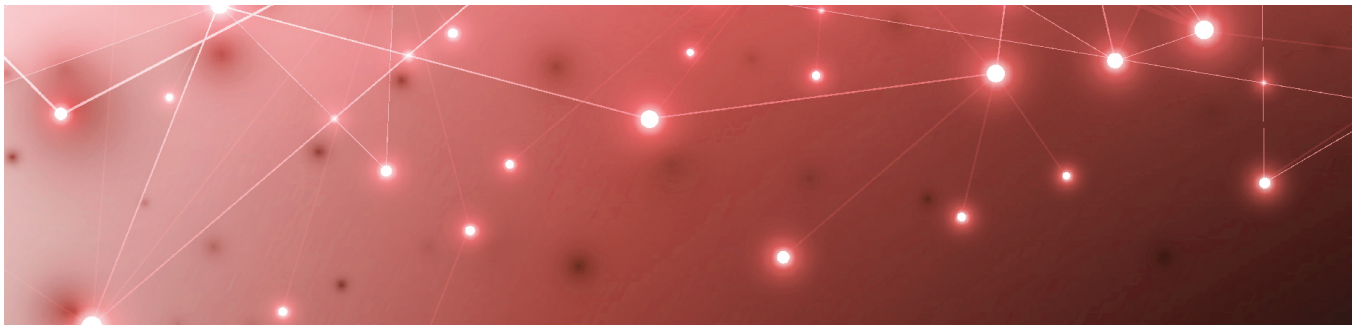


MARTELLO | *GSX* is a subsidiary of Martello Technologies

Martello Gizmo

CLOUD DEPLOYMENT GUIDE

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

Cloud Deployment Guide
Release 2.2 - July 16, 2021

Contents

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

CHAPTER 5

CHAPTER 6

CHAPTER 7

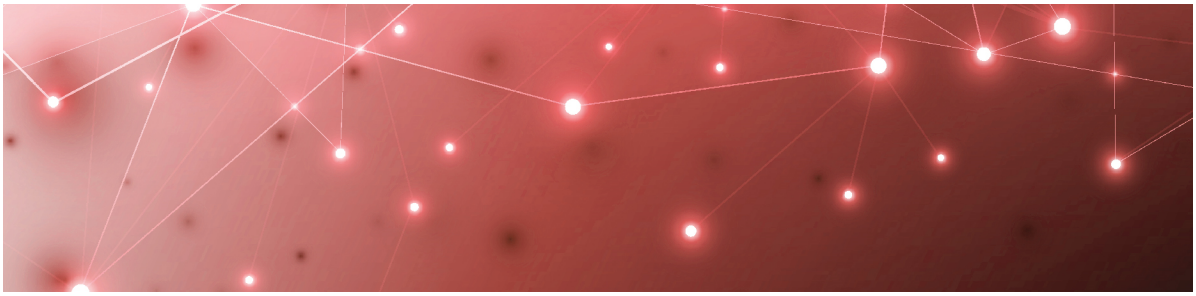
CHAPTER 8

CHAPTER 9

CHAPTER 10

CHAPTER 11

CHAPTER 12



CHAPTER 1

Introduction

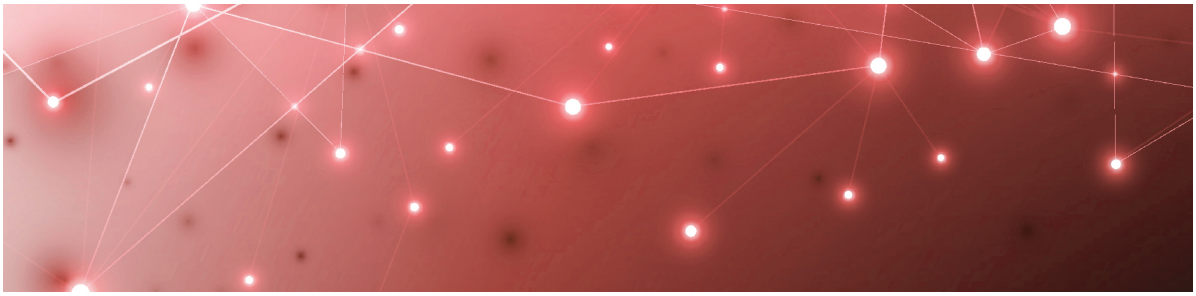
Document Purpose and Intended Audience

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 Cloud Deployment Guide, Release 2.2



CHAPTER 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 6
- "Security" on page 9
- "Security Architecture" on page 9

Components

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

- "Gizmo Web UI" on page 6
- "Robot Manager Service" on page 7
- "Robots" on page 7
- "Workloads" on page 7

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.

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.

