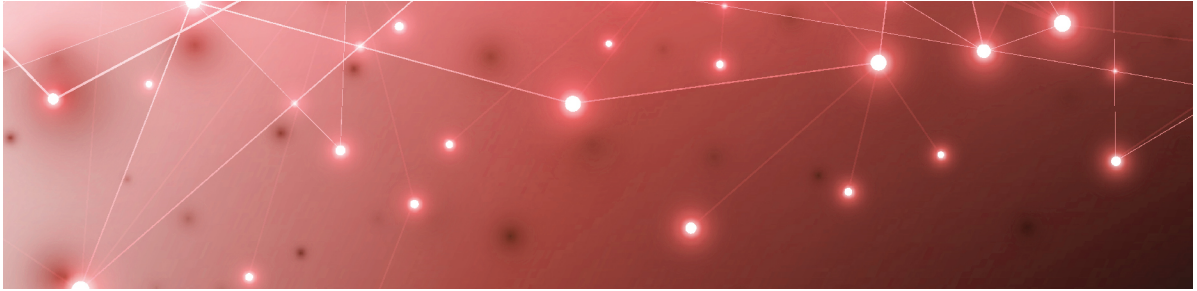


Note: We recommend that you use the default installation procedure. This ensures that each Robot Manager has a different certificate, which enhances security.

Power BI Desktop Requirements

The machine used for Power BI Desktop requires the following:

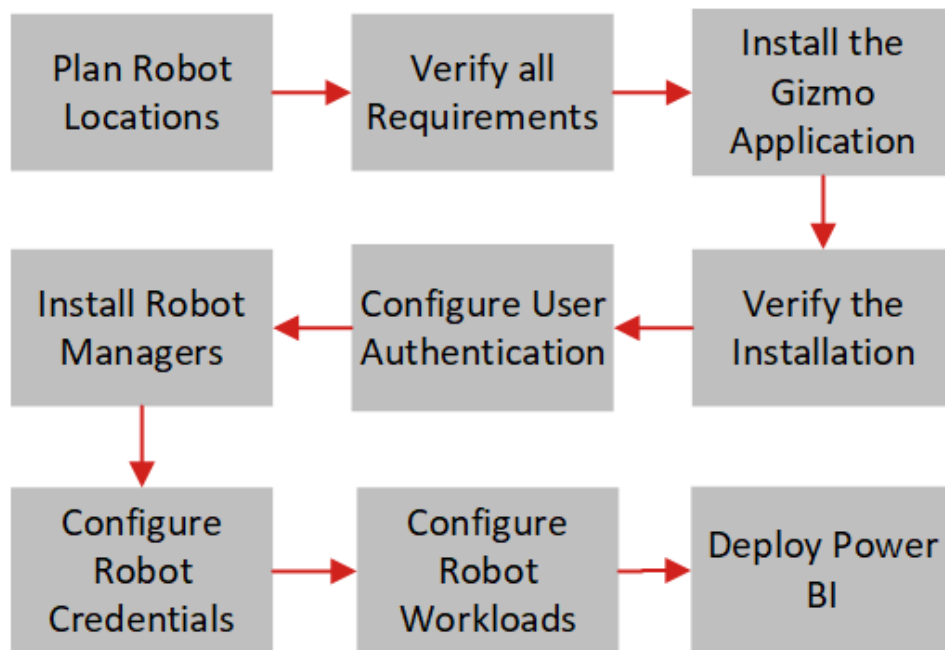
- 4 CPUs
- 8GB of RAM (16GB recommended for large deployments)

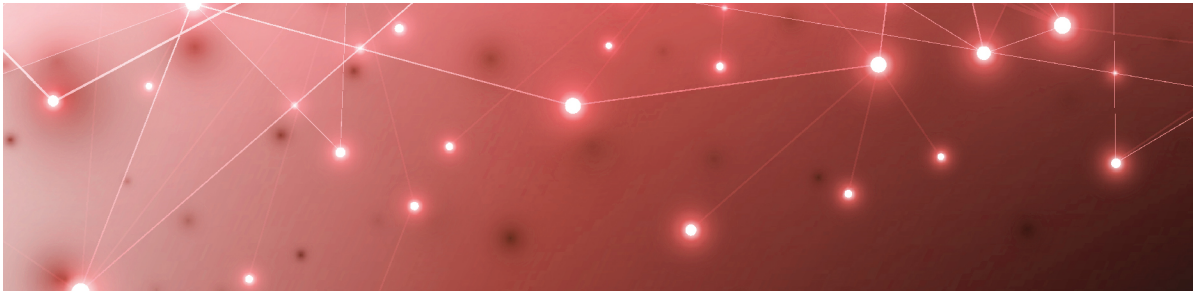


Installation Process

Refer to the following diagram for an overview of the Gizmo installation process.

Figure 6: Installation Process





Install the Gizmo Application

Use the procedures in this section to install the Gizmo application.

Before you Begin

- Ensure that your system meets all the prerequisites listed in "[Gizmo Application Requirements](#)" on page 21.
- Request the installation package from the Martello website at: <https://martellotech.com/documentation/martello-gizmo/>

The installation package contains the following:

- Installer
- Validation script
- Migration scripts
- Power BI template

After you download the installation package, complete the following tasks:

Task	Description
"Request a License Code" on page 30	Obtain a license code. We recommend that you perform this procedure several days in advance of your installation.
Choose one of the following options: <ul style="list-style-type: none">• "Install Gizmo—Online" on page 31• "Install Gizmo—Offline" on page 33	Follow the procedure for online installation if the server has internet connectivity; otherwise, follow the procedure for offline installation.
"Validate the Installation" on page 35	Ensure that the installation was successful.

Request a License Code

Use this procedure to obtain a license code.

Before you Begin

Ensure you perform this procedure on the server where the Gizmo application is installed.

1. Open the PowerShell console.
2. Get the Gizmo Server's ID using the PowerShell cmdlet `Get-GSXMachineID`.
3. Send the ID via email to your dedicated Martello Gizmo delivery engineer. You will receive a license code in return.
4. Apply this License code using the PowerShell cmdlet `Set-GSXLICENSECODE <license code>` where `<license code>` is the license code that applies on the Gizmo server.
A `True` returned value indicates that the license has been successfully applied.

Install Gizmo—Online

Use this procedure to install Gizmo when the server has internet connectivity. You must have administrator privileges on the server to perform this installation.

If you encounter any error messages during the installation, refer to ["Respond to Error Messages" on page 62](#)

Before you Begin

- Ensure that you have the `GSX.Gizmo.<major_version>.<minor_version>.<patch_version>.<build_number>.exe` file available.
- Ensure that the server has access to the following URL:
`https://gsxdownloads.blob.core.windows.net/downloads/` This site contains sub-components required for the installation of underlying third-party tools and libraries.
- Ensure that you are logged in with a local user profile and not a roaming profile. A local profile is stored directly on the computer, whereas a roaming profile is stored on a network server.
- Ensure that there are no open PowerShell sessions.



Note: During the installation process, pop-up messages may display and prompt you to open an executable file. If this occurs, click **Cancel** to dismiss the pop-up message and continue to follow the installation wizard.

1. Right-click the `GSX.Gizmo.<version>.exe` file and select **Run as Administrator**.
2. Review the **End User License Agreement** and click **Next** to accept it.
3. On the **Install folder** screen, select the location where you want to install Gizmo and click **Next**.

4. On the **Service Account** screen, choose one of the following **Built-in accounts** to run the services and then click **Next**:

- Local System (Default)
- Local Service
- Network Service
- Other

We recommend that you use the Local System (Default) account. If you use Windows Authentication to access SQL, you must select Other and provide credentials for a user that has permission to access the database.

