Goliath Application Availability Monitor for Microsoft RDS Installation Guide

Goliath Application Availability Monitor Proof of Concept Limitations

Goliath Application Availability Monitor Proof of Concepts (POC) will be limited to launching a single Microsoft Remote Desktop Services application or desktop from one location.

If your evaluation or POC process requires a different configuration than the licensing allows for, please contact your account manager or Goliath Sales or Support as follows for assistance:

Sales
Email: sales@goliathtechnologies.com
Phone: 1-855-465-4284

Support
Email: support@goliathtechnologies.com
Phone: 1-855-465-4282

http://www.goliathtechnologies.com

Legal Notices

Goliath Technologies believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." GOLIATH TECHNOLOGIES MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any Goliath Technologies software described in this publication requires an applicable software license.

Linux is a registered trademark of Linus Torvalds.

Windows is a registered trademark of Microsoft Corporation.

VMware, ESX, ESXi, vCenter, and vSphere are either trademarks or registered trademarks of VMware Corporation.

Citrix, Xen, XenServer, and XenCenter are either trademarks or registered trademarks of Citrix Systems Inc.

All other trademarks and copyrights referred to are the property of their respective owners.

Support, Sales, Renewals and Licensing

- For information on new sales, licensing and support renewals you can email sales@goliathtechnologies.com

- For additional information about Goliath Technologies products and services, go to http://www.goliathtechnologies.com

- For customers and partners with an active support agreement, you can use the support web board or email support@goliathtechnologies.com for information about software patches, technical documentation, and support programs.

Note: A valid support agreement is necessary to receive new release and software updates.

Table of Contents

Goliath Application Availability Monitor for RDS Installation Prerequisites

Note: On the Goliath Server, if it is running **Windows Server 2012-2016**, .NET 3.5 needs to be installed from the Features Wizard as .NET 4.5 is not backwards compatible. Goliath can be accessed over the network or WAN to your local computer.

International users: For installations in environments requiring foreign language versions of Windows, Goliath requires that the base installation be performed with the English version of Windows OS. Localization should be done using language packs only, no localized Windows OS install.

Table 1 - Goliath Application Availability Monitor for Citrix System Requirements

Component	Requirement
Goliath Server (please disregard if also using Goliath Performance Monitor)	□ Virtual Machine or Physical Server □ Windows Server 2008 R2 – 2016 64 bit □ .NET 3.5 Framework □ Static IP address □ Minimum of 4 vCPU □ Minimum of 8 GB RAM □ Minimum of 25 GB Disk Available □ **Dependencies**: ○ PowerShell 3.0 ○ Internet Explorer 11
Launch Endpoint	□ **OS**: Windows Server 2008 R2 – 2016 64 bit, Windows 7-10 □ **Resources**: Minimum of 2vCPU and 2 GB RAM □ **Dependency**: Goliath Agent deployed □ **Web Browser**: Internet Explorer 11 □ **User Account Control**: Disabled at the System level, not through Control Panel □ **IE Enhanced Security**: Disabled for Administrators and Users □ **Trusted Sites**: Add RDS Web Access Portal to whitelist for trusted sites and the security zone set to “Low” to bypass file downloads □ **Test Account**: Dedicated test account with rights to RDS applications or desktops to be launched □ **Windows Account**: Dedicated account that must be logged in/disconnected to the endpoint at all times. This can be the same as the RDS account, especially if you’re automating logons using integrated Windows authentication.
Firewall	*Goliath Server* □ HTTPS 443/TCP 80* opened inbound and outbound for web console connection □ TCP 8282* opened inbound for agent connection to agent location *Goliath Intelligent Agent* □ TCP 8282* opened outbound for agent connection to the Goliath Server * Default ports listed and can be modified.

Goliath Service Accounts

Infrastructure Component	Rights	Notes
Launch Endpoint	Local Admin Rights	This can be a local account or a domain account
Full SQL (for Goliath DB)*	DBO	Needs to be applied to the Goliath Database.
Goliath Server*	Local Admin Rights	The account that has DBO rights to the Goliath database will also need local admin rights on the Goliath server.
RDS Launch Account	Access to apps and desktops	Needs rights to launch the applications and desktops

*only needed for Goliath Application Availability Monitor Standalone (not integrated with Goliath Performance Monitor) if using an external database

Goliath Firewall Settings

A. Goliath Intelligent Agent for Launch Endpoint

Source	Destination	TCP Port	Traffic	Notes
Agent Location	Goliath Server	8282	Outbound	Agent connection. Default port listed, port can be modified.

Monitoring Endpoints/Workstations that reside **outside** your network will require the following:

- NAT policy on the firewall to allow agent communication inbound via TCP 8282 (default port, this can be changed)
- Public IP address of the firewall

B. Goliath Application Availability Monitor Server

Source	Destination	TCP Port	Traffic	Notes
(Anywhere)	Goliath Server	8282	Inbound	Agent connection. Default port listed, port can be modified.
(Anywhere)	Goliath Server	80	Inbound	Web console connection. Default port listed, port can be modified.
Goliath Server	(Anywhere)	80	Outbound	Web console connection. Default port listed, port can be modified.

Goliath Antivirus Exclusions/Filters

While not a-typical, we have been exposed to client environments which require antivirus filtering, or exclusion rules needing implemented due to the antivirus software conflicting with the Goliath Intelligent Agent. For that reasoning, we do recommend implementing exclusion rules which consist of the following:

- Directory Exclusions:
  - \Program Files\MonitorIT – This is the install directory of the agent
  - \Program Files (x86)\MonitorIT – This is the install directory of the Goliath Server
- Process Exclusions:
  - RPMAgent.exe – This is the process which is launched by the Agent’s Service
  - RPMCCS.exe – This is the process which is launched by the Server’s Service
  - LogonSimulator.exe – This is the process which is launching the Application Availability Monitor

Are You Ready to Install?

To complete the installation of Goliath Application Availability Monitor, please ensure you have the following items available and prepared:

1. Goliath installation file (**gpmserver_setup64.exe**)
2. Your license key (for POC's the key is **'eval'**)
3. Static IP applied to the server hosting Goliath Performance Monitor
4. .NET 3.5 Installed if using Windows Server 2012 and newer as this is not enabled by default
5. **Confirm all prerequisites listed in section 1 are in place on the Goliath Server and Launch Endpoint**

Goliath Application Availability Monitor Server Installation Steps

In the following section, we will install the Goliath Server. **Please note, the Application Availability Monitor integrates into the Goliath Performance Monitor technology. If you already have this product deployed, please skip this section and proceed to the next section.** The **Setup** program will install the Goliath server on the system you want to be designated as the Server computer.

NOTE: The default installation for evaluations/POC's is to install Goliath with the embedded SQL Express database. If you are evaluating and would like to use a remote SQL Server, please contact your Account Executive or support@goliathtechnologies.com to obtain an appropriate license key.

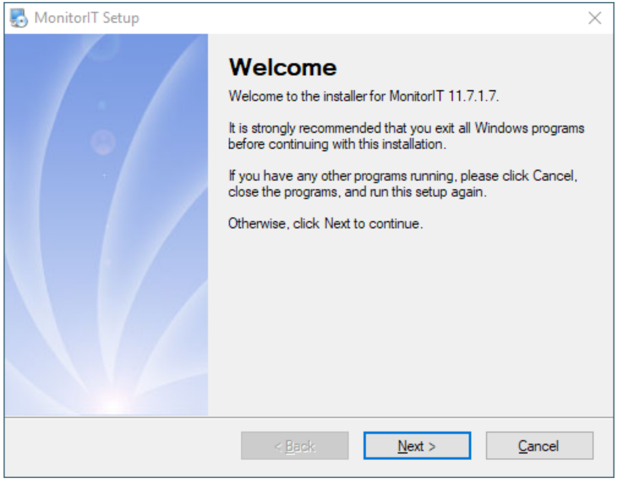
Please be aware at this point, that you will see screens indicating you are about to install **Goliath Performance Monitor**. The Goliath Application Availability Monitor is architecturally integrated into the Goliath Performance Monitor Server. The setup screens will also feature references to Goliath Performance Monitor and MonitorIT, which is correct.

Begin:

1. Exit all programs

2. To install GPM, run the downloaded executable **(gpmserver_setup64.exe)**

3. The executable will start the install process and display a Welcome screen



MonitorIT Setup

Welcome

Welcome to the installer for MonitorIT 11.7.1.7.

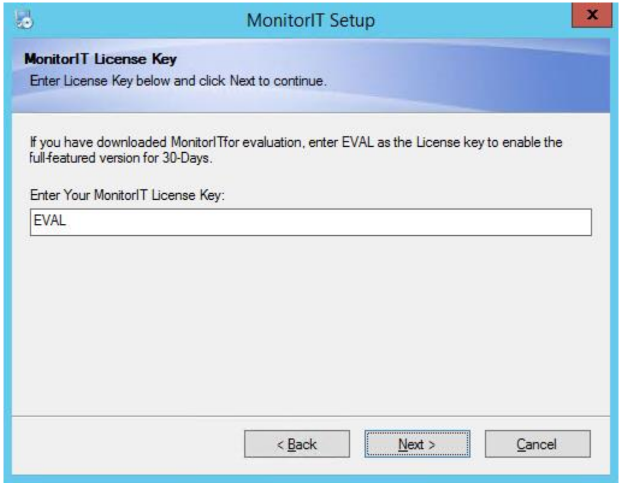
It is strongly recommended that you exit all Windows programs before continuing with this installation.