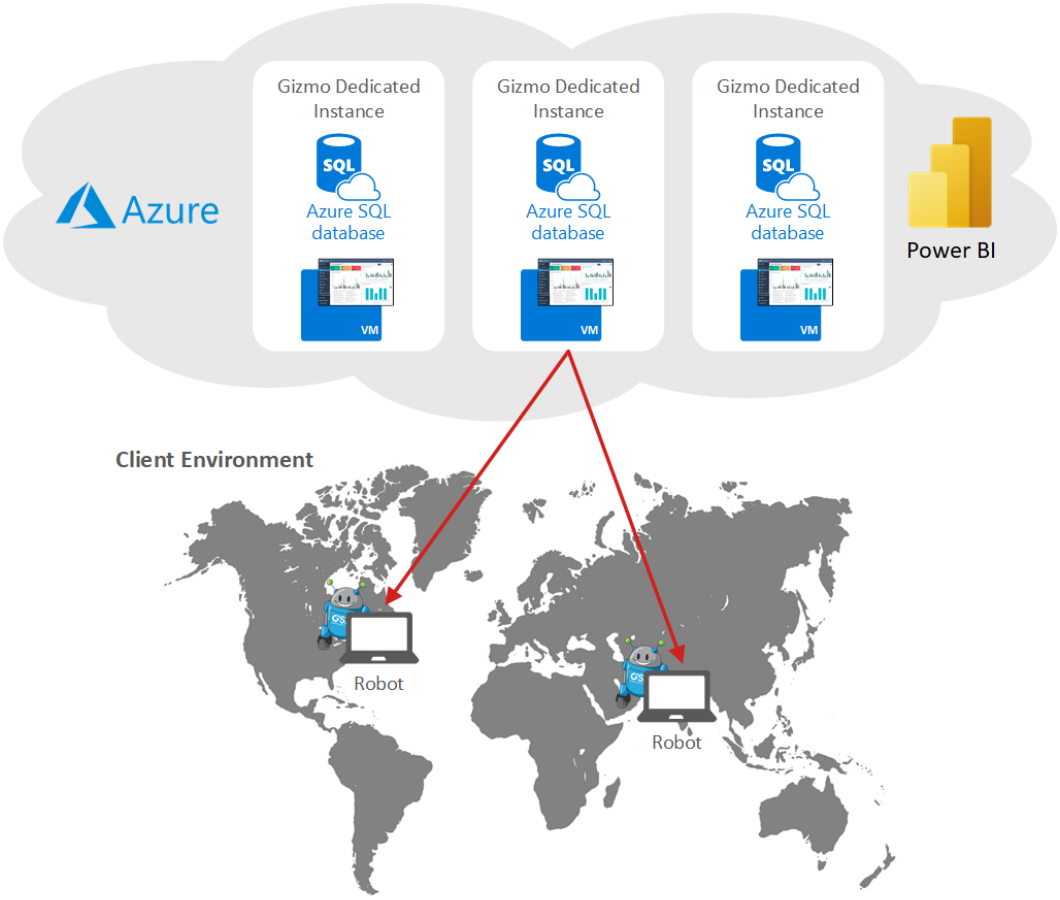
Gizmo connects to Microsoft workloads using HTTPS. Client data is logically separated in our databases and is only accessible to administrators with your explicit consent.

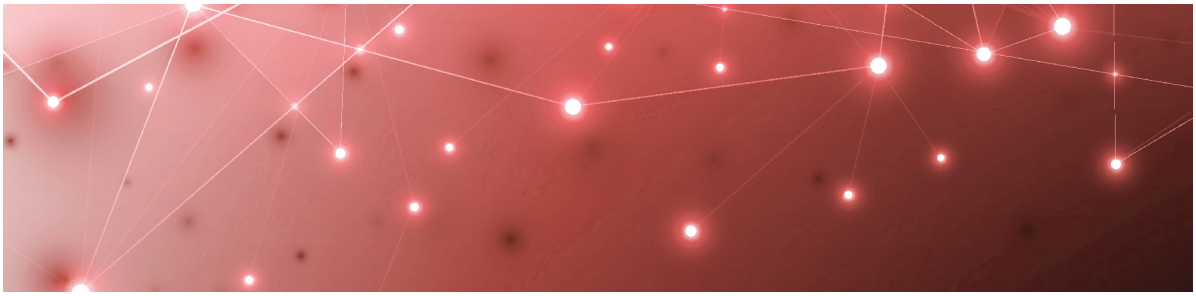
Security Architecture

The Gizmo web servers redirect all visitors to a forced SSL (HTTPS) connection to prevent the transmission of customer data in plain text. All traffic between the user's web browser and our web server is encrypted and secured with Azure Application Gateway. All our Azure infrastructure is secured with Firewalls, Multi Factor (MFA), and Azure Just in Time VM Access (JIT) authentication are implemented.

The following diagram shows the security architecture between the Gizmo server and the customer environment.