5. On the **IIS Website** screen, configure the following settings and then click **Next**:

- **Website name**
- **Application pool**
- **Built-in account**—This is the account that runs the IIS Website. Select **Other**.

6. On the **Database Connection** screen, configure the following settings and then click **Next**:

- **Database Server**—Click **Load** to use the existing database server.
- **Database**—The newly added SQL database.
- **User**—The username for the database owner of the newly added database. This can be the SA (SQL Authentication) or the Windows credentials, depending on how the database user was configured.
- **Password**—The password for the database owner of the newly added database.
- **Install SQL Server 2017 Express**—For trail versions only. Select the checkbox to install SQL Server 2017 Express. When you select this option, the default username is gizmo and the password is randomly generated.

7. On the **RabbitMQ Connection** screen, configure the following settings and then click **Next**:

- **Host**
- **Port**
- **SSL**—Select the checkbox to use SSL. The default port is 5671.
- **Virtual Host**
- **User**
- **Password**
- **Install RabbitMQ 3.8.1**—Select this checkbox to install RabbitMQ. The installer uses the FQDN of this server as the host. The default username is gizmo and the password is randomly generated.

8. On the **GSX Downloads** screen, set the locations of the **Downloads** folder and the **Downloads URI** and click **Next**.

We recommend that you use the default values for both of these settings.

9. Review the information on the **Ready to install** screen and click **Install**.

10. When the installation is complete, you must restart the computer for the changes to take affect. We recommend that you wait for up to 2 minutes before you click the **Restart** button or restart the computer manually.
11. Clear the browsing cache in order to display updated data.

Install Gizmo—Offline

You can download the installation files for Gizmo and then perform the installation at a time when the server is offline. Use this procedure if you want to perform an offline installation.

You must have administrator privileges on the server where you are performing the installation. If you encounter any error messages during the installation, refer to ["Respond to Error Messages" on page 62](#)

Before you Begin

- Ensure that you are logged in with a local user profile and not a roaming profile. A local profile is stored directly on the computer, whereas a roaming profile is stored on a network server.
- Ensure that there are no open PowerShell sessions.
- Obtain the installation package from Martello:
<https://martellotech.com/documentation/martello-gizmo/>
- After you download the archive, make sure you unblock it before you extract the files:
 - Right-click on the archive file.
 - Click **Properties**.
 - Select the **Unblock** checkbox.
 - Click **OK**.



Note: During the installation process, pop-up messages may display and prompt you to open an executable file. If this occurs, click **Cancel** to dismiss the pop-up message and continue to follow the installation wizard.

1. Right-click the `GSX.Gizmo.<version>.exe` file and select **Run as Administrator**.
2. Review the **End User License Agreement** and click **Next** to accept it.
3. On the **Install folder** screen, select the location where you want to install Gizmo and click **Next**.
4. On the **Service Account** screen, choose one of the following **Built-in accounts** to run the services and then click **Next**:
 - Local System (Default)

- Local Service
- Network Service
- Other

We recommend that you use the Local System (Default) account. If you use Windows Authentication to access SQL, you must select Other and provide credentials for a user that has permission to access the database.

5. On the **IIS Website** screen, configure the following settings and then click **Next**:
 - **Website name**
 - **Application pool**
 - **Built-in account**—This is the account that runs the IIS Website. Select **Other**.
6. On the **Database Connection** screen, configure the following settings and then click **Next**:
 - **Database Server**—Click **Load** to use the existing database server.
 - **Database**—The newly added SQL database.
 - **User**—The username for the database owner of the newly added database. This can be the SA (SQL Authentication) or the Windows credentials, depending on how the database user was configured.
 - **Password**—The password for the database owner of the newly added database.
 - **Install SQL Server 2017 Express**—For trial versions only. Select the checkbox to install SQL Server 2017 Express. When you select this option, the default username is gizmo and the password is randomly generated.
7. On the **RabbitMQ Connection** screen, configure the following settings and then click **Next**:
 - **Host**
 - **Port**
 - **SSL**—Select the checkbox to use SSL. The default port is 5671.
 - **Virtual Host**
 - **User**
 - **Password**
 - **Install RabbitMQ 3.8.1**—Select this checkbox to install RabbitMQ. The installer uses the FQDN of this server as the host. The default username is gizmo and the password is randomly generated.
8. On the **GSX Downloads** screen, set the locations of the **Downloads** folder and the **Downloads URI** and click **Next**.

We recommend that you use the default values for both of these settings.
9. Review the information on the **Ready to install** screen and click **Install**.
10. When the installation is complete, you must restart the computer for the changes to take affect. We recommend that you wait for up to 2 minutes before you click the **Restart** button or restart the computer manually.
11. Clear the browsing cache in order to display updated data.

During the installation, the wizard prompts you to select files from the archive that you downloaded.

12. Navigate to the `GSX.Gizmo.<version>_Offline_Requirements` folder and select the specified `.exe` file.

Validate the Installation

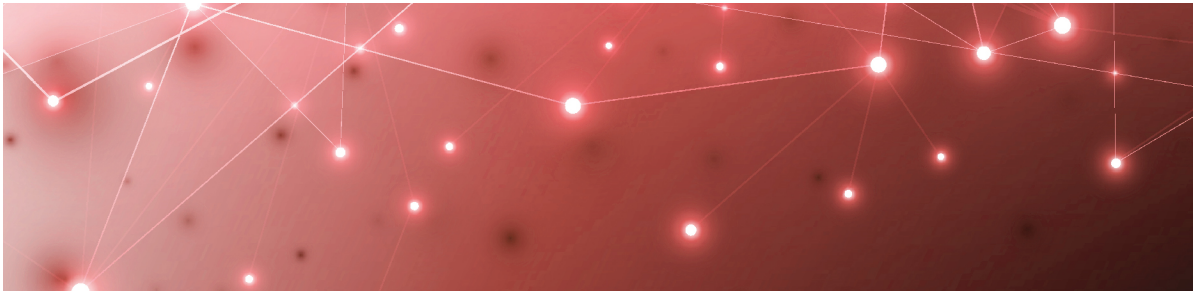
Use this procedure to ensure that the Gizmo Web UI installed successfully and that the services are running. The validation script that you need for this procedure is included in the installation package.

Before you Begin

- Ensure that any installer windows are closed.
 - If you are using Windows authentication to connect to the SQL server, the validation script must be executed by the same user.
1. Right-click the `GSX.Gizmo.<version>.Validation.Script.exe` file and select **Run as Administrator**.
 2. In the PowerShell console, review the results of the validation script:
 - Red—Indicates errors and that the installation was not successful. You need to take actions to address those errors.
 - Yellow—Provides information about the checks performed during the validation. No additional actions are required.
 - Green—Successful.

When the script is complete, all of the information that displayed in the console is saved to a log file.

3. To view the results in the log file, open the following file: `%ProgramData%\GSX Solutions\ValidationScript\<version>\Gsx.Gizmo.<version>_ValidationScriptOutput_<date>.log`.



Configure User Authentication

Gizmo includes optional authentication features. If you want to use Azure Active Directory (AD) to authenticate users and provide role-based access to them, you must also configure single sign-on.

Gizmo users are assigned one of the following roles, based on how they are configured in your Azure AD:

- **Viewer**—This user has read-only access to dashboards.
- **Administrator**—This user has read and write access and must be specified as an administrator in Azure AD.

Complete the procedures in the table below to enable authentication with Azure AD. After you complete these tasks, users can sign into Gizmo using Azure AD credentials and security policies.

Task	Description
"Submit Your Domain" on page 36	To allow Gizmo to authenticate with Azure AD, submit your domain to our support team.
"Enable HTTPS" on page 37	Use this procedure to enable HTTPS access to Gizmo.
"Configure Single Sign-On" on page 37	Use this procedure to give Gizmo permission to use your Azure AD instance to authenticate users.
"Configure Role-Based Access" on page 38	Use this procedure to give users access to Gizmo based on their defined role in Azure AD.