If you have any other programs running, please click Cancel, close the programs, and run this setup again.

Otherwise, click Next to continue.

4. Click **'Next'** to view the End User License Agreement. Read the agreement and if you agree with the terms, select **'I agree to the terms of this license agreement'** and click **'Next'**. If you do not agree or do not wish to continue, select **'I do not agree to the terms of this license agreement'** and click **'Cancel'** to exit the installer.

5. If you have downloaded Goliath for an evaluation, enter **'EVAL'** as the license key to enable the full featured version for 30 days. If this is not an evaluation, enter your Goliath license key provided by Goliath Technologies and select **'Next'** to continue.



MonitorIT Setup

MonitorIT License Key

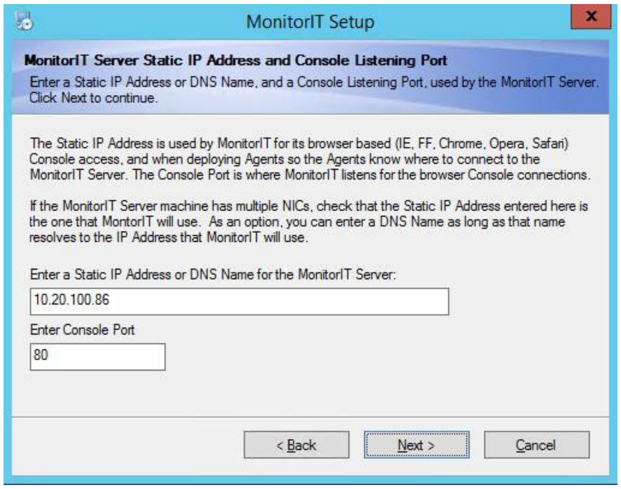
Enter License Key below and click Next to continue.

If you have downloaded MonitorITfor evaluation, enter EVAL as the License key to enable the full-featured version for 30-Days.

Enter Your MonitorIT License Key:

EVAL

6. Please verify and or specify the **'STATIC IP Address'** or **'DNS Name'** for the Goliath Server and Web Interface **'Console Port'**. When finished select **'Next'** to continue.



MonitorIT Setup

MonitorIT Server Static IP Address and Console Listening Port

Enter a Static IP Address or DNS Name, and a Console Listening Port, used by the MonitorIT Server. Click Next to continue.

The Static IP Address is used by MonitorIT for its browser based (IE, FF, Chrome, Opera, Safari) Console access, and when deploying Agents so the Agents know where to connect to the MonitorIT Server. The Console Port is where MonitorIT listens for the browser Console connections.

If the MonitorIT Server machine has multiple NICs, check that the Static IP Address entered here is the one that MontorIT will use. As an option, you can enter a DNS Name as long as that name resolves to the IP Address that MonitorIT will use.

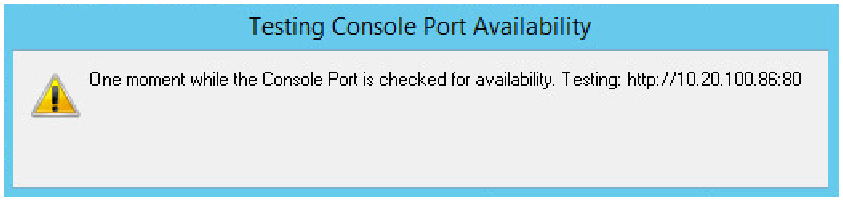
Enter a Static IP Address or DNS Name for the MonitorIT Server:

10.20.100.86

Enter Console Port

80

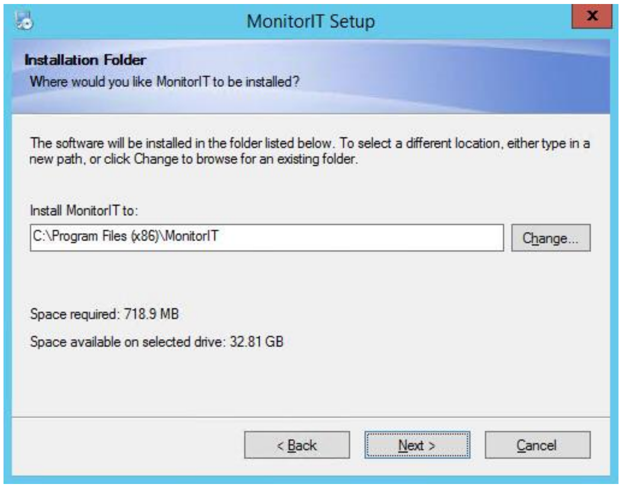
7. Once **'Next'** is selected, the wizard will verify that the **Console Port** is available. If it is, Goliath Performance Monitor will then connect to it.



Testing Console Port Availability

One moment while the Console Port is checked for availability. Testing: http://10.20.100.86:80

8. The next step lets you select where to install the Goliath Performance Monitor program. When the appropriate location is confirmed or entered, click **‘Next’** to continue.
    a. On 64-bit versions of Windows, the default location is **‘C:\Program Files (x86)\MonitorIT’**



MonitorIT Setup

Installation Folder

Where would you like MonitorIT to be installed?

The software will be installed in the folder listed below. To select a different location, either type in a new path, or click Change to browse for an existing folder.

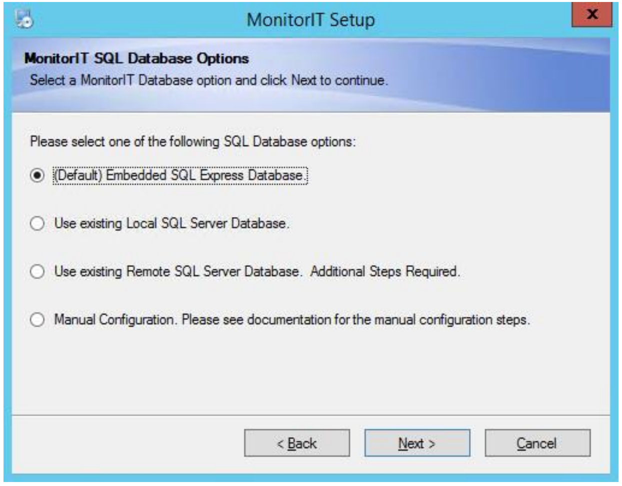
Install MonitorIT to:

C:\Program Files (x86)\MonitorIT

Space required: 718.9 MB

Space available on selected drive: 32.81 GB

9. If this is a full installation with an **official license key,** you will see the following options for configuring the database settings. Please keep the defaulted SQL Express option select and Click **‘Next’**
    a. If this is an evaluation are you are using the **EVAL key**, please move to the next step as this is not applicable.



MonitorIT Setup

MonitorIT SQL Database Options

Select a MonitorIT Database option and click Next to continue.

Please select one of the following SQL Database options:

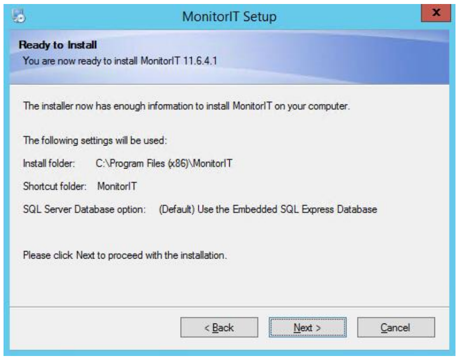
● (Default) Embedded SQL Express Database

○ Use existing Local SQL Server Database.

○ Use existing Remote SQL Server Database. Additional Steps Required.

○ Manual Configuration. Please see documentation for the manual configuration steps.

10. Verify that the following installation settings are correct, if so select **‘Next’** to proceed with the installation or **‘Back’** to make the appropriate modifications.



Ready to Install

You are now ready to install MonitorIT 11.6.4.1

The installer now has enough information to install MonitorIT on your computer.

The following settings will be used:

Install folder: C:\Program Files (x86)\MonitorIT

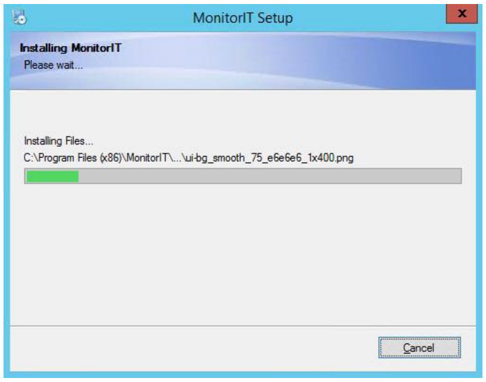
Shortcut folder: MonitorIT

SQL Server Database option: (Default) Use the Embedded SQL Express Database

Please click Next to proceed with the installation.

11. During the installation process, a progress bar will show the progress of installing the Goliath Server, as seen in the figure below. You will also see the installation of the SQL Express database installation take place if applicable.

    Please Note: At some points during the installation your screen may go blank. This is a normal part of the installation process.