Figure 1: Security Architecture





CHAPTER 3

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

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	Use Gizmo to test the connectivity to the Exchange server, check the protocols, and check the status of the services and the transport queue. 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.
Exchange Online	Outlook is slow	Use Gizmo to test the connection between the Exchange Online service and the end user. In this scenario, you could deploy a pair of robots in any of the following locations: • 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	OneDrive performance depends on many network factors, such as the distance between the end user and the host, DNS resolution, and proxy connections. In this scenario, you could deploy a pair of robots to make the following comparisons: • 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 14
- "Monitor the Route from Sites to the Cloud" on page 15
- "Monitor the Full Route to the Cloud " on page 16
- "Monitor Performance in an Office Building " on page 17
- "Monitor Cloud Performance" on page 18

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.

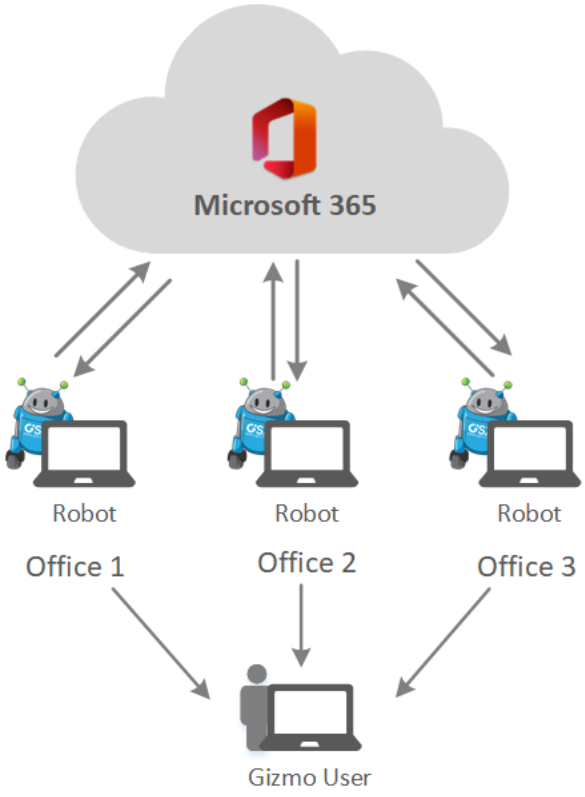
We recommend that you select sites that meet one or more of the following criteria:

- 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 you 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 2: Robot Deployment to Monitor Office 365 at Critical Locations



Monitor the Route from Sites to the Cloud

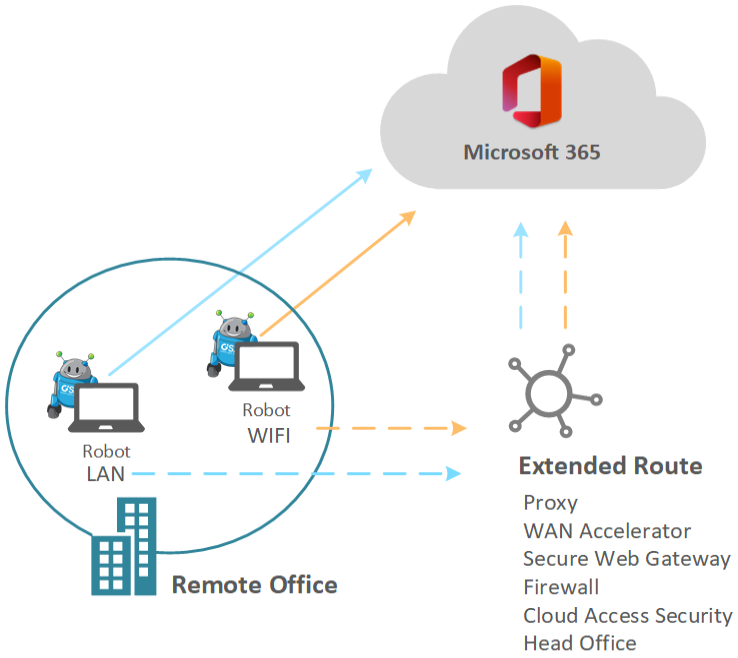
You can use Gizmo to monitor the route between your cloud-based infrastructure and your sites. This type of deployment allows you to analyze remote office connectivity and end-user experience.

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 3: 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 you 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 16.