Submit Your Domain

To allow communication between Azure AD and Gizmo, our support team must whitelist the domain that you use to access Gizmo. Follow this procedure to submit your domain to our support team.

1. Identify the Gizmo URL used in your environment by end users.

2. Send this URL to your Delivery Engineer or Customer Success representative. You can also contact the Cloud Team to forward your request.
You will receive confirmation from your Delivery Engineer when your domain has been whitelisted.



Warning: Do not enable until you receive confirmation from your Delivery Engineer that your domain is whitelisted.

Next Steps

- ["Enable HTTPS" on page 37.](#)

Enable HTTPS

Use this procedure to enable HTTPS access to Gizmo. Perform this procedure on the Windows server where Gizmo is installed.

Before you Begin

- Ensure that your server has a valid SSL security certificate.
1. Open the Internet Information Services (IIS) Manager application.
 2. Select the **Default Web Site** and click **Bindings...**
 3. Click **Add...**
 4. In the **Type** list, select **https**.
 5. In the **SSL Certificate** list, select your certificate.
 6. Click **OK**.
Gizmo is now listed on ports 80 and 443 (HTTP and HTTPS).
 7. Restart IIS Manager.

Configure Single Sign-On

Perform this procedure in the Gizmo Web UI. You must be a tenant administrator in Azure AD to perform this procedure.

Before you Begin

- ["Submit Your Domain" on page 36](#)
 - ["Enable HTTPS" on page 37](#)
 - Ensure that you have received confirmation from the Martello support team that your domain is whitelisted.
1. Click the **Settings** button and select **Authentication**.
 2. On the **Authentication** page, use the toggle to select **Enable Single Sign-On**.
You are redirected on Azure AD Login page.

3. Enter your Azure AD credentials to log in.
A dialog box lists the permissions that Gizmo is requesting.
4. Click **Accept**.
You are redirected to the Gizmo application.

Configure Role-Based Access

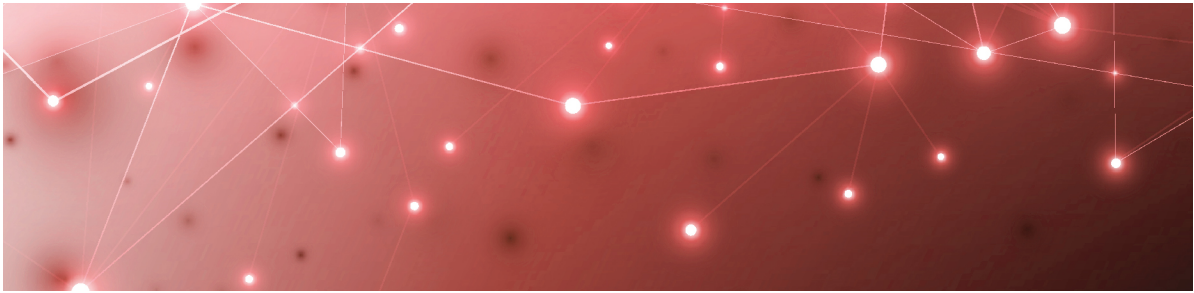
Use this procedure to give users access to Gizmo based on their defined role in Azure AD.

By default, Gizmo provides administrator privileges to users who you add to an Azure AD group called GizmoAdmins. You can specify a different group in Azure AD for administrators, but you must create the GizmoAdmins group before you can edit this setting.

Before you Begin

- In Azure AD, create a group called GizmoAdmins and ensure that you add any users who need to have administrator privileges in Gizmo.
- Ensure that you are logged into Gizmo with an account that is an administrator of the Azure AD tenant and is part of the GizmoAdmins group.
- ["Configure Single Sign-On" on page 37](#)

1. Click the **Settings** button and select **Authentication**.
2. Optional. Perform this step only if you want to use a custom Azure AD group for administrators.
 - Click the edit icon next to **Gizmoadmins** and enter the name of your Azure AD group.
 - Log out of the Gizmo WebUI, and then log in using an account that is an administrator of the Azure AD tenant and that is part of the group you specified.
3. On the Authentication page, click the **Enable Role Based Access** button.
A dialog box prompts you to give Gizmo permission to access Azure AD.
4. Select the checkbox to **Consent on behalf of your organization**.
5. Click **Accept**.
You are redirected to Gizmo.



Install the Robot Manager Service

Use the procedures in this section to install the Robot Manager service.

Complete the following tasks:

Task	Description
"Verify Robot Manager Prerequisites" on page 39	Verify that each Robot Manager machine meets the prerequisites for a successful installation. Complete this procedure on each machine where you plan to deploy robots.
"Verify Exchange Server and PowerShell Endpoints" on page 40	Optional. If you are monitoring on-premises Exchange servers, ensure that Robot Manager machines have Exchange server and PowerShell access. Complete this procedure on each machine where you plan to deploy robots.
"Install Robot Manager" on page 41	Install the Robot Manager service. Complete this procedure at each location where you plan to deploy robots.

Verify Robot Manager Prerequisites

Use the following PowerShell script to verify the .NET Framework version, the PowerShell version, and the remote execution settings.

Perform this procedure on each machine where you plan to deploy robots. You must be an administrator to perform this procedure.

Before you Begin

- Ensure the following ports are open: TCP ports 5671/5672 and 80/433 to allow communication from each robot to the Gizmo server.

- Ensure that the `CheckRobotPrerequisites.ps1` PowerShell script is available. You can download it from here:
<https://gsxch.sharepoint.com/:u:/s/downloads/EdDRntvJSodDi8HzDvnWOXUB8RXXydA7zM4JaPqUYEdOuA>
1. Open PowerShell as an administrator.
 2. Navigate to the script location in PowerShell.
 3. Type the following command:
`Get-ExecutionPolicy`
If the result shows 'Restricted', enter the following cmdlet: `Set-ExecutionPolicy Unrestricted`.
 4. Type the following command:
`.\CheckRobotPrerequisites.ps1`
 5. Choose **Run once (R)** at the security warning.
The script validates that all required prerequisites are met and highlights any that are missing. Address any missing prerequisites before you proceed with the installation.

Verify Exchange Server and PowerShell Endpoints

Perform this procedure only if you are using Gizmo to monitor on-premises Exchange servers. Use this procedure to verify that the machine where you plan to install the Robot Manager can communicate with the Exchange server, and that PowerShell is available.

Perform this procedure on each machine where you plan to deploy robots. You must be an administrator to perform this procedure.

Before you Begin

- Ensure that the user account for the Exchange server is properly configured. See ["Accounts" on page 25](#).
 - Review the Exchange server workload requirements. See ["Exchange and Exchange Edge Server Requirements" on page 27](#)
1. Open PowerShell as Administrator.
 2. To test the remote PowerShell connection on the Microsoft.Exchange endpoint, enter the following commands:
`$Cred = Get-Credential <domainname\username>`
`$SessionOption = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck`
`$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUrihttp://<YourServerName>/PowerShell -Credential $Cred -SessionOption $SessionOption -Authentication Kerberos`
`Invoke-Command -Session $Session -ScriptBlock {Get-ExchangeServer}`

3. To test the remote PowerShell connection on Microsoft.PowerShell endpoint, enter the following commands:

```
$Cred = Get-Credential <domainname\username>

$SessionOption = New-PSSessionOption -SkipCACheck -SkipCNCheck -
SkipRevocationCheck

$Session = New-PSSession -ConfigurationName Microsoft.PowerShell -
ConnectionUri http://<YourServerName>:5985/wsman -Credential $Cred
-SessionOption $SessionOption -Authentication Kerberos

Invoke-Command -Session $Session -ScriptBlock {Get-WmiObject -
Query "SELECT Name, Description, State, AcceptStop, AcceptPause
FROM Win32_Service"}
```



Tip: Change the port number to 5986 if you are using SSL.