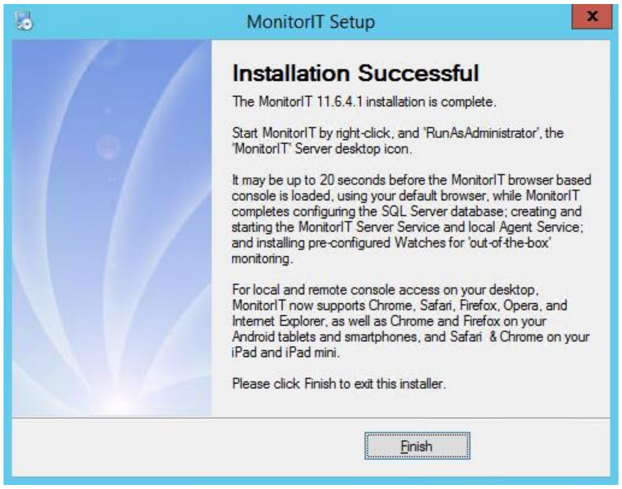
Installing MonitorIT

Please wait...

Installing Files...

C:\Program Files (x86)\MonitorIT\...\ui-bg_smooth_75_e6e6e6_1x400.png

12. Once Goliath and SQL Express are successfully installed the install program will display a message that the installation is complete. Click **'Finish'** to exit the install program.



Installation Successful

The MonitorIT 11.6.4.1 installation is complete.

Start MonitorIT by right-click, and 'RunAsAdministrator', the 'MonitorIT' Server desktop icon.

It may be up to 20 seconds before the MonitorIT browser based console is loaded, using your default browser, while MonitorIT completes configuring the SQL Server database; creating and starting the MonitorIT Server Service and local Agent Service; and installing pre-configured Watches for 'out-of-the-box' monitoring.

For local and remote console access on your desktop, MonitorIT now supports Chrome, Safari, Firefox, Opera, and Internet Explorer, as well as Chrome and Firefox on your Android tablets and smartphones, and Safari & Chrome on your iPad and iPad mini.

Please click Finish to exit this installer.

15. You have successfully installed Goliath Application Availability Monitor and can now launch the application via the Desktop icon.

Post Installation: What's Next?

In the following section, we will discuss the details for configuring the Application Availability Monitor post install. This includes how to prepare your Launch Endpoint to allow simulations to execute, how to configure the simulations, and how to schedule them to run successfully.

> ⚠ **NOTE**: If your instance of Goliath Application Availability Monitor is integrated with Goliath Performance Monitor, for POC purposes the Launch Endpoint can be the same as the Goliath Performance Monitor Server, but for full implementations we do recommend that the instances stay separate.
>
> If you have any questions at any time feel free to reach out to support@goliathtechnologies.com for assistance.

A. Prepare the Launch Endpoint(s)

Now that Goliath Application Availability Monitor (GAAM) is installed, next you'll want to configure the Launch Endpoint. The Launch Endpoint is the server, virtual machine, or workstation in which the Application Availability Monitor will be executing the launches from. For the launch to successfully and consistently run, the following items will need to be completed.

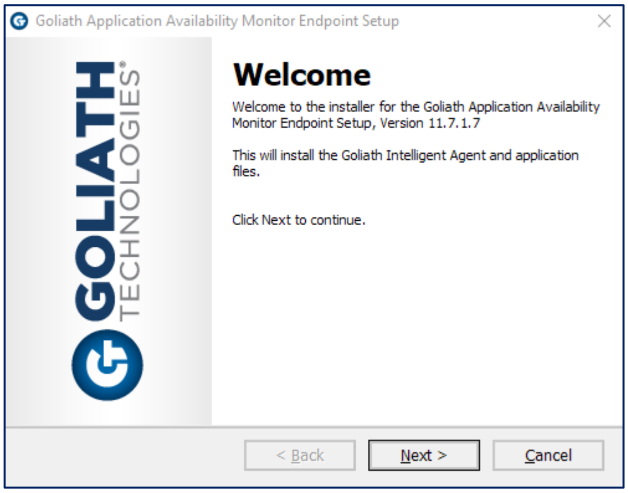
Follow the below steps for the endpoint installer. The installer will configure & confirm the following endpoint prerequisites:

- Disable UAC at the System level
- Install the Goliath Intelligent Agent, if not already installed
- Confirm Internet Explorer 11 is installed
- Start the LogonSimulator.exe process and place it in the startup folder

Instructions:

- On the Goliath Server, navigate to the 'Bin' folder within the install directory.
    a. The default location is 'C:\Program Files (x86)\MontiorIT\Bin'
- Locate the **'GAAMEndpoint'** executable
    a. If the launches will be executing locally on the Goliath Server, launch the executable.
    b. If the launches will be executing on a remote machine:
        i. Log into the machine as the Local Windows Service Account created for GAAM
        ii. Copy over the **'GAAMEndpoint'** executable and launch it

- The executable will start the install process and display a Welcome screen, click **'Next'** to proceed.



Goliath Application Availability Monitor Endpoint Setup

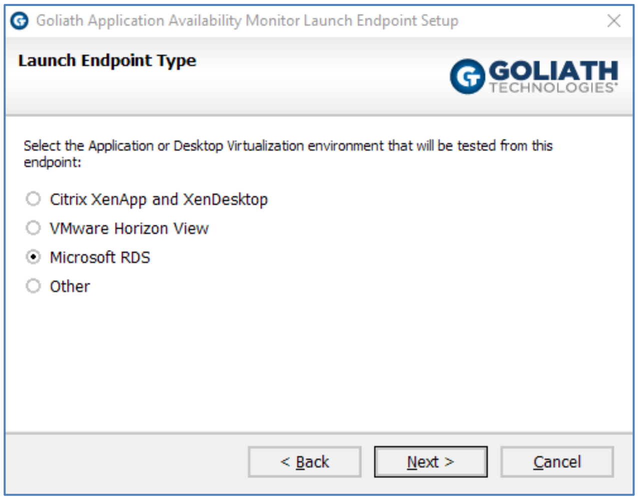
Welcome

Welcome to the installer for the Goliath Application Availability Monitor Endpoint Setup, Version 11.7.1.7

This will install the Goliath Intelligent Agent and application files.

Click Next to continue.

- The installer will prompt for the launch type, Citrix XenApp & XenDesktop is selected by default, choose the option for **'Microsoft RDS'** and then click **'Next'** to proceed



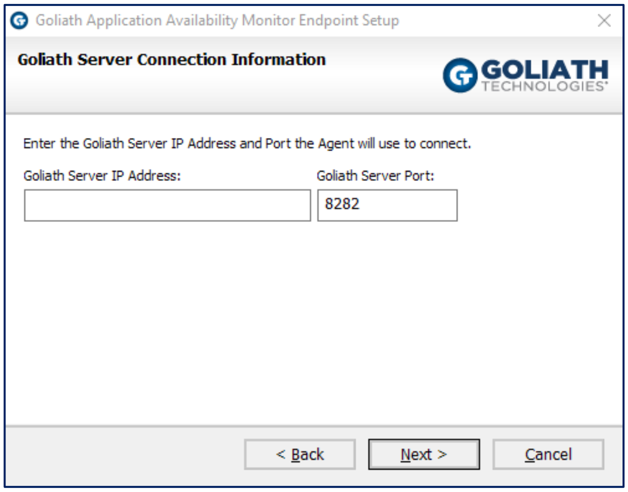
Goliath Application Availability Monitor Launch Endpoint Setup

Launch Endpoint Type

Select the Application or Desktop Virtualization environment that will be tested from this endpoint:

○ Citrix XenApp and XenDesktop
○ VMware Horizon View
● Microsoft RDS
○ Other

- If the launch endpoint is the Goliath Server, proceed to step 6. If the launch endpoint is a remote machine, enter the '**IP Address'** or **'DNS Name'** for the Goliath Server and the port used for agent communication.



Goliath Application Availability Monitor Endpoint Setup

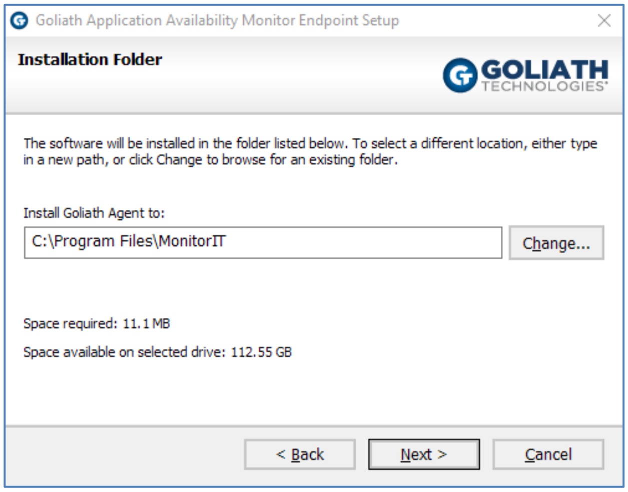
Goliath Server Connection Information

Enter the Goliath Server IP Address and Port the Agent will use to connect.

Goliath Server IP Address:

Goliath Server Port: 8282

- If the launch endpoint is the Goliath Server, proceed to step 6. If the launch endpoint is a remote machine, you will next be prompted to verify the install directory of the



Goliath Application Availability Monitor Endpoint Setup

Installation Folder

The software will be installed in the folder listed below. To select a different location, either type in a new path, or click Change to browse for an existing folder.