Monitor the Full Route to the Cloud

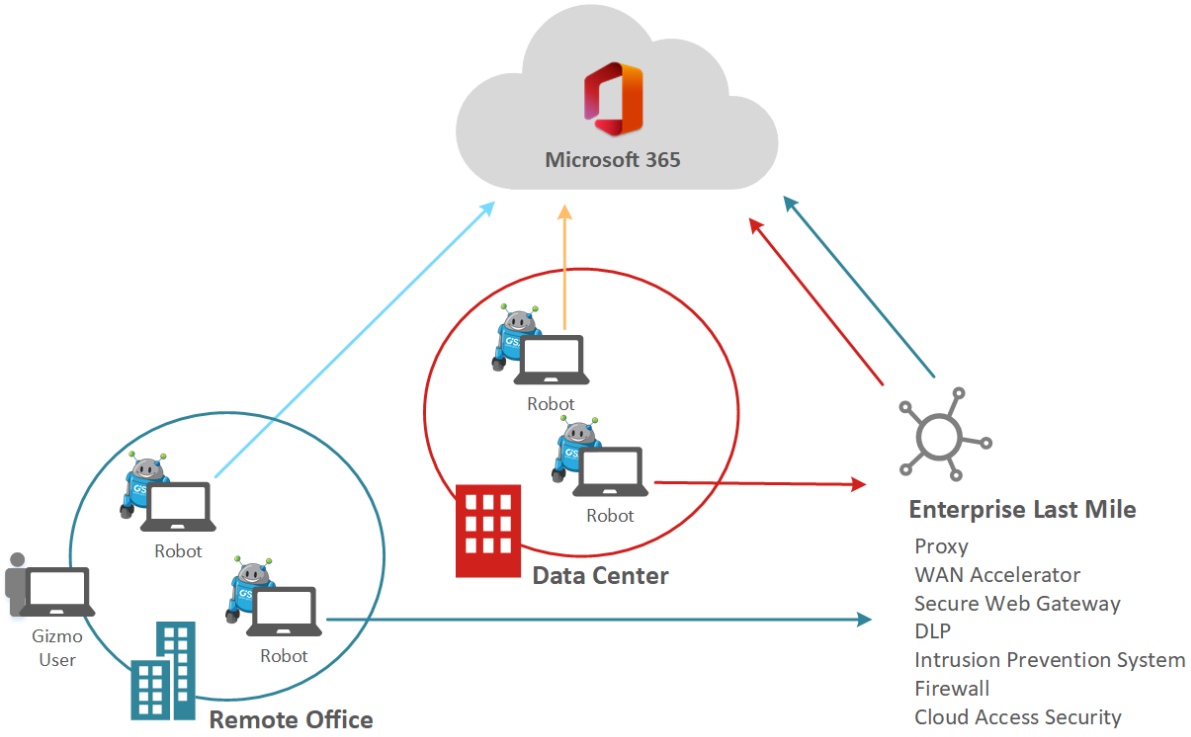
You can use Gizmo to monitor the route between your cloud-based infrastructure, your head office, and your remote sites. This type of deployment is beneficial if performance improvement is a higher priority than monitoring services geographically.

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 4: 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 you 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

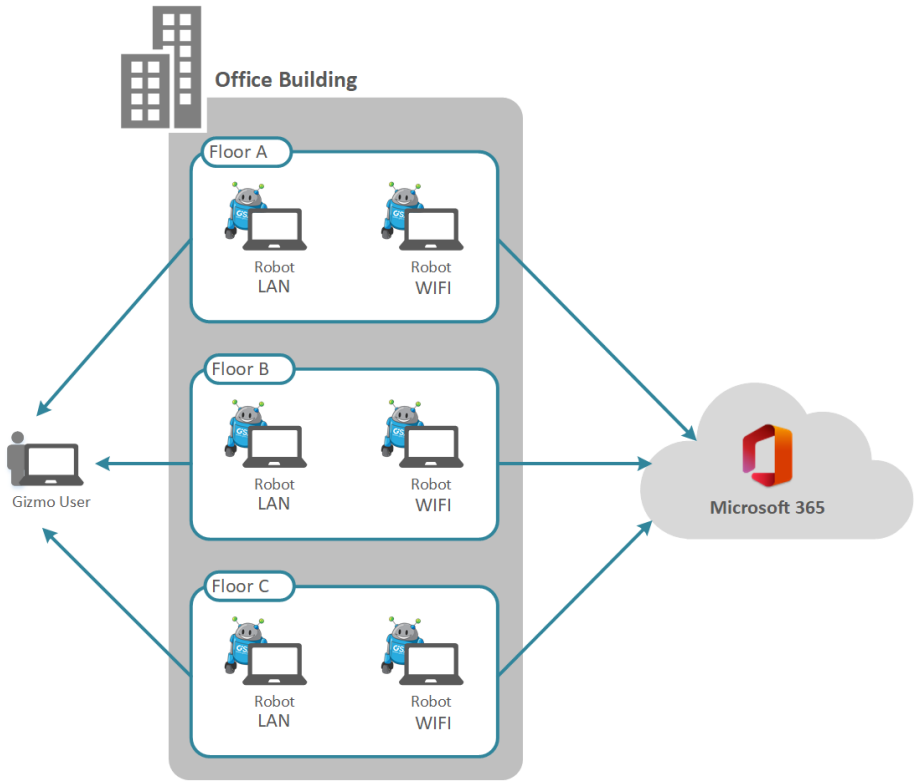
collected by the robots is specific to each floor. You can extend this deployment to include last mile connectivity checks.