Install Robot Manager

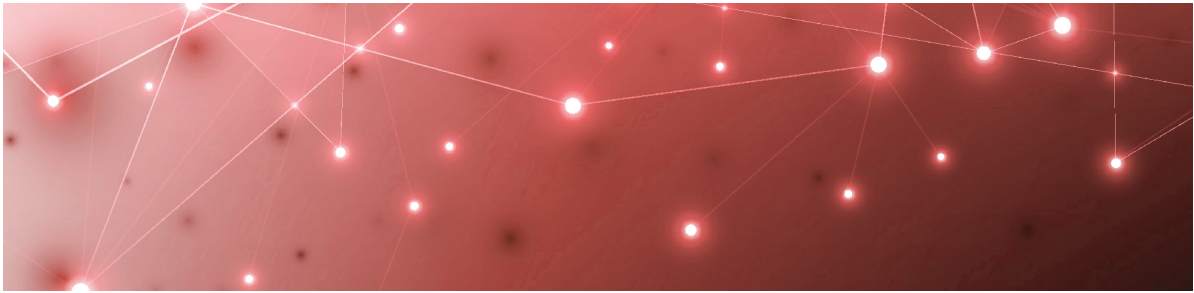
Use this procedure to install the Robot Manager service.

Perform this procedure on each machine where you plan to deploy robots.

1. In a browser, go to `http://<gizmo-server-fqdn>/downloads/Gsx.RobotManager.zip` where `<gizmo-server-fqdn>` is the FQDN of your Gizmo Server.
2. Extract the following files:
 - `Gsx.RobotManager.msi`—This file is used by the script.
 - `Install-GsxRobotManager.ps1`—This file is the script to run.
 - `Transform.mst`—This file is used by the script.

No specific location is required.
3. Open PowerShell as Administrator.
4. Enter the cmdlet `Set-ExecutionPolicy RemoteSigned`
5. Choose **[A] Yes to All**.
6. To run the `Install-GsxRobotManager.ps1` script, navigate to the script location path in PowerShell and run the following command:


```
.\Install-GsxRobotManager.ps1
```
7. Choose **[R] Run once** after the Security Warning.



Configure Robot Credentials

Robots require credentials to log into your applications and perform tests. For example, a robot that monitors Office 365 workloads requires credentials for an Office 365 user account.

Gizmo provides placeholders for these credentials, to indicate the correct format. The following table lists the placeholders that Gizmo creates.

Table 4: User Credentials for Robots


Task	Description
Office 365 User	myusername@example.com
Exchange Mailbox Server Credential	domain\username
On-Premises User	myusername@example.com
Exchange Edge Server Credential	domain\username
Office 365 Echo User	myusername@example.com

Use the procedures in this section to edit the placeholders, and to create new credentials if you require additional robot accounts.

Task	Description
"Edit Monitoring Credentials" on page 43	Use the placeholders to create credentials that robots can use to access the applications that you want them to monitor.
"Add Monitoring Credentials" on page 43	Create additional credentials if your deployment requires them.

Edit Monitoring Credentials

Use this procedure to edit credentials that robots use to access workloads. Perform this procedure in the Gizmo Web UI.

1. Select **Settings > Credentials** from the navigation panel.
2. On the credential that you want to edit, click  and select **Edit**.
3. Edit any of the following information as needed, and then click **Save**.
 - **Alias**—Type a brief name or description for the monitoring credential.
 - **Username**—Type the username that the robot will use.
 - **Password**—Type the password associated with the account.
 - **Confirm Password**—Type the password again for confirmation.

Next Steps

- ["Configure Workloads " on page 44](#)

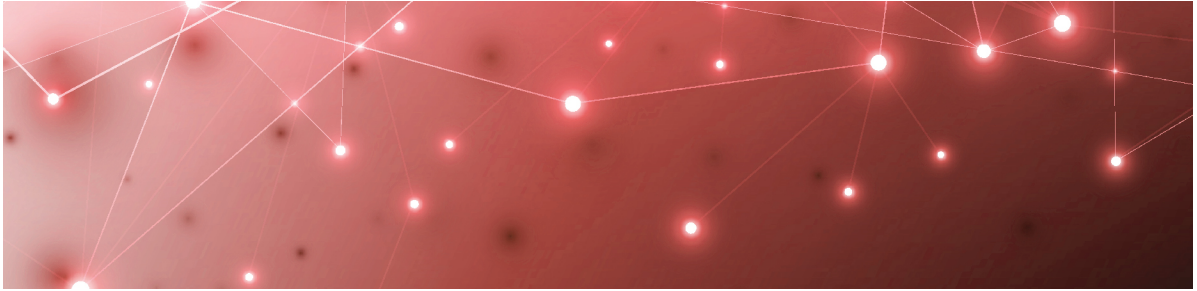
Add Monitoring Credentials

Use this procedure to add credentials that robots can use to access workloads. Perform this procedure in the Gizmo Web UI. For information about the number of monitoring accounts that you need, see ["Accounts" on page 25](#)

1. Select **Settings > Credentials** from the navigation panel.
2. Enter the following information, and then click **Add**.
 - **Alias**—Type a brief name or description for the monitoring credential.
 - **Username**—Type the username that the robot will use.
 - **Password**—Type the password associated with the account.
 - **Confirm Password**—Type the password again for confirmation.

Next Steps

- ["Configure Workloads " on page 44](#)



Configure Workloads

Complete the tasks in the following table.

Task	Description
"Create Monitoring Configurations" on page 44	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 45	Specify the applications that you want the robots to monitor at each site.
"Add a Location Tag" on page 46	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 45](#)

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 44](#)
- 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, 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 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.

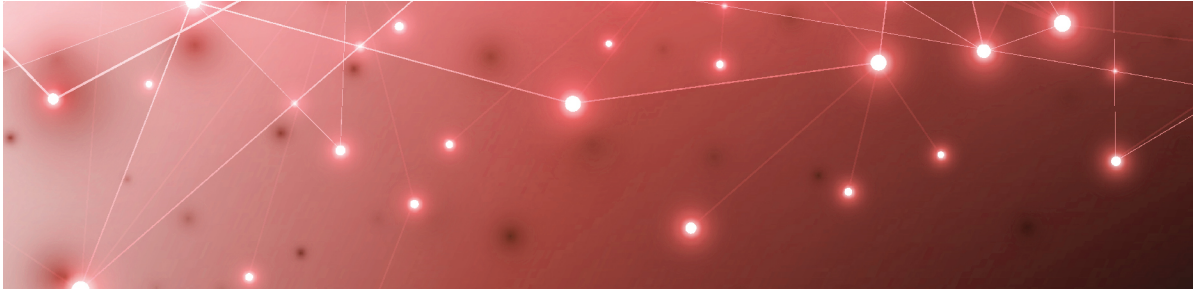
Next Steps

- ["Add a Location Tag" on page 46](#)

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**.



Deploy Power BI

Use the information in this section to deploy Microsoft Power BI with Gizmo.

Task	Description
"Import the Power BI Template" on page 47	Import the Power BI templates for the workloads that you want to monitor in Gizmo.
"Share a Report Using Power BI Service" on page 48	Share the report created from the Power BI Template with others using the Power BI Service.
"Verify the Power BI Template" on page 1	Ensure that the template installed successfully.

Import the Power BI Template

Use the following procedure to import the Gizmo template into Microsoft Power BI and load the report data.



Warning: We strongly recommend that you do not make any changes to this template. Any changes are unsupported and may result in errors or inconsistencies in your reported data, or an inability to retrieve data to populate this report.