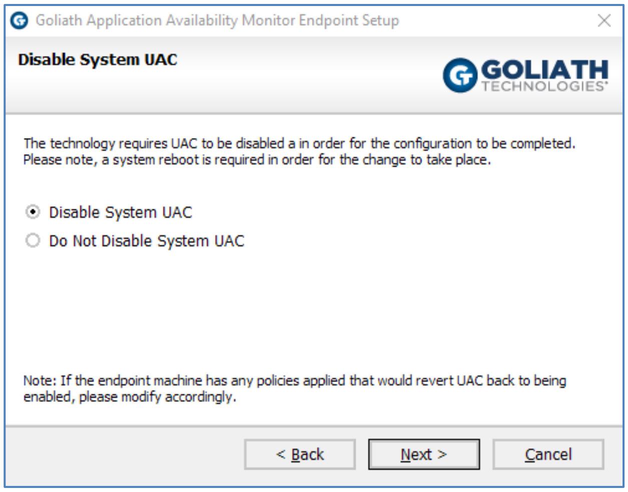
Install Goliath Agent to:

C:\Program Files\MonitorIT

Space required: 11.1 MB

Space available on selected drive: 112.55 GB

- Next, choose if to disable UAC at the system level via the installer. **Please note, a reboot is required in order for the change to take place. Also, if UAC is not disabled the technology will no function and the configuration will be incomplete.**



Goliath Application Availability Monitor Endpoint Setup

Disable System UAC

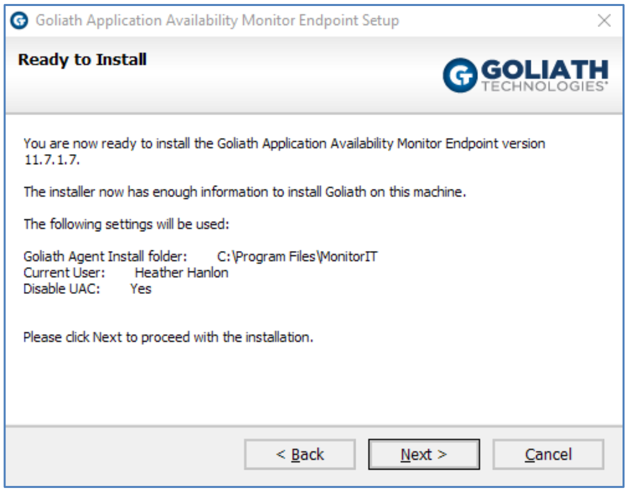
The technology requires UAC to be disabled a in order for the configuration to be completed. Please note, a system reboot is required in order for the change to take place.

● Disable System UAC

○ Do Not Disable System UAC

Note: If the endpoint machine has any policies applied that would revert UAC back to being enabled, please modify accordingly.

- Verify that the following installation settings are correct, if so select **'Next'** to proceed with the installation or **'Back'** to make the appropriate modifications.



Ready to Install

You are now ready to install the Goliath Application Availability Monitor Endpoint version 11.7.1.7.

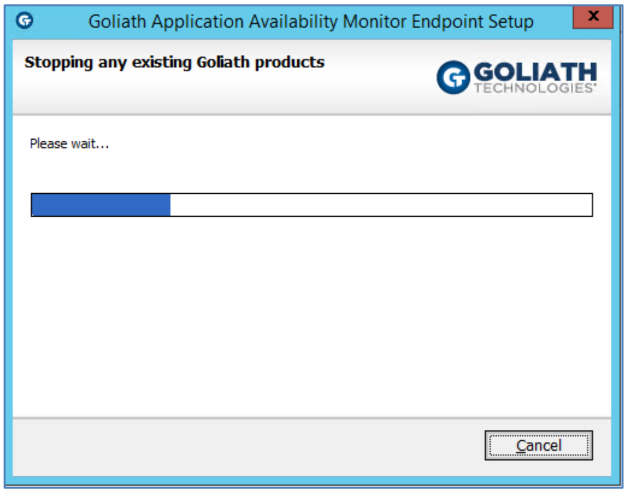
The installer now has enough information to install Goliath on this machine.

The following settings will be used:

Goliath Agent Install folder: C:\Program Files\MonitorIT
Current User: Heather Hanlon
Disable UAC: Yes

Please click Next to proceed with the installation.

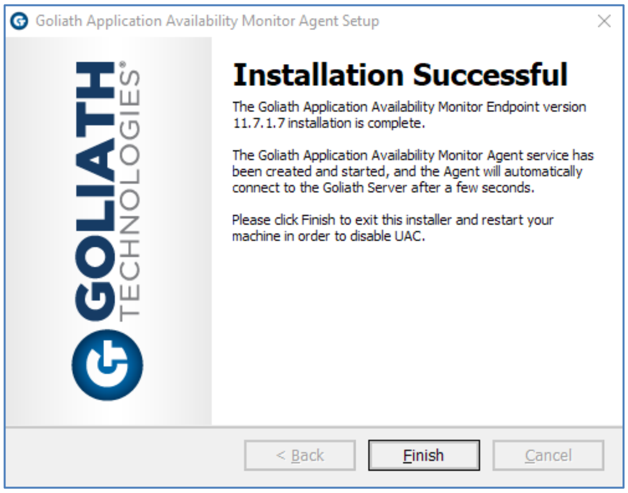
- During the installation process, a progress bar will show the progress of installing the Launch Endpoint, as seen in the figure below.



Stopping any existing Goliath products

Please wait...

- Once the Launch Endpoint is successfully installed the install program will display a message that the installation is complete. Click 'Finish' to exit the install program.



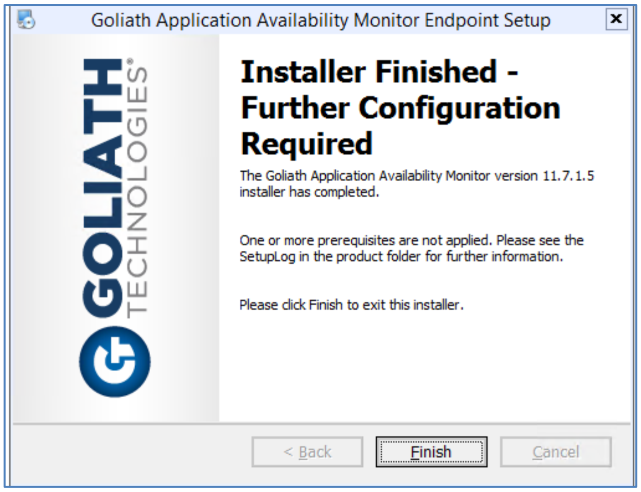
Installation Successful

The Goliath Application Availability Monitor Endpoint version 11.7.1.7 installation is complete.

The Goliath Application Availability Monitor Agent service has been created and started, and the Agent will automatically connect to the Goliath Server after a few seconds.

Please click Finish to exit this installer and restart your machine in order to disable UAC.

If the Launch Endpoint is not fully installed the install program will display a message that the installation requires further configuration.



Installer Finished - Further Configuration Required

The Goliath Application Availability Monitor version 11.7.1.5 installer has completed.

One or more prerequisites are not applied. Please see the SetupLog in the product folder for further information.

Please click Finish to exit this installer.

This message can if any/all of the below are missing:

- End User Opted out of Disabling UAC
- Internet Explorer version 11 is not found on the machine

This information can be found in the SetupLog located in the install directory. Sample log details:

- Lastly, the Web Access Site that will be launched need to be added to Internet Explorers 'Trusted Sites'. Please see the following instructions for modifying the settings.
  i. Open Internet Explorer
  ii. Click the gear icon and select the menu option for 'Internet Options'
  iii. Navigate to the 'Security' tab, and select the 'Trusted Sites' zone
  iv. Click the 'Sites' button, add your Citrix portal address and click close when finished
  v. Under 'Security level for this zone' move the slider down to the lowest possible setting
  vi. Lastly, click 'Apply' and then 'OK' to save these settings

- Optionally, Goliath recommends configuring Automatic Logons for the Windows Service Account so that if the endpoint machine is ever shut down or restarted, the service account will be logged back in automatically and the launches will be resumed. This can be done by:
  a. Navigating to the install directory:
     i. Default location is 'C:\Program Files\MonitorIT'
  b. Opening the folder labeled 'AutoLogon'
  c. Launching the 'AutoLogon' executable and following the on-screen prompts

B. Configure the Launches

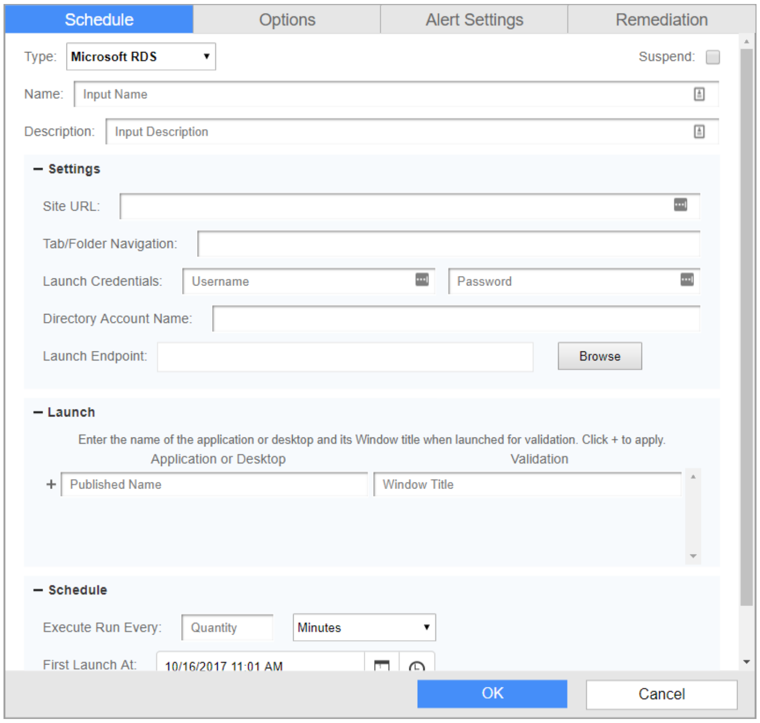
Now that the prerequisites are taken care of, in this section we will create the launch conditions, test the launches and cover some common troubleshooting steps. Please note, it is important to do a manual launch of the applications/desktops on the Launch Endpoint as you are configuring the simulations to verify all settings and bypass any prompts.