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 5: Robot Deployment in an Office Building



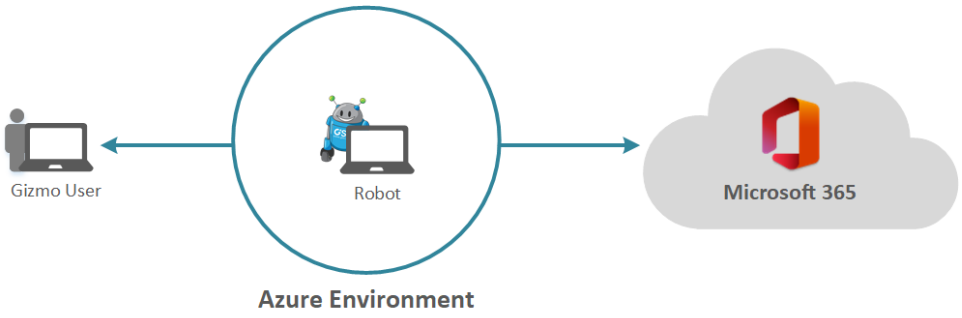
Monitor Cloud Performance

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.

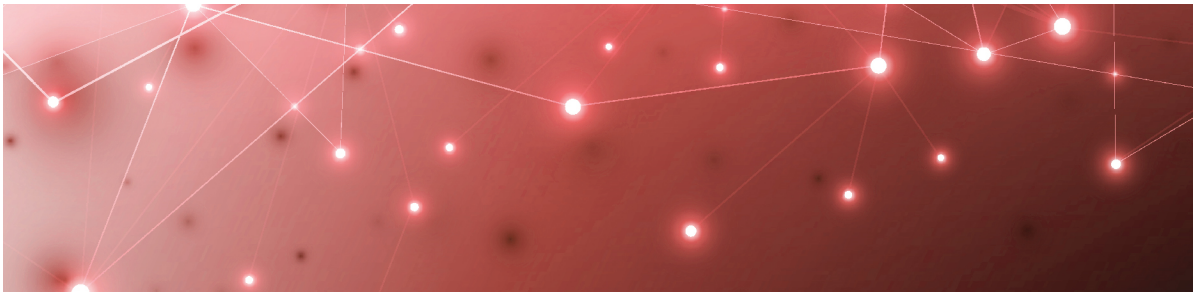
To set up this type of deployment, you need to deploy a robot on a virtual machine in your cloud-based infrastructure.

The following image shows an example of this deployment option.

Figure 6: Robot Deployment to Monitor Cloud Performance



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



CHAPTER 4

Requirements

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

Robot Manager Requirements

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

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 2: 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	A user account with a provisioned mailbox and a set timezone. An attendee user account with a provisioned mailbox and set timezone. 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.
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.

Workload	Account Information
Exchange MAPI	A user account with a provisioned mailbox and a set timezone. An attendee user account with a provisions mailbox and set timezone. 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.
Mail Routing	A user account with a provisioned mailbox and a set timezone.
Office 365 Web Apps	A user account with the intended Office 365 application provisioned. • The account must be cloud-only (ADFS is not supported) • The account must be licensed for the intended Office 365 application
One Drive	Up to 30 robots can use one account. A user account with OneDrive provisioned.
Teams/Teams Advanced	Up to five robots can use one account. You need two user accounts. • 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.  **Tip:** If you are monitoring Teams Advanced from multiple locations, use separate credentials for the robots at each location.

Workload	Account Information
Teams Video	You need two accounts per robot. • 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 section provides information about the requirements that the mail routing workload must meet in order to be correctly monitored.

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:

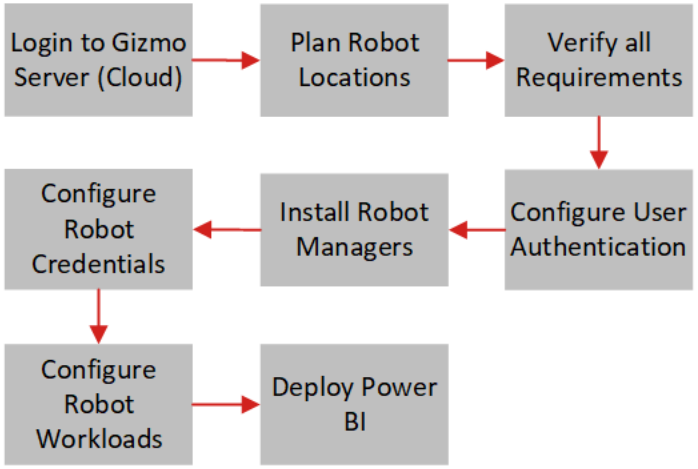
- 4 CPUs
- 8GB of RAM (16GB recommended for large deployments)