Before you Begin

- Download and install the latest version of Power BI. For information and instructions see: <https://docs.microsoft.com/en-us/power-bi/fundamentals/desktop-get-the-desktop>
- Ensure that you have the latest version of the Gizmo Analytics Power BI Template. The template is included in the installer archive.
- Ensure that you have a Power BI license to publish reports. We recommend a Power BI Pro license so that you can share your reports with a team.

1. Double click the `Gizmo Analytics Full-2.3.3.16543.pbix` template file to launch Power BI Desktop and load the template.
2. Click the link at the bottom of the **Welcome** page and enter the Power BI license associated with your Office 365 account.
3. On the **Gizmo Analytics** page, provide the following information, then click **Load**:
 - Server—The SQL server database to use.
 - Database—The name of the database.
 - Range Start—Use 01/01/2020 or any date prior to the installation of Gizmo.
 - Range End—Use 01/01/2025 or any date later than today's date.
4. On the **SQL Server database** window, select the **Database** tab, provide the credentials for the SQL Server database, then click **Connect**.
5. On the **Native Database Query** page, click **Run**.
The template loads the data from SQL Server.

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 Gizmo Analytics 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 via email, or to embed the report in SharePoint or to a website or portal.



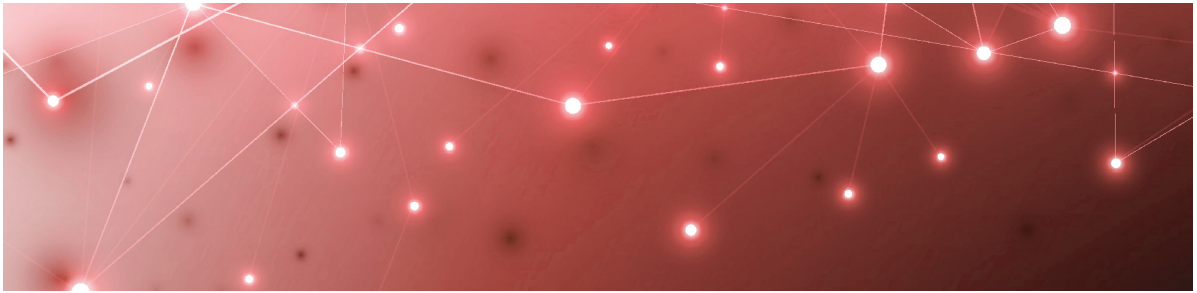
Tip:

To ensure that the data in your Power BI report is refreshed



regularly, use the scheduling feature:

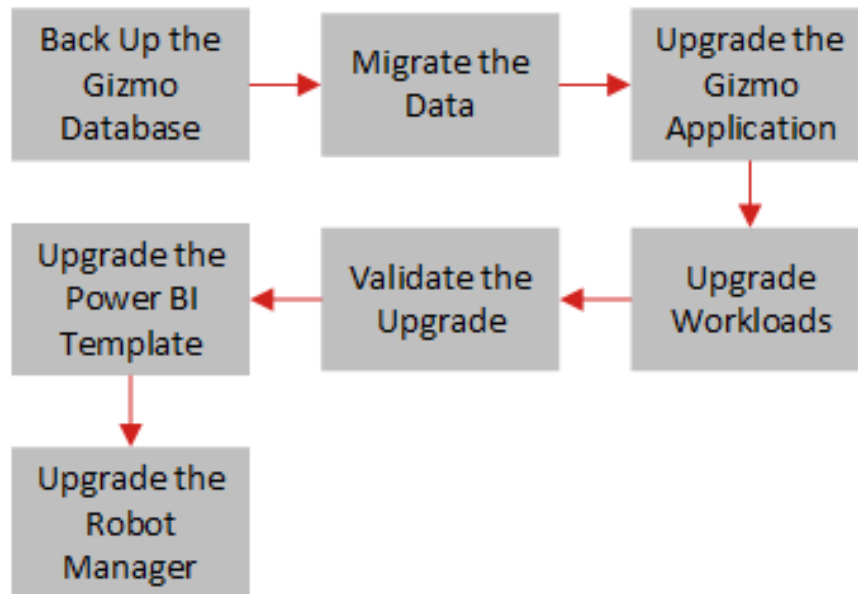
<https://docs.microsoft.com/en-us/power-bi/connect-data/refresh-scheduled-refresh>



Upgrade Process

The following diagram provides an overview of the Gizmo upgrade process.

Figure 7: Upgrade Process

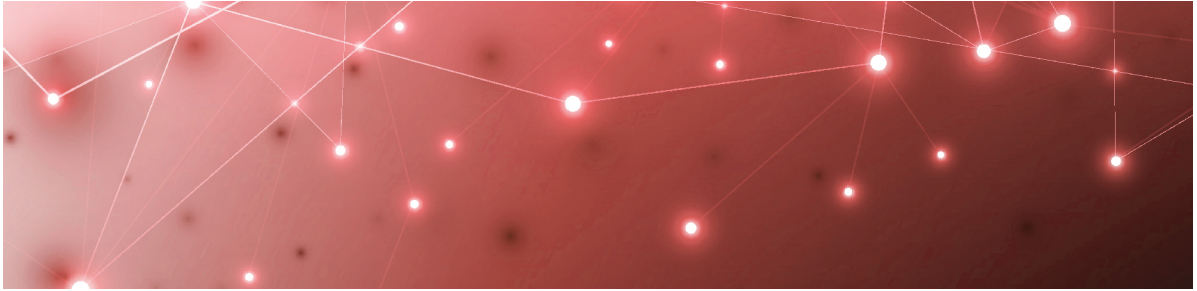


Time Requirements

The time required to perform an upgrade depends on your deployment. Typical upgrades require a maintenance window of 1 to 4 hours.

Supported Upgrade Paths

You can upgrade to Gizmo 2.2 directly from Release 2.0 or Release 2.1. If you are upgrading from an earlier release, you must upgrade to Release 2.0 as an intermediate step before upgrading to 2.2.



Upgrade the Gizmo Web UI

Use the procedures in this section to upgrade the Gizmo Web UI.

Task	Description
"Migrate Data" on page 51	If you are upgrading from Gizmo Release 1.9, you need to migrate data from your existing installation so that it is available for Power BI reports after the upgrade. If you are upgrading from a later release, you do not need to perform this procedure.
"Retrieve Account and Service Information" on page 52	Retrieve service account and IIS user information from the current installation. You need this information during the upgrade process.
"Upgrade the Application" on page 53	Upgrade the Gizmo Web UI.
"Validate the Upgrade" on page 54	Run a script to validate that the upgrade was successful.
"Upgrade the Power BI Template" on page 55	Import the Gizmo templates for the new release into Microsoft Power BI.

Migrate Data

Use this procedure to migrate data from your existing installation so that it is available for Power BI reports on your upgraded version. Perform this procedure only if you are upgrading from Gizmo Release 1.9.

Before you Begin

- Back up the database.
- Stop the DataTier service.
- Ensure that Power BI is not running.

1. Open the SQL Server Management Studio.
2. Connect to the SQL Server.
3. Execute the `GetNumberOfDaysOfHistoryInScanHot.sql` script, which is available in the installer archive file.
The script provides you with the number of days of history that you have stored in your existing installation.
4. Press Ctrl+ O to open a file and select the `MigrateDataFromScanHotToHistoricalData.sql` script from the installer archive file.
5. If required, customize the parameters of the script to fit your requirements:

Parameter	Description
nbDaysToMigrate	Search <code>DECLARE @nbDaysToMigrate INT = 183</code> in the SQL file. The default value for <code>nbDaysToMigrate</code> is 183 days (6 months). Set the number of days of data that you want to migrate. Any data that is not within this range will be lost after the upgrade.
packetLengthInMinutes	Search <code>DECLARE @packetLengthInMinutes INT = 1440</code> in the SQL file. The default value for <code>packetLengthInMinutes</code> is 1440 minutes (transactions of one day of data).