Create a New Launch

- Open the Goliath console
- Navigate to the **'Application Availability'** tab and then choose **'Schedule'**
- Click **'New'** at the bottom of the page and a pane will appear with multiple tabs at the top
- Starting with the default **'Schedule'** tab, please enter the appropriate data for each field:

Field Name	Description
Type	Use the drop-down menu and select the option for 'Microsoft RDS'
Name	The unique name to identify the launch
Description	Description of the launch
Site URL	The URL of your RDS Web Access
Tab/Folder Navigation *(optional)*	If the app/desktops reside in a tab and or folder that is not the default page once the user logs in, please define the path to the Application and or Desktop.
Launch Credentials	Microsoft RDS credentials for GAAM service account. These must be entered the same exact way they will be entered into the Web Access site
Directory Account Name	Enter the Microsoft RDS username in the format of DOMAIN\username.
Launch Endpoint	The machine in which the launches will be executing
Application or Desktop & Validation	Enter the information for the Applications and or Desktops that you would like to launch in the 'Application or Desktop' field and then the Window Title in the 'Validation' field. Click the '+' symbol to complete the add and repeat the above for each app/desktop. **Please Note:** • Application and Desktop must be entered the exactly as they appear on the Web Access site but are not case sensitive. • The window title only needs to be a partial match. If the application does not have a window title, one does not need to be defined. • GAAM will launch the apps/desktops in the order in which you define them. • The applications/desktops defined in a given launch must reside in the same location on the Web Access site (i.e. folder/tab)
Execute Run Every	Frequency in which the launch will execute. It is important to make sure that your scheduled launches have the appropriate time to execute and logoff properly before another one begins. Once this launch is saved Goliath with display the maximum launch time and will display any launch conflicts. The maximum simulation time is the amount of time the simulation would take to execute if all the apps/desktops configured were to fail.
First Launch At	Define the Date & Time in which the first launch will execute. Future launches will execute based on the 'run every' schedule defined above
Launch Duration	To alert on the launch duration of an app/desktop, the time from app click to GAAM

(optional)	identified successful, enter the threshold.
Severity *(optional)*	Criticality ranking
Alert 1st time after *(optional)*	To alert have multiple failures, instead of the first, enter the number in which the alert should be sent. I.E., 2 failures in a row.
Notify on Restore *(optional)*	Check the box to receive an alert notification when a launch changes from a failed state to a success state.



Type: Microsoft RDS

Suspend: □

Name: Input Name

Description: Input Description

− Settings

Site URL:

Tab/Folder Navigation:

Launch Credentials: Username Password

Directory Account Name:

Launch Endpoint:

− Launch

Enter the name of the application or desktop and its Window title when launched for validation. Click + to apply.

Application or Desktop	Validation
+ Published Name	Window Title

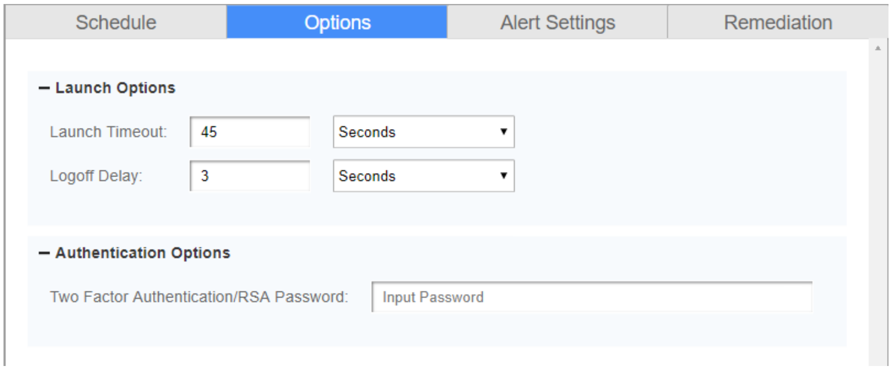
− Schedule

Execute Run Every: Quantity Minutes

First Launch At: 10/16/2017 11:01 AM

- On the ‘**Options**’ tab, the following settings can be applied if applicable:

Field Name	Description
Launch Timeout	This is the threshold for whether or not the simulation is a success or failure. If any stage of the simulation process exceeds this threshold the simulation will report back as failed.
Logoff Delay	Once the simulation has been deemed a success, the session will delay to logoff after the defined number plus 60 seconds. Therefore, if you’d like to keep the session open for 2 minutes, you’d input 60 into this field.
Two Factor Authentication/ RSA Password *(optional)*	If multifactor authentication is used, please enter the static token in this field. Please note, if this is your configuration we suggest contacting the Goliath Support team as some customer specific modifications may be needed.



− Launch Options

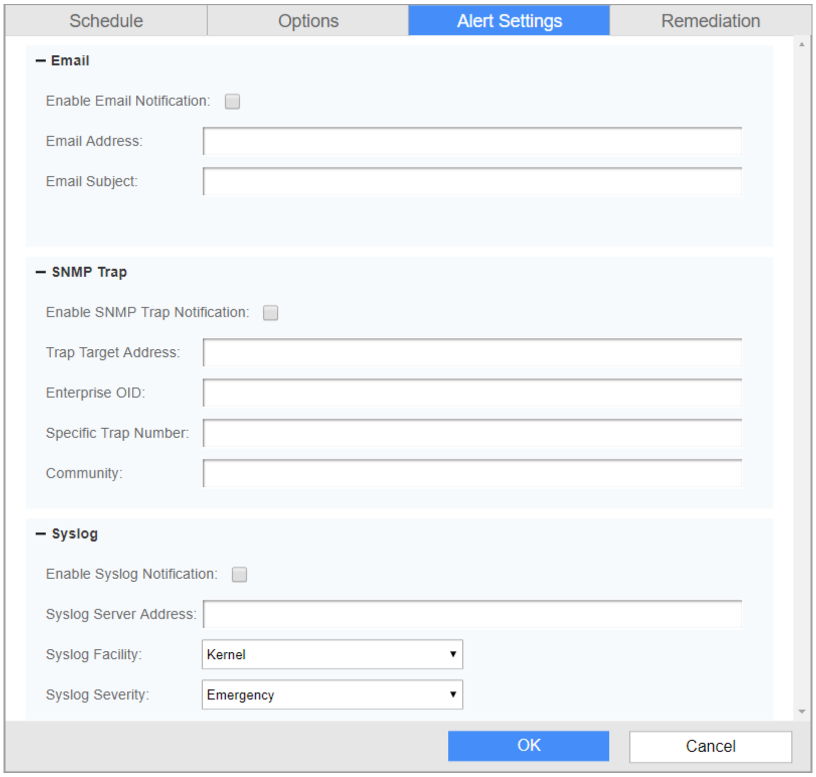
Launch Timeout: 45 Seconds

Logoff Delay: 3 Seconds

− Authentication Options

Two Factor Authentication/RSA Password: Input Password

- To configure alert notifications, choose the **'Alert Settings'** tab. Configure the below settings as appropriate
  - **Email** - Please see Appendix E for creating custom email groups & defining the SMTP Server Parameters
    - Select the checkbox to enable email notifications
    - Define a comma delimited list of email addresses or Goliath Email Groups
    - Define the email subject
  - **SNMP Trap -** Please see Appendix E for SNMP Trap prerequisites
    - Select the checkbox to enable SNMP Trap notifications
    - Enter the IP Address or FQDN of the machine that Goliath is sending the Trap notifications to
    - Enter **'1.3.6.1.4.1.50410.9'** into the Enterprise OID field. '50410' is the Goliath designation, that is registered with IANA and represents Goliath Technologies. The proceeding '9' represents the Goliath Application Availability Monitor
    - Specify the unique Trap Number for the notification
    - Define the community string used for SNMP Traps
  - **Syslog**
    - Select the checkbox to enable Syslog notifications
    - Enter the IP Address or FQDN of the machine to which Goliath is sending the notification
    - Using the **'Syslog Facility'** drop down menu, chose the so-called Facility that defines where the Syslog message is originating. This field is used in conjunction with the Severity field to form the syslog message priority code.
    - For the **'Syslog Severity'** drop down menu, chose the so-called Severity that defines the severity level of the Syslog message. This field is used in conjunction with the Facility field to form the syslog message priority code.