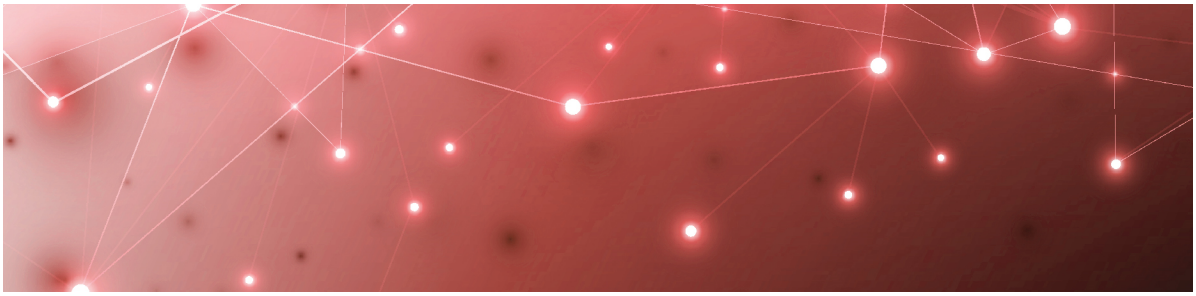
CHAPTER 5

Installation Process

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

Figure 7: Installation Process





CHAPTER 6

Configure User Authentication

Gizmo includes optional authentication features. For cloud deployments, single sign-on is already configured by default. You can also configure Azure Active Directory (AD) to authenticate users and provide role-based access to them.

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.

To set up role-based access to give users access to Gizmo based on their defined role in Azure AD, see "Configure Role-Based Access" on page 26.

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.

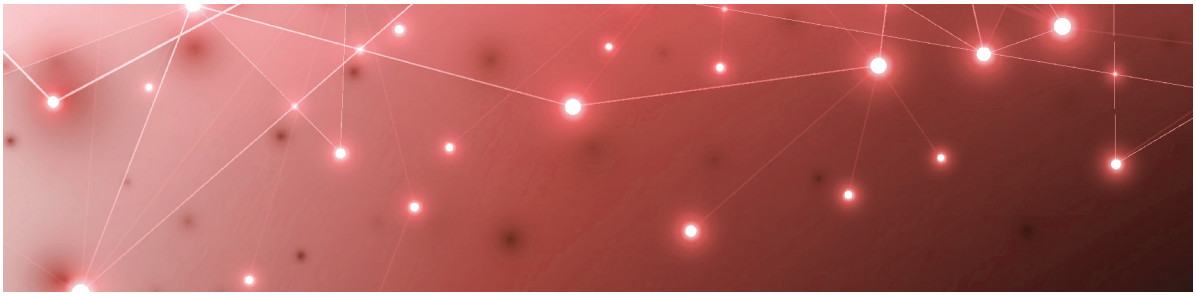
Before you Begin

- 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.

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.



CHAPTER 7

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 28	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 29	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 30	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 and 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/EdDRntvJSodDi8HzDvnW0XUB8RXXydA7zM4JaPqUYEd0uA

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 22.
- Review the Exchange server workload requirements. See "Exchange Server Requirements" on page 1.

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.

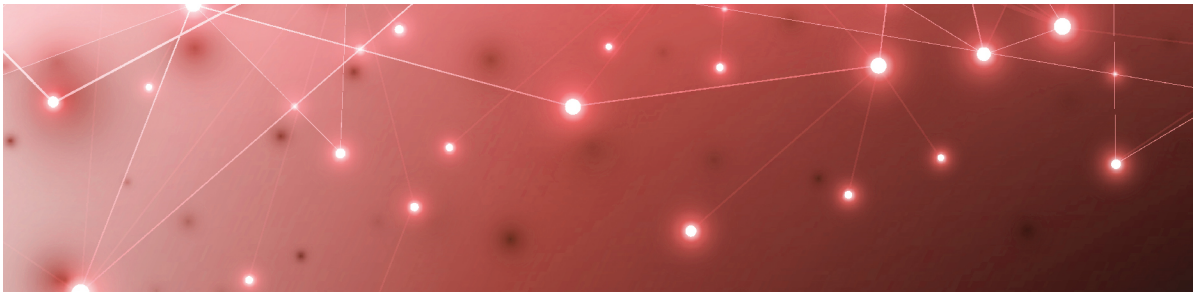
Install Robot Manager

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.



CHAPTER 8

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 3: 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 32	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 32	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 33

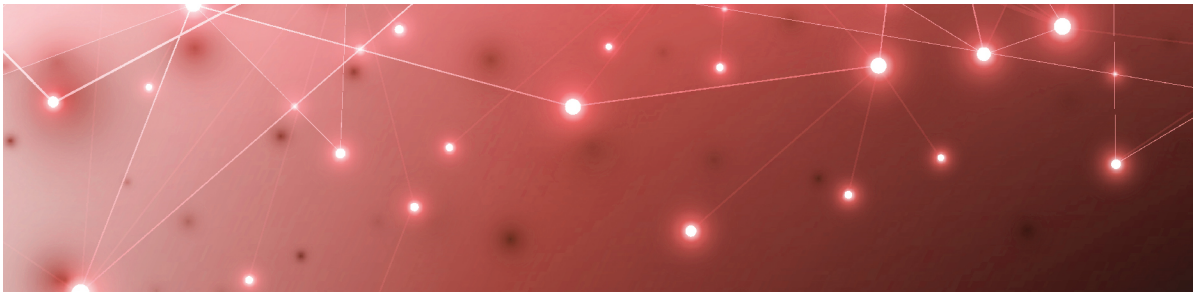
Add Monitoring Credentials

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 22

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 33



CHAPTER 9

Configure Workloads

Complete the tasks in the following table.