6. Launch the SQL script `MigrateDataFromScanHotToHistoricalData.sql` and wait for it to finish running.
7. While the script is running, you can check the status of the migration by launching the script `CheckMigration.sql`.
When the status displays **Finished** with a value of **Yes**, all the required data is migrated. Dates in the report are in local time.



Tip: If errors occur during the migration process, execute the SQL script again.

Retrieve Account and Service Information

Use this procedure to retrieve the following information from the currently installed version:

- The service account.

- The IIS user.

The wizard prompts you to enter this information when you install the Gizmo Web UI.

1. To retrieve the service account used in the currently installed version, open PowerShell and run the following command:

```
Get-WmiObject win32_service -Filter "Name LIKE 'Gsx.%'" | format-table name, startname
```

This command lists the current services in the `name` column and the service account that started each of them in the `startname` column.
2. To retrieve the IIS User, search for IIS and launch it.
3. Double-click on the IIS Server, select Application Pools, and locate the Gizmo App Pool. The information is in the Identity column.
The default App Pool name for Gizmo is DefaultAppPool.

Upgrade the Application

Use this procedure to upgrade the Gizmo application.

Before you Begin

- ["Retrieve Account and Service Information" on page 52](#)

1. Right-click the `GSX.Gizmo.<version>.exe` file and select **Run as Administrator**.
2. Review the **End User License Agreement** and click **Next** to accept it.
3. On the **Install folder** screen, select the location where you want to install Gizmo and click **Next**.
4. On the **Service Account** screen, choose one of the following **Built-in accounts** to run the services and then click **Next**:
 - Local System (Default)
 - Local Service
 - Network Service
 - Other

We recommend that you use the Local System (Default) account. If you use Windows Authentication to access SQL, you must select Other and provide credentials for a user that has permission to access the database.

5. On the **IIS Website** screen, configure the following settings and then click **Next**:
 - **Website name**
 - **Application pool**
 - **Built-in account**—This is the account that runs the IIS Website. Select **Other**.

6. On the **Database Connection** screen, configure the following settings and then click **Next**:
 - **Database Server**—Click **Load** to use the existing database server.
 - **Database**—The newly added SQL database.
 - **User**—The username for the database owner of the newly added database. This can be the SA (SQL Authentication) or the Windows credentials, depending on how the database user was configured.
 - **Password**—The password for the database owner of the newly added database.
 - **Install SQL Server 2017 Express**—For trail versions only. Select the checkbox to install SQL Server 2017 Express. When you select this option, the default username is gizmo and the password is randomly generated.
7. On the **RabbitMQ Connection** screen, configure the following settings and then click **Next**:
 - **Host**
 - **Port**
 - **SSL**—Select the checkbox to use SSL. The default port is 5671.
 - **Virtual Host**
 - **User**
 - **Password**
 - **Install RabbitMQ 3.8.1**—Select this checkbox to install RabbitMQ. The installer uses the FQDN of this server as the host. The default username is gizmo and the password is randomly generated.
8. On the **GSX Downloads** screen, set the locations of the **Downloads** folder and the **Downloads URI** and click **Next**.

We recommend that you use the default values for both of these settings.
9. Review the information on the **Ready to install** screen and click **Install**.
10. When the installation is complete, you must restart the computer for the changes to take affect. We recommend that you wait for up to 2 minutes before you click the **Restart** button or restart the computer manually.
11. Clear the browsing cache in order to display updated data.

Validate the Upgrade

Use this procedure to ensure that the Gizmo Web UI installed successfully and that the services are running. The validation script that you need for this procedure is included in the installation package.

Before you Begin

- Ensure than any installer windows are closed.
- If you are using Windows authentication to connect to the SQL server, the validation script must be executed by the same user.

1. Right-click the `GSX.Gizmo.<version>.Validation.Script.exe` file and select **Run as Administrator**.
2. In the PowerShell console, review the results of the validation script:
 - Red—Indicates errors and that the installation was not successful. You need to take actions to address those errors.
 - Yellow—Provides information about the checks performed during the validation. No additional actions are required.
 - Green—Successful.

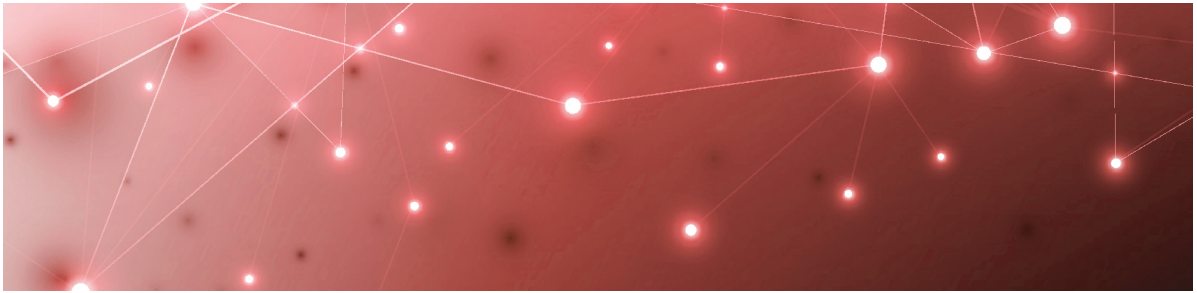
When the script is complete, all of the information that displayed in the console is saved to a log file.
3. To view the results in the log file, open the following file: `%ProgramData%\GSX Solutions\ValidationScript\<version>\Gsx.Gizmo.<version>_ValidationScriptOutput_<date>.log`.

Upgrade the Power BI Template

Use the following procedure to import the Gizmo templates for the new release into Microsoft Power BI.

Before you Begin

- Download and install the latest version of Power BI. For information and instructions see: <https://docs.microsoft.com/en-us/power-bi/fundamentals/desktop-get-the-desktop>
 - Ensure that you have the latest version of the Gizmo Analytics Power BI Template. The template is included in the installer archive.
 - Ensure that you have a Power BI license to publish reports. We recommend a Power BI Pro license so that you can share your reports with a team.
1. Double click the `Gizmo Analytics Full-2.3.3.16543.pbix` template file to launch Power BI Desktop and load the template.
 2. Click the link at the bottom of the **Welcome** page and enter the Power BI license associated with your Office 365 account.
 3. On the **Gizmo Analytics** page, provide the following information, then click **Load**:
 - Server—The SQL server database to use.
 - Database—The name of the database.
 - Range Start—Use 01/01/2020 or any date prior to the installation of Gizmo.
 - Range End—Use 01/01/2025 or any date later than today's date.
 4. On the **SQL Server database** window, select the **Database** tab, provide the credentials for the SQL Server database, then click **Connect**.
 5. On the **Native Database Query** page, click **Run**.
The template loads the data from SQL Server.



Upgrade the Robot Manager Service

The Robot Manager service has been updated for Gizmo Release 2.2. If you are upgrading from a previous release of Gizmo, we strongly recommend that you upgrade your deployments of the Robot Manager service.

Use the procedures in this section to upgrade the Robot Manager service.

Task	Description
"Upgrade the Robot Manager Service" on page 56	Perform this procedure on each computer where Robot Manager is installed.
"Validate the Upgrade on the Robot Manager Host" on page 57	Perform this procedure on each computer where Robot Manager is installed.
"Validate the Upgrade on the Gizmo Server" on page 57	Perform this procedure on the server where Gizmo is installed.

Upgrade the Robot Manager Service

Use this procedure to upgrade the Robot Manager service.

Before you Begin

Uninstall the current version of Robot Manager.