Email

Enable Email Notification: □

Email Address:

Email Subject:

SNMP Trap

Enable SNMP Trap Notification: □

Trap Target Address:

Enterprise OID:

Specific Trap Number:

Community:

Syslog

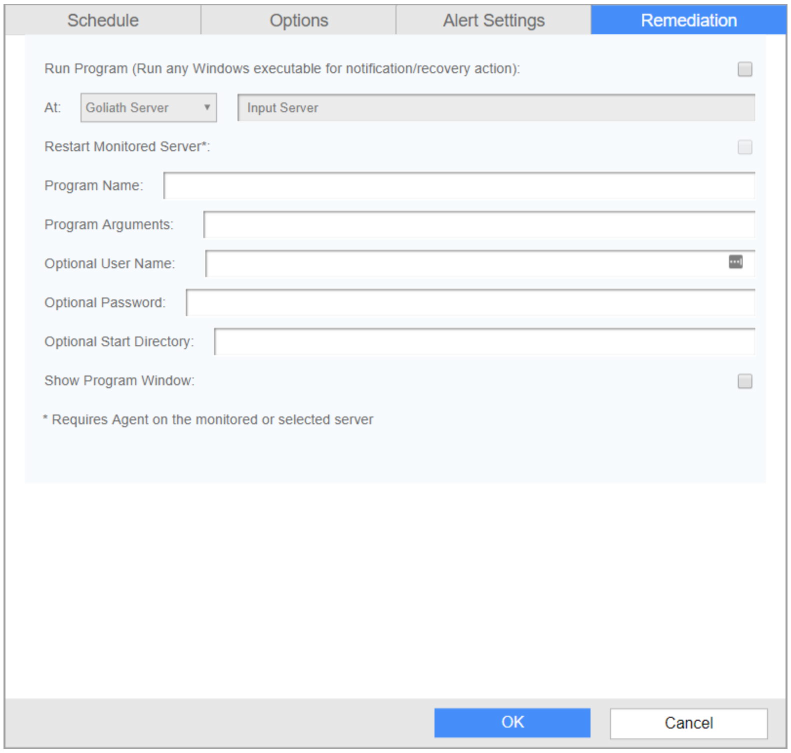
Enable Syslog Notification: □

Syslog Server Address:

Syslog Facility: Kernel

Syslog Severity: Emergency

- To configure remediation and self-healing actions, select the last tab labeled ‘Remediation’. Please follow the link below for full documentation.
  - Remediation Documentation



Run Program (Run any Windows executable for notification/recovery action): □

At: Goliath Server Input Server

Restart Monitored Server*: □

Program Name:

Program Arguments:

Optional User Name:

Optional Password:

Optional Start Directory:

Show Program Window: □

* Requires Agent on the monitored or selected server

- **Test the Launch**

  We suggest scheduling a launch to run right away and watching it take place the first time through. This is to validate that the launch is configured properly and to also make sure that nothing interrupts the Application Availability Monitor. Once this has been done one can go back in and configure its normal launch sequence/frequency.

  .

  Common examples are:

  - prompt to download the mstsc file
  - Incorrect application name or window title

C. Launch Scheduling

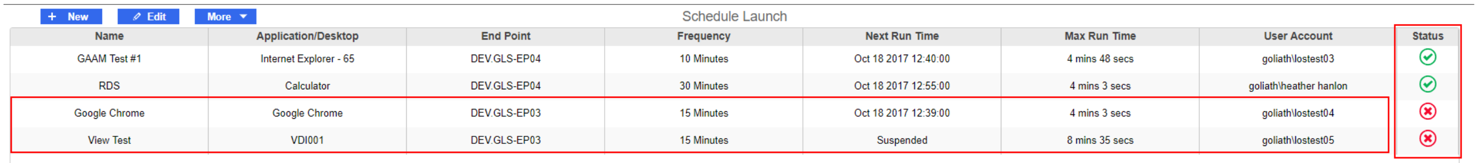
Launch Scheduling is a key part in ensuring that the launches will be successful. There are 2 main factors to follow for scheduling:

1) There can't be more than one launch running on the same launch endpoint at the same time.
2) The launch user account can't be running on more than one launch endpoint at the same time.

The technology has built in assistance to help one determine if condition #1 is going to happen. When a launch is created, Goliath uses an algorithm to determine the maximum amount of time that it would take the launch to execute (max run time). This is maximum run time is the time from launch start to finish if there was a failure for all apps/desktops within the launch. The algorithm takes into consideration:

- The number of apps/desktops being launched
- The launch timeout threshold
- The Web logoff delay

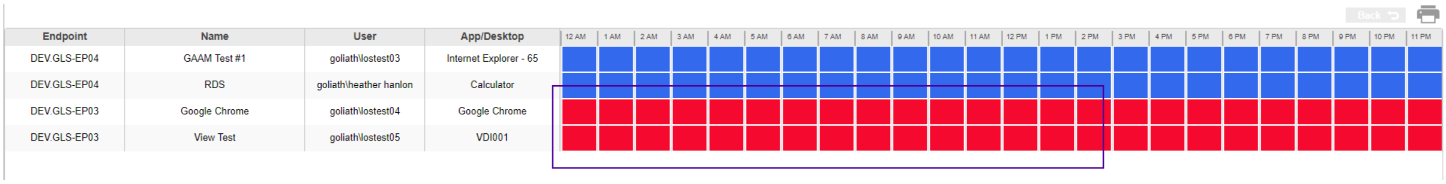
Once a new launch is created and saved, on the 'Schedule' page one will see the launch details at the bottom of the page. With the launch details, there is a column names 'Status'. The status column will have a green check box if the launch has no conflicts with another previously scheduled launch. However, if a conflict is going to occurring, the status icon will change to a red 'X' for the multiple launches that will be affected. Please note, suspended launches are still taken into consideration.



Schedule Launch

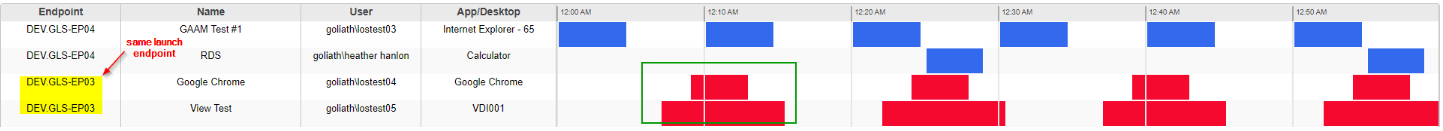
Name	Application/Desktop	End Point	Frequency	Next Run Time	Max Run Time	User Account	Status
GAAM Test #1	Internet Explorer - 65	DEV.GLS-EP04	10 Minutes	Oct 18 2017 12:40:00	4 mins 48 secs	goliath\lostest03	✓
RDS	Calculator	DEV.GLS-EP04	30 Minutes	Oct 18 2017 12:55:00	4 mins 3 secs	goliath\heather hanlon	✓
Google Chrome	Google Chrome	DEV.GLS-EP03	15 Minutes	Oct 18 2017 12:39:00	4 mins 3 secs	goliath\lostest04	⊗
View Test	VDI001	DEV.GLS-EP03	15 Minutes	Suspended	8 mins 35 secs	goliath\lostest05	⊗

In addition to the launch schedule status showing a red status icon, the grid at the top of the schedule page will also change from blue to red.



Endpoint	Name	User	App/Desktop	12 AM	1 AM	2 AM	3 AM	4 AM	5 AM	6 AM	7 AM	8 AM	9 AM	10 AM	11 AM	12 PM	1 PM	2 PM	3 PM	4 PM	5 PM	6 PM	7 PM	8 PM	9 PM	10 PM	11 PM
DEV.GLS-EP04	GAAM Test #1	goliath\lostest03	Internet Explorer - 65	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
DEV.GLS-EP04	RDS	goliath\heather hanlon	Calculator	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
DEV.GLS-EP03	Google Chrome	goliath\lostest04	Google Chrome	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
DEV.GLS-EP03	View Test	goliath\lostest05	VDI001	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥

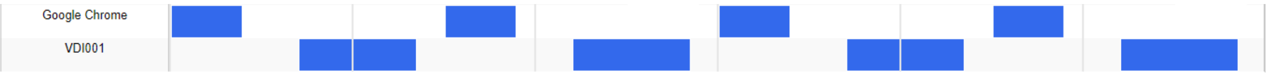
The purpose of the grid at the top of the schedule page is to assist one with resolving a launch conflict. The grid at the top of the page is displaying a 24-hour time line. The boxes that change from blue to red are indicating that there is a conflict within that hour time period. If you click on one of the boxes, it will drill down into a 1-hour period which will display the exact time line.



Endpoint	Name	User	App/Desktop
DEV.GLS-EP04	GAAM Test #1	goliath\lostest03	Internet Explorer - 65
DEV.GLS-EP04	RDS	goliath\heather hanlon	Calculator
DEV.GLS-EP03	Google Chrome	goliath\lostest04	Google Chrome
DEV.GLS-EP03	View Test	goliath\lostest05	VDI001

same launch endpoint

Looking at the above screenshot, one can see that 'Google Chrome' is launch every 15 mins and has a duration of 4 mins and 3 seconds, where 'VDI001' is also launch every 15 mins, but has a duration of 8 mins and 35 seconds. One can also visibility identify that they conflict from 3:09- 3:13. To resolve the conflict, one should change the start of the Google Chrome launch from the 9-minute hour mark to the top of the hour, where there is an opening. In making that adjustment the launches now look like this and no longer overlap:



Also, if one hovers over the boxes on the grid a tool tip will appear that display the start and end time of the launch.