Task	Description
"Create Monitoring Configurations" on page 33	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 34	Specify the applications that you want the robots to monitor at each site.
"Add a Location Tag" on page 35	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 34

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 33
- 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.

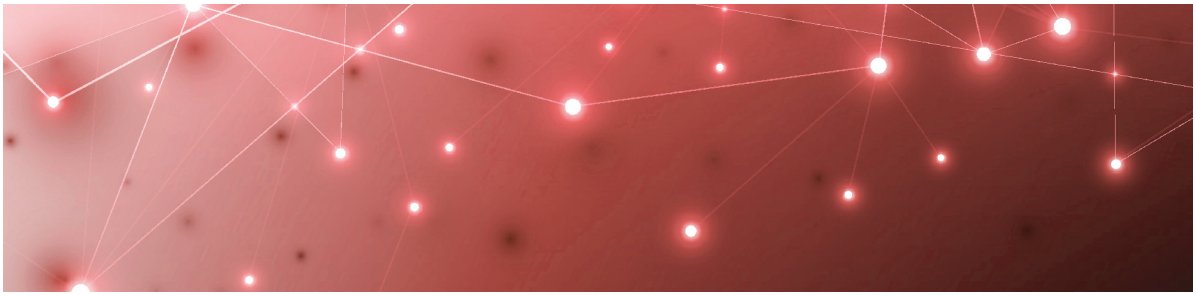
Next Steps

- "Add a Location Tag" on page 35

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**.



CHAPTER 10

Deploy Power BI

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

Task	Description
"Import the Power BI Template for Cloud Deployments" on page 36	Configure the Power BI templates for the workloads that you want to monitor in Gizmo.
"Verify the Power BI Template" on page 1	Ensure that the template installed successfully.

Import the Power BI Template for Cloud Deployments

Use the following procedure to open the Gizmo template in Microsoft Power BI and then configure and import the data source in the Power BI Service. The procedure makes the report data accessible in the cloud.

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

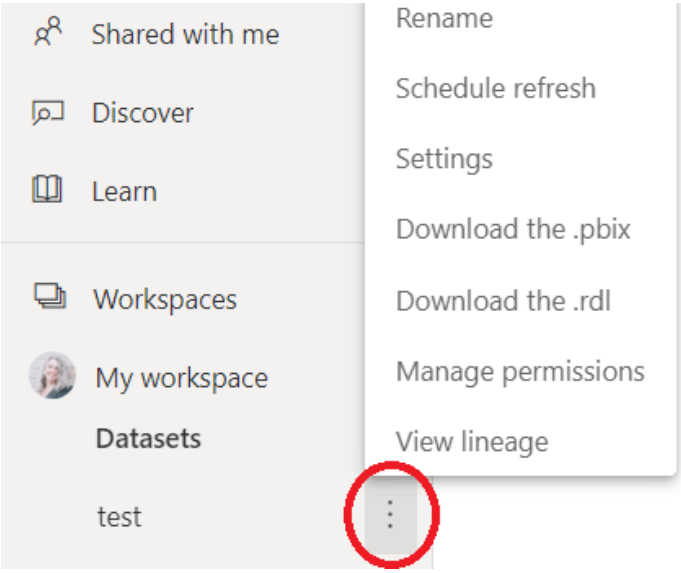
- Download and install the latest version of Power BI. For information and instructions see: https://docs.microsoft.com/en-us/power-bi/fundamentals/desktop-get-the-desktop
- A workspace created in Power BI. See https://docs.microsoft.com/en-us/power-bi/collaborate-share/service-create-the-new-workspaces.
- Ensure that you have the latest version of the Gizmo Analytics Power BI Template. Contact gsx-support@martellotech.com to obtain the template.

- 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.