1. In a browser, go to `http://<gizmo-server-fqdn>/downloads/Gsx.RobotManager.zip` where `<gizmo-server-fqdn>` is the FQDN of your Gizmo Server.
2. Extract the following files:
 - `Gsx.RobotManager.msi`—This file is used by the script.
 - `Install-GsxRobotManager.ps1`—This file is the script to run.
 - `Transform.mst`—This file is used by the script.

No specific location is required.

3. Open PowerShell as Administrator.
4. Enter the cmdlet `Set-ExecutionPolicy RemoteSigned`
5. Choose **[A] Yes to All**.
6. To run the `Install-GsxRobotManager.ps1` script, navigate to the script location path in PowerShell and run the following command:
`.\Install-GsxRobotManager.ps1`
7. Choose **[R] Run once** after the Security Warning.

Validate the Upgrade on the Robot Manager Host

Use this procedure to verify that Robot Manager has been updated to the latest version. Perform this procedure on every computer that hosts the Robot Manager.

1. Execute the following command in PowerShell as Administrator:

```
Get-ItemProperty  
'HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\*' | Select-Object DisplayName, DisplayVersion, Publisher,  
InstallDate | where-object { $_.displayname -eq 'Robot Manager' -  
and $_.publisher -eq 'GSX Solutions' }
```

The command returns a table that lists the currently installed version of the Robot Manager.
2. Verify that the newly installed version is listed.
For the Gizmo 2.2, the latest version of the Robot Manager is 4.3.2.0.

Validate the Upgrade on the Gizmo Server

Use this procedure to verify that Robot Manager has been updated to the latest version. Perform this procedure on the server where the Gizmo Web UI is installed.

1. Open the GSX Management Shell and execute the following command:

```
Get-GsxRobotManager | Where-Object { $_.Hostname -eq  
"$RobotManagerStationFQDN" } | fl
```

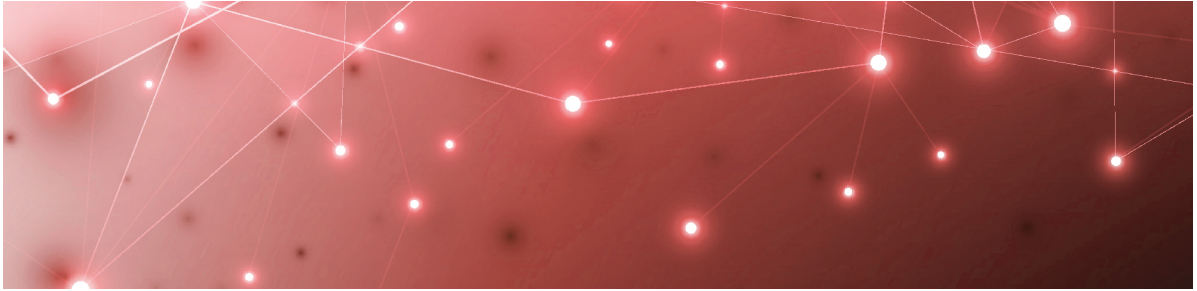
where:
\$RobotManagerStationFQDN is the FQDN of the server where Gizmo is installed.

The command returns a list that includes the current version of the Robot Manager.

```
Guid : e7cf63e9-7045-4e37-ac6c-4ce781ab2b76  
Hostname : YOUR_ROBOT_MANAGER_STATION_FQDN  
Alias : YOUR_ROBOT_MANAGER_STATION_ALIAS  
Description :  
RegistrationState : Success  
HeartBeatDate : <date>
```

```
HeartBeatState : Healthy
Version : 4.3.2.0
AdminTaskStatus : None
AdminTaskDate :
AdminTaskError :
TagValues : {}
```

- 2.** Verify that the newly installed version is listed.
For Gizmo2.2, the latest version of the Robot Manager is 4.3.2.0.



Backup and Restore

Use the information and procedures in this section to perform the following tasks.

Task	Description
"Back up the Gizmo Environment" on page 59	Create a backup of all the components in the Gizmo environment.
"Restore the Gizmo Web UI" on page 59	Restore Gizmo after a server failure, or if you need to move Gizmo from one virtual machine to another.

Back up the Gizmo Environment

To be able to recover your Gizmo environment, you must create backups for the following components:

- **Windows server registry**—On the server that hosts the Gizmo Web UI, export the registry “Computer\HKEY_LOCAL_MACHINE\SOFTWARE\GSX Solutions” in a .reg file.
- **RabbitMQ**—All connection settings to RabbitMQ are stored in the `GizmoRegistry.reg` file. Note that passwords are encoded, not encrypted. Ensure that you have a record of the passwords.
- **SQL database**—All connection settings to the database are stored in the `GizmoRegistry.reg` file. Note that passwords are encoded, not encrypted. Ensure that you have a record of the passwords.
- **Robot Manager Installer**—Create a backup of the Robot Manager Installer, which is available in this default location:
`C:\ProgramData\Gsx Solutions\Downloads\Gsx.RobotManager.zip`

Restore the Gizmo Web UI

Use the following procedure in the event that the machine that hosts Gizmo failure, or if you need to move Gizmo from one machine to another.

While the server that hosts the Gizmo Web UI is offline, it cannot receive messages from the Robot Manager services. Messages sent by the Robot Manager services

during this time are lost. You can find errors related to these messages in the log file. The Gizmo Web UI begins receiving messages from the Robot Manager services as soon as the restore operation is complete and the server is online.

Before you Begin

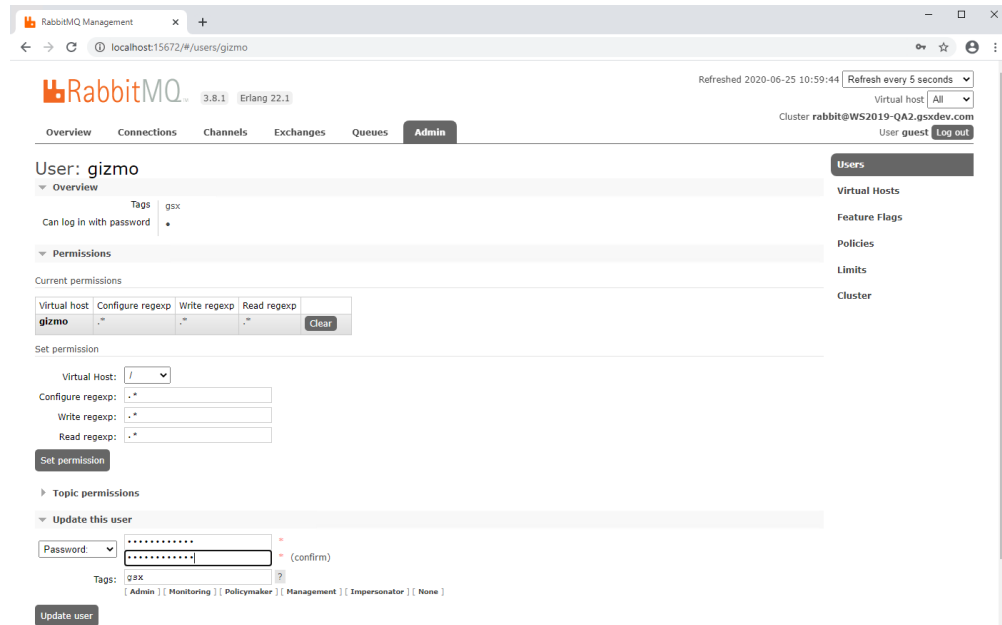
- Right-click the `GizmoRegistry.reg` file and select **Run as Administrator**; this populates the registry as if Gizmo is already installed.
1. Right-click the `GSX.Gizmo.<major_version>.<minor_version>.<patch_version>.<build_number>.exe` file and select **Run as Administrator**.
 2. Enter the Database Connection settings:
 - Database Server
 - Database
 - Username and Password



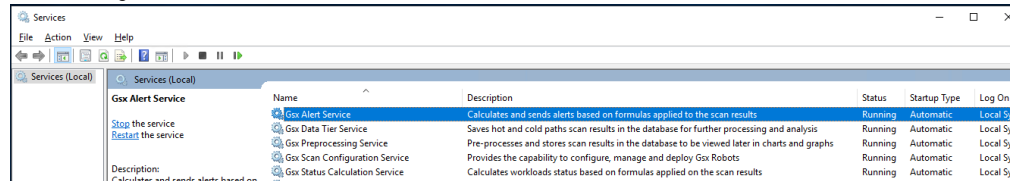
Warning: Do not select "Install SQL Server 2017 Express".