D. Understanding the Launch Results

Once the launches have completed, the GAAM Analysis includes all the results for the most recent simulations, as well as a historical lookback to previous launches. Please note, launch details can also be reported on.

- **Navigating to the Analysis page**
  1. Open the Goliath Console
  2. Click the 'Application Availability Monitor' tab
  3. Select the option for 'Analysis'

- **Analyzing/Understanding the Simulation Results**
  - Successful launches will appear in green and failed simulations will appear in red in the 'Availability' Column.
  - You can drill into the simulation details by selecting the button in the 'Details' column
  - Launch Details Information:

Message	Description
SF Resources Page Not Found	This error is indicative of the Logon Simulator being unable to confirm that it has successfully signed into Storefront successfully. This error can manifest for 2 reasons, first is invalid user credentials and the second is the storefront server is down and not accepting logins as the simulator was unable to reach the storefront page.

Resource '________' Not Found	This error entails that the Logon Simulator was unable to find the defined application/desktop on the Storefront page. When first deploying the simulator, please ensure that application/desktop is spelled correctly and matches the content on the page exactly. If the resource is spelled correctly, we often suggest our customers to do an 'Inspect Element' of the resource to ensure there is no hidden space characters that may not be visible.
WARNING: Unable to confirm that session launched for Resource = '__' and Title= '__'	This error is the result of the Logon Simulator being unable to confirm that the session has been successfully launched. Once the simulator clicks on the application/desktop, next the simulation will confirm that the session did indeed launch by using the defined window title for the application/desktop. If any windows open instead of the application, ie an error prompt, the window title will be included the lines above this message. Also, confirm that the 'Wasp.dll' file is in place on the endpoint.
Try#__ Waiting	This is an informational message, not an error message. With the simulation configuration process, a 'Launch Timeout' value is defined. This value is the threshold that is used for the stages of the Logon Simulation. If any stage of the simulation process, ie loading the page, signing in, finding the application, etc, exceeds the threshold the simulation is deemed as a failure. The 'Try' messages simply countdown how long it takes each stage to execute. If the 'try' reaches the value of the launch timeout a failure will occur.
Unable to Start the Logon Simulator Powershell Command and Script for App=……	This message entails that the Logon Simulator was unable to start. Please check and make sure all prerequisites are in place as well as that all default fields are entered into the configuration.
Blank	This means that the simulation could not start due to an invalid or missing parameter. Please check and make sure all required fields in the simulation rule are filled in appropriately. Also, please make sure that User Account Control is turned off on the Launch Endpoint. This can be confirmed by opening a command prompt (with normal privileges) and checking the window name. If it starts with "Administrator:", UAC is off.

Appendix

A. Agent Install

1. Start up and sign into the Gold Image
2. Open the web browser
3. Navigate to ***http://nn.nn.nn.nn:##/InstallAgent.exe*** where **nn.nn.nn.nn** is the IP Address or FQDN of the Goliath Server and **##** is the web port for the Goliath Server. If you are unsure of the IP Address or FQDN of the Goliath Server, please see the instructions in Appendix B on how to obtain it. If you are unsure of the web port for the Goliath Server, please see the instructions in Appendix D on how to obtain it.

B. Determining the Goliath Server IP Address/FQDN

1. Sign into the Goliath Server
2. Navigate to the install directory of Goliath Performance Monitor. The default location is **C:\Program Files (x86)\MonitorIT**
3. Open the Bin directory
4. Launch **'MonitorITCFU.exe'** as administrator
5. Within the application, go to File and Open
6. Navigate to the Bin directory of the Goliath Performance Monitor install directory. The default location is **C:\Program Files (x86)\MonitorIT\Bin**
7. Select the file named **'default.btc'** to open
8. The Goliath Server IP address or FQDN is in the **'Server IP Addr'** field

C. Determining the Goliath Agent Port

1. Sign into the Goliath Server
2. Navigate to the install directory of Goliath Performance Monitor. The default location is **C:\Program Files (x86)\MonitorIT**
3. Open the Bin directory
4. Launch **'MonitorITCFU.exe'** as administrator
5. Within the application, go to File and Open
6. Navigate to the Bin directory of the Goliath Performance Monitor install directory. The default location is **C:\Program Files (x86)\MonitorIT\Bin**
7. Select the file named **'default.btc'** to open
8. The Goliath Agent port is in the **'Agent Port'** field.

D. Determining the Goliath Web Port

1. Sign into the Goliath Server
2. Navigate to the install directory of Goliath Performance Monitor. The default location is **C:\Program Files (x86)\MonitorIT**
3. Open the Bin directory

4. Launch **'MonitorITCFU.exe'** as administrator
5. Within the application, go to File and Open
6. Navigate to the Bin directory of the Goliath Performance Monitor install directory. The default location is **C:\Program Files (x86)\MonitorIT\Bin**
7. Select the file named **'default.btc'** to open
8. The Goliath Agent port is in the **'Web Port'** field.

E. Alert Notification Information

This section will cover the additional items related to alert notifications.

1. Email – Configure SMTP Server Parameters

- In the technology, select the 'Settings' Link in the top right-hand corner
- In the 'User & Email' section, choose the option for 'Email SMTP Setup'
- A pop-up window will open, on this page you will define the following:
  - Specify the **SMTP server address** for where emails should be sent for transmission. This can be an IP address or a domain name. The default port for the SMTP server is 25, to override this default port, append a colon character followed by the override port number. For example, to use port 26 versus the default port 25, "192.168.1.100:26" or "mail:26".
  - Specify the **originating Email address** in the format of *name@mydomain.com*
  - If your SMTP Server requires authentication, check the box at the bottom of the page and enter the username and password credentials for the originating email address in the two fields. The username must be in the format of name@mydomain.com
- When finished, click the 'OK' button. The Goliath server will then validate a connection to the SMTP server.
- This information is then saved Globally and will not need to be defined again.
- Please note, is you are using Office 365 or another hosted mail provider please email support@goliathtechnologies.com to receive the appropriate instructions as the configuration is slightly different.

2. Email – Create Custom Email Groups

- In the technology, select the 'Settings' Link in the top right-hand corner
- In the 'User & Email' section, choose the option for 'Email Group Management'
- From the Create and Manage Email Groups pop-up, you will see a drop-down list of the current email groups configured. If there are no email groups configured the drop-down will be blank. One can:
  - To **edit** an existing email group, click the 'Manage' button. A new window will appear, use the dropdown list at the top to choose the group you would like to edit and then click the 'Edit' button at the bottom of the page. From there one can define the group name and add in the recipients.
  - To **create** a new email group, click the 'New' button at the bottom of the page. From there one can then add/remove emails/phone numbers

3. SNMP Traps – Prerequisites

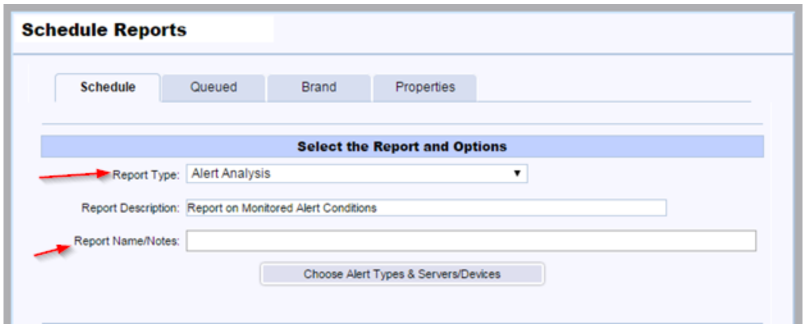
- On the Goliath Server, ensure that the SNMP Service Feature is installed. If is it not, please install it using **‘Add Roles and Features’** in Server Manager
- Once the SNMP Service is installed ensure that it is running
- Right click the service and choose **‘Properties’**
- Navigate to the **‘Security’** tab, on this tab verify that:
  - The **‘Send Authentication Trap’** checkbox is enabled
  - In the ‘accepted community names’ field that the community string has been added and has at least ‘read only’ rights
- Next, navigate to the **‘Traps’** tab, on this tab verify that:
  - The community string is defined in the **‘Community Name’** drop-down list
  - The IP Address or FQDN of the machine that Goliath is sending the Trap notifications to is added into the **‘Trap Destinations’** field

F. Reporting

To see historical launch results, there is a report that can be generated. The report will list all the launches that succeeded or failed and will also contain a copy of all the logs in collapsible frames. These reports can be scheduled or ran on-demand.