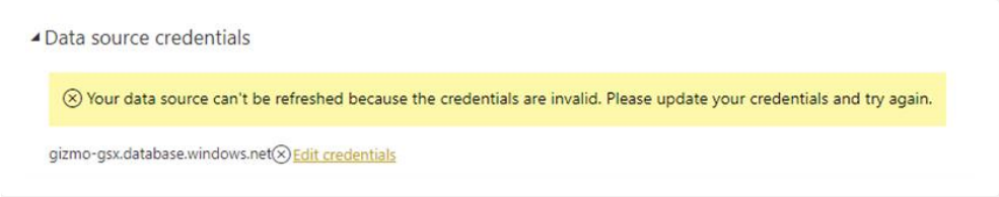
1. Double-click on the `Gizmo Analytics Full-2.1.0.13344.pbit` file to launch load the Power BI template.
2. On the **Gizmo Analytics** page, provide the following information:
   - Server—The SQL server database that is listed in your Welcome email.
   - Database—The name of the database that is listed in your Welcome email.
   - Range Start—Use 01/01/2020 or any date prior to the installation of Gizmo.
   - Range End—Use 01/01/25 or any date later than today's date.
3. If prompted, click the link at the bottom of the **Welcome** page and enter the Power BI license associated with your Office 365 account.
4. On the **Gizmo Analytics** page, click the drop-down next to the **Load** button and select **Edit**.
5. With the Gizmo Power BI template open in Power BI Desktop, from the home menu, click **Publish**.
6. Save the report when prompted.

Warning: If prompted to apply pending query changes, click **Apply Later**.

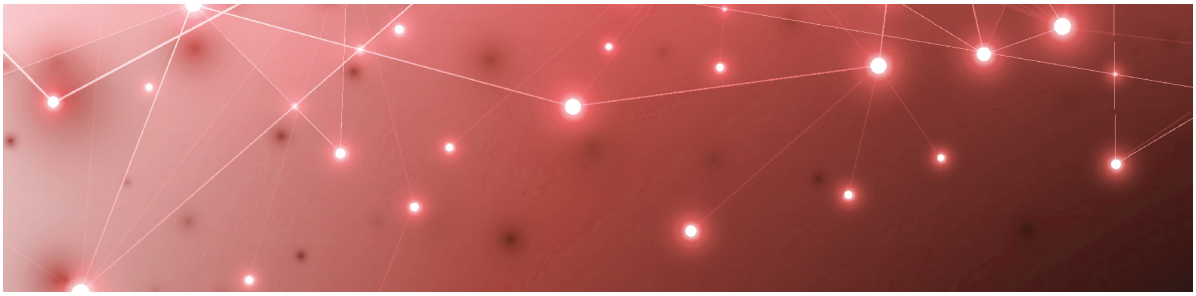
7. Supply your Power BI credentials if prompted.
8. On the **Publish to Power BI** page, click the workspace where you want to share the report, then click **Select**.
9. Once the report is generated, click the link to open the report in Power BI Service.
   Power BI opens in a browser window and the report is displayed.
10. On the left menu pane, scroll down to **My Workspaces >Datasets**, and expand the Datasets menu option.
11. Hover you mouse over the dataset for the report, then click the three vertical dots to display the menu.



12. From the menu, select **Settings**.
13. On the **Datasets** tab, expand the **Parameter** section, provide the following information, then click **Apply**:
    - Database—The SQL server database to use.
    - Server—The name of the database.
14. On the Datasets tab, expand the **Data source credentials** section. If the following error is displayed, click **Edit credentials**:



15. Provide the following user credentials, then click **Sign In**.
    - **Authentication method**: Select the method to use from the list.
    - **User name**: The user name for the data source.
    - **Password**: The password for the data source.
    - **Privacy level setting for this data source**: Select the privacy level to use from the list.
16. Return to the left menu pane, scroll down to **My Workspaces >Datasets**. For the same dataset, click the three vertical dots to open the menu and select **Refresh now**.
17. Wait for the refresh to complete.
    You can view the status of the refresh by clicking the **Refresh history** link on the **Datasets** tab.



CHAPTER 11

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 39	Perform this procedure on each computer where Robot Manager is installed.
"Validate the Upgrade on the Robot Manager Host" on page 40	Perform this procedure on each computer where Robot Manager 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.

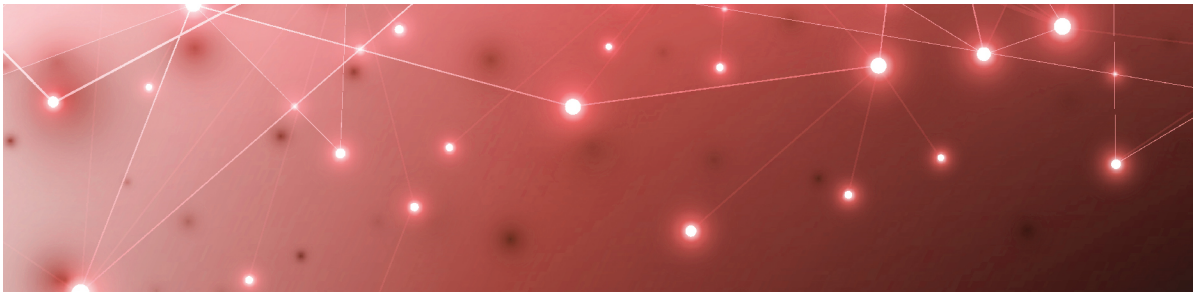
   No specific location is required.
3. Open PowerShell as Administrator.

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.



CHAPTER 12

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.