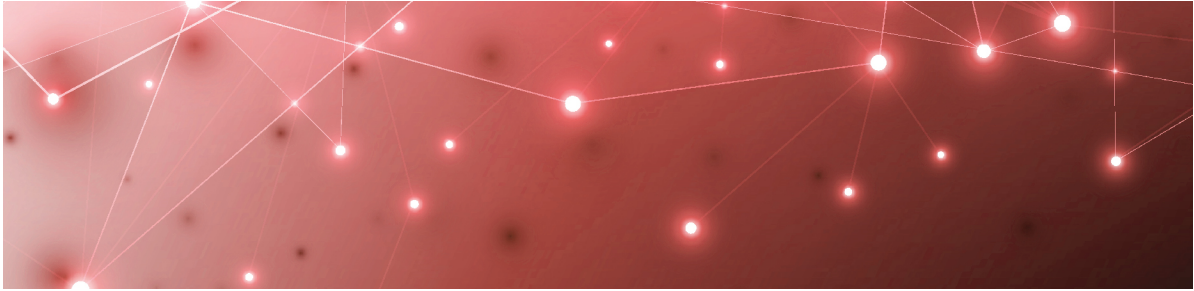
3. In case that RabbbitMQ has to be installed on the same dedicated machine as Gizmo, select the option "Install RabbitMQ 3.8.1" in the wizard page:

4. Update the Gizmo username and password in the RabbitMQ management web page to match the username and password that was set previously from the machine that was used to create the backup:



5. For GSX Downloads, replace the file with the backup one:
C:\ProgramData\Gsx Solutions\Downloads\Gsx.RobotManager.zip
6. Run the GizmoRegistry.reg again to override the RabbitMQ settings.
7. Manually restart all the Gizmo Services.





Troubleshooting

Use the information and procedures in this section to troubleshoot installation issues.

Task	Description
"Respond to Error Messages" on page 62	Respond to error messages that occur during an installation or upgrade.
"Repair an Installation" on page 64	Use the Repair feature to address installation issues.
"Submit a Support Ticket" on page 64	If the installation fails or issues occur that are not addressed by the other procedures in this section, submit a ticket to our support team.

Respond to Error Messages

Use the information in the table below if you encounter error messages during the installation.

Table 5: Error Messages

Error Type	Description
Database connection error	<p>If you select Windows Authentication when the wizard prompts you to configure the Database Connection, you might encounter a failure connecting to the database server. The following error message displays:</p> <pre>Failed connecting to DB server The type initializer for 'System.Data.SqlClient.SqlConnection' threw an exception.</pre> <p>To fix this issue, click OK on the error message, cancel the installation and then start the installation again.</p>
RabbitMQ connection error	<p>If Gizmo cannot connect to RabbitMQ, the following error message displays:</p> <pre>Could not load file or assembly 'RabbitMQ.Client, Version=5.0.0.0, Culture=neutral, PublicKeyToken=89e7d7c5feba84ce' or one of its dependencies. The system cannot find the file specified.</pre> <p>To fix this issue, click OK on the error message, cancel the installation and then start the installation again.</p>
IIS download files errors	<p>If Gizmo cannot download IIS files an error message is displayed.</p> <p>To fix this issue, click OK on the error message, cancel the installation and then start the installation again.</p>
Certificate store access error	<p>If Gizmo cannot access the certificate store, an error message is displayed.</p> <p>To fix this issue, click OK on the error message, cancel the installation and then start the installation again.</p>

Error Type	Description
	When you upgrade Gizmo, you may encounter the following error in the installer interface:
Files in use error	<p>Files in use. The following applications are using files that need to be updated by this setup. Click 'Ignore' to continue setup (reboot may be required). Click 'Abort' to abort setup. Click 'Shut down' to close the applications.</p> <p>To resolve this issue, close all PowerShell consoles and click Ignore.</p>
Failure to execute a command during an upgrade	<p>When you upgrade Gizmo, the following error can occur in the installer interface if you do not close your PowerShell sessions first:</p> <pre>Failed executing command "C:\Windows\system32\Windows PowerShell\v1.0\powershell.exe" -Command "& 'C:\Program Files\GSXSolutions\PowerShell\Installer.GsxManagementShell\CopyDependencies.ps1'</pre> <p>To resolve this issue, ensure that all of your PowerShell sessions are closed and then click the Retry button to resume the upgrade.</p>

Repair an Installation

If you encounter issues during the installation, use the Repair feature.

1. In Windows, open the **Control Panel** and select **Programs and Features**.
2. Right-click on Gizmo and select **Change**.
3. In the pop-up window, click **Repair**.

Next Steps

- If this issue is not resolved, ["Submit a Support Ticket" on page 64](#)

Submit a Support Ticket

If the installation fails or issues occur that are not addressed by the Repair feature, submit a support ticket. Use this section to prepare the information that you need to provide when you submit a support ticket.

Collect the following information:

- **Problem description**—Describe the symptom or failure. Include as many details as possible. Indicate whether this was a new installation, or an upgrade.
- **Screen captures**—Provide screen captures of the errors.

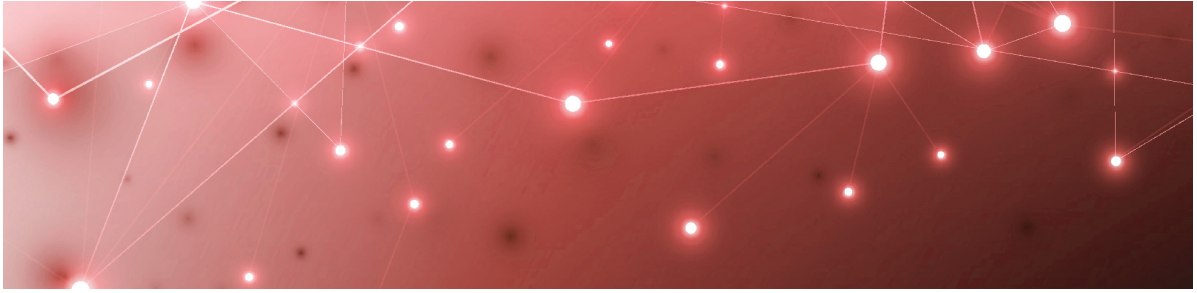
- **Gizmo logs**—Collect installation logs and the microservices logs by creating a zip file that includes following folders located at C:\ProgramData\Gsx Solutions\
 - Alert
 - Data Tier
 - Installer Logs; if you are using Windows Server 2019, these logs may be located in the Temp directory.
 - Preprocessing
 - Scan Configuration
 - Status Calculation
 - WebUI
- **Windows logs**—Windows Event Application and System Logs saved as .evtx files.
- **Environment specifics**—Information about the operating environment, such as:
 - The server OS and version.
 - SQL database information, such as location, version, and authentication method.
 - The RabbitMQ version if you have an existing installation and did not use the version in the Gizmo installation package.
 - A list of installed programs.



Note: Ensure that you close the Gizmo install wizard before you create the zip file.

After you have collected all of the information, use the following link to submit a support request:

<https://helpcenter.gsx.com/hc/en-us/requests/new>



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.