Schedule a GAAM Report:

1. Click the **‘Report’** tab and then select the **‘Schedule’** submenu
2. Once the Schedule page is fully loaded, choose the **‘Alert Analysis’** report type
3. In the **‘Report Name/Notes field’**, enter **‘Goliath Application Availability Monitor Report’**

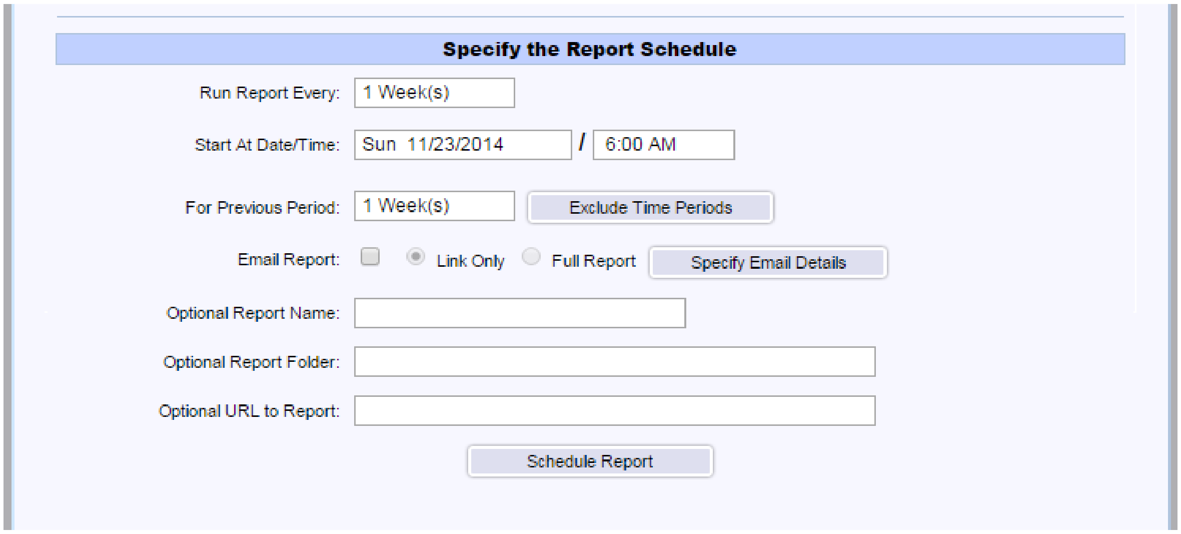

Schedule Reports
Schedule
Queued
Brand
Properties
Select the Report and Options
Choose Alert Types & Servers/Devices

Report Type: Alert Analysis

Report Description: Report on Monitored Alert Conditions

Report Name/Notes:

4. Select the **‘Choose Alert Types & Servers/Devices’** button
5. A **‘Specify Report Parameters’** page will appear, check the box for **‘AdvancedWatch & LOS Alerts’**
   a. By default, the report will include the information for all the Logon Simulations created. To only report on one simulation, click the **‘Select’** button and choose the simulations you want to report on.
6. Click **‘Ok’** to approve the report parameters
7. Select the time the report should be run, how often it will run, and the historical period it should analyze.



Specify the Report Schedule

Run Report Every: 1 Week(s)

Start At Date/Time: Sun 11/23/2014 / 6:00 AM

For Previous Period: 1 Week(s)

Email Report: □ ● Link Only ○ Full Report

Optional Report Name:

Optional Report Folder:

Optional URL to Report:

Run the GAAM Report On-demand:

1. Click the **'Report'** tab and then select the **'View'** submenu
2. Once the page is fully loaded, choose the **'Alert Analysis'** report type highlighted in blue
3. Click the **'Analyze'** button at the bottom of the page
4. A **'Specify Timeframe for Alert Notifications'** page will appear
5. Choose how many days/hours that you'd like to report on and then check the box for **'AdvancedWatch & LOS Alerts'**
   a. By default, the report will include the information for all the launches created. To only report on one simulation, click the **'Select'** button and choose the simulations you want to report on.
6. Click **'Ok'** to approve the report parameters and run the report
   a. Please note that the report generation process is tied to this page. If you navigate away from the page or click any other buttons on the page it will break the report process.
7. When the report is completed, select the report and then click the **'Status'** tab to view the results.

G. Launch Endpoint Manual Configuration

Instead of using the GAAMEndpoint.exe, one can also configure the prereqs manually.

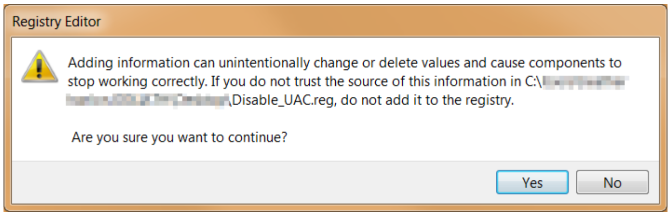
A. Windows Account that is always in a Logged on or Disconnected state:

- Since the Logon Simulator is creating real Citrix sessions, you will need a local or domain service account that is logged into the endpoint at all times, either logged in or disconnected. Please create this service account and **log in with it before continuing.**
- We suggest enabling Automatic logons for this account so that if the machine is rebooted the user will be logged in right away. Here is a link to a Windows Utility that will allow you to accomplish this https://technet.microsoft.com/en-us/sysinternals/autologon.aspx

B. UAC Disabled at the Kernel/System level:

- While the simulations are launching, the technology is making a number of system level call. In order to avoid unexpected prompt, UAC must be disabled at the system level (not through Control Panel). To accomplish this, Goliath includes a registry file to update the system. This file **requires a machine reboot**. Below are instructions:

- On the Goliath Server, open Windows File Explorer and navigate to **C:\Program Files (x86)\MonitorIT\Tools**
- Locate the **Disable_UAC.reg** file and copy it over to the Launch Endpoint(s)
- Double click to run the file
- A warning will appear for changing the registry, click **'Yes'** to continue

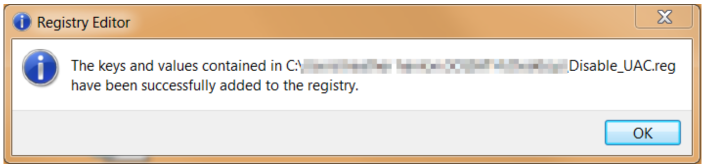


Registry Editor

Adding information can unintentionally change or delete values and cause components to stop working correctly. If you do not trust the source of this information in C:\[redacted]\Disable_UAC.reg, do not add it to the registry.

Are you sure you want to continue?

- A confirmation window will appear, click **'Ok'**



Registry Editor

The keys and values contained in C:\[redacted]\Disable_UAC.reg have been successfully added to the registry.

- Reboot the Launch Endpoint

C. Internet Explorer 11:

- The Logon Simulator is leveraging a series API calls during the simulation sequence. Therefore, Internet Explorer version 11 is required. Below are instruction on who to determine what version of Internet Explorer is currently installed.
  - Open Internet Explorer
  - Select the gear icon in the top right hand corner
  - Choose the menu option labeled 'About Internet Explorer'
  - A new window will open and display the versions details. If you are running version 11 then that is excellent. If not, you will need to update your browser to version 11.

D. Goliath Agent:

- The Goliath Agent is used to connect to the main Goliath server in order to run the simulations at their scheduled time, as well as report the data back to the console. If your simulation is the same as the goliath server there is no need to install the agent as it is deployed by default. Otherwise, please follow the instructions below for installing the agent.
  - On the Launch Endpoint, enter in the URL for the goliath console and append '\installagent.exe' to the end. For example, http://10.20.10.10:8080\installagent.exe
  - An agent installer will download, when ready run the installer.
  - When prompted enter the IP address or FQDN of the Goliath Server
  - The default agent port is 8282, if you are using a different port, please define your agent communication port in the 'server port' field.
  - Click next to install the agent
  - When the installation in complete click finish
  - After a minute, open the Goliath Console and navigate to the inventory page to

confirm that the agent is connecting in to the product.

E. LogonSimulator.exe is running:

- The LogonSimulator.exe is the application that works with the Goliath Agent in order to execute the simulation at their scheduled time. This application functions as a background process that must be running in order for the simulations to execute. Please follow the below instructions for obtaining and executing the application.
  - On the Launch Endpoint, open the Start Menu and run 'shell:startup'
  - On the Goliath Server, navigate to the Bin folder inside the install directory
    - The default location is C:\Program Files (x86)\MonitorIT\Bin
  - Copy the LogonSimulator.exe file and paste it into the Startup folder on the Launch Endpoint
  - Double click to run the file, this file runs in the background so you will not see anything happen. Use Task Manager to confirm there is only 1 instance running
    - *If there are security prompts when you run it the first time, please uncheck the box to check the executable in the future, to ensure successful starts of LogonSimualtor.exe following restarts of the Launch Endpoint.*

F. Trusted Sites:

- When the Logon Simulator executes, it assumes that the ICA file will be opened automatically. To ensure this process, Trusted Sites settings must be lowered and the Citrix address must be added to trusted sites. Please see the following instructions for modifying the settings.
  - Open Internet Explorer
  - Click the gear icon and select the menu option for 'Internet Options'
  - Navigate to the 'Security' tab, and select the 'Trusted Sites' zone
  - Click the 'Sites' button, add your Citrix portal address and click close when finished
  - Under 'Security level for this zone' move the slider down to the lowest possible setting
  - Lastly, click 'Apply' and then 'OK' to save these settings

G. WASP.dll:

- On the Goliath Server, open Windows File Explorer and navigate to **C:\Program Files (x86)\MonitorIT\Bin**
- Find the file **'WASP.dll'**
- Copy the file and past it into the agent install folder on the Launch Endpoint.
  - The default location on a Launch Endpoint is C:\Program Files\MonitorIT
  - If you are running the launches on the same machine as the base install please paste the into C:\Program Files (x86)\MonitorIT