
Version 1.0

Monitors over a firewall

All Versions

Installation Guide for OpenText™ Customers

opentext™

Document release date: June 2024

Legal Notices

© Copyright 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Disclaimer

Certain versions of software accessible here may contain branding from Hewlett-Packard Company (now HP Inc.) and Hewlett Packard Enterprise Company. This software was acquired on September 1, 2017 by Micro Focus and is now offered by Open Text, a separately owned and operated company. Any reference to the HP and Hewlett Packard Enterprise/HPE marks is historical in nature, and the HP and Hewlett Packard Enterprise/HPE marks are the property of their respective owners.

Contents

Contents	3
2 Document Purpose and Target Audience	4
3 How to use this guide	4
4 Terminology/Glossary	5
5 Prerequisites	6
5.1 Determining the location of your host(s)	6
5.2 MOFW hardware and software requirements	6
5.3 Downloading required components	7
6 Installation	9
6.1 Checking for pre-installed components	9
6.2 Base installation	9
6.3 Installation of the latest patches	12
7 Configuration	12
7.1 MOFW Agent Configuration	12
7.2 Monitors Configuration	16
7.3 LRE Configuration	18
8 Troubleshooting	22
9 Using SiteScope with MOFW (Optional)	23
9.1 SiteScope Configuration	23
9.2 MOFW Configuration for SiteScope	23
10 Appendix	26
10.1 Configuring the MOFW Agent as either Service or Process	26
10.2 Reinstalling the Standalone Monitor Over Firewall Software	27
10.3 Applying the Latest Patch Upgrades	28
10.4 Test if the firewall is open for MOFW to SaaS Communication	28

2 Document Purpose and Target Audience

Welcome to the OpenText “Monitors over a firewall - Installation Guide”.

The purpose of this guide is to assist OpenText customers in performing new Windows-based Monitor Over Firewall (MOFW) setups located in their own networks.

Note that this guide does not attempt to include all potential setup situations. Instead, it focuses on the process and typical aspects of the MOFW installation.

The target audience of this document is technical personnel of OpenText SaaS customers who are involved with operating performance tests within OpenText LRE and/or installing and maintaining matching MOFW agents in their own network that are connected to OpenText SaaS LRE environments. The audience typically includes load test specialists, QA lab managers, and QA managers.

3 How to use this guide

The recommended installation procedure consists of 3 phases to be followed in sequence. This guide provides a chapter for each phase.

“**5 Start Here**” lists typical steps of preparation that are required before the actual MOFW software can get installed. Performing these is crucial for a successful installation later.

“**6 Installation**” walks through the actual installation of the MOFW software.

“**7 Configuration**” guides though the parameters to be configured after installation.

4 Terminology/Glossary

Monitor Over Firewall (MOFW)

During an in-house performance test are the online monitors directly polling the monitored machines or applications, but that is not possible in a SaaS environment due to firewall(s) between the LRE instance and the application under test (AUT). To overcome that limitation, an MOFW Agent is installed inside the firewall to collect and forward the monitored data through the firewall to the LRE instance.

Agent Configuration

An application installed on the MOFW host that is used to configure the specific MOFW. It is typically accessible through “Start/All Programs/Micro Focus/Load Runner Agent Configuration”.

Agent Service (Agent)

A Windows service (called “LoadRunner Agent Service”) that runs on the MOFW host to connect it to OpenText SaaS LRE. In rare cases, the Agent is alternatively installed as a process instead that needs to be started by a logged in user.

Firewall

In the context of this document, we refer to the firewall(s) in the customer’s network that typically separate(s) the injector hosts from the internet.

MI Listener (MIL)

An MI Listener is a server located in the OpenText SaaS network that acts as a proxy to connect the customer’s injectors with LRE in the OpenText SaaS datacenters. Each MOFW must be configured in the Agent Configuration to point to that host (by entering the preferable the public DNS name, alternatively the public IP address, of the MIL into the “MI Listener” field).

System/Application Under Test (SUT/AUT)

The target system or application of the performance test against which the Vusers are running.

5 Prerequisites

Before a successful installation and configuration of the MOFW Agent can take place, it is necessary to follow certain brief steps of preparation as outlined below.

5.1 Determining the location of your host(s)

First, decide on the specific location of the MOFW Agent that you want to use, network topology, and available hardware.

Network requirements between the MOFW Agent and the System Under Test

- Any machines or applications to be monitored needs to be accessible from the MOFW Agent, either directly in the same network or through firewall(s) inside your company network, or between physical data center locations through company VPN (recommended only for special cases).
- The closer the MOFW Agent is to the monitored machines and applications, the better, since firewalls, distance and especially VPN access can add latency in the update of the graphs during load tests. Hence, we recommend selecting MOFW hosts in the same network as the AUT if possible.

Network requirements between the MOFW Agent and OpenText SaaS

- The MOFW host must have *outbound* access to the public OpenText SaaS MI Listener DNS name, or alternatively, IP address.
- No *inbound* ports should be opened in the company firewall from the MI Listener to the MOFW host.
- While we recommend direct traffic whenever the firewall can be opened, alternatively a proxy server may be used if available in your network. Often such proxies are already configured for allowing browser traffic to the internet and may be reused for tunneling outbound traffic from the MOFW to the MI Listener as well.
- Which method of access is required for your MOFW depends on the configuration of your network and firewall, to some extent determined by the security policies laid down by your IT organization.
- The specific public DNS name (IP address) of the MI Listener will be obtained later in the process by request from OpenText SaaS.

5.2 MOFW hardware and software requirements

We generally recommend dedicating the MOFW host to that purpose only whenever possible, though MOFW and SiteScope installation on the same host are ok.

Do not install any web server such as IIS or others on the same host.

It is not possible to install a Load Generator on the same host, as it directly interferes with the function of the MOFW Agent software.

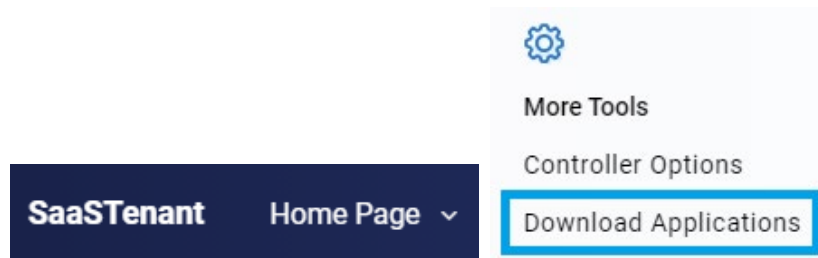
Please refer to the online help for the latest hardware and software system requirements located at the following URL: <https://admhelp.microfocus.com/lre/>

- *Get Started -> Support Matrix -> Support Matrix documentation.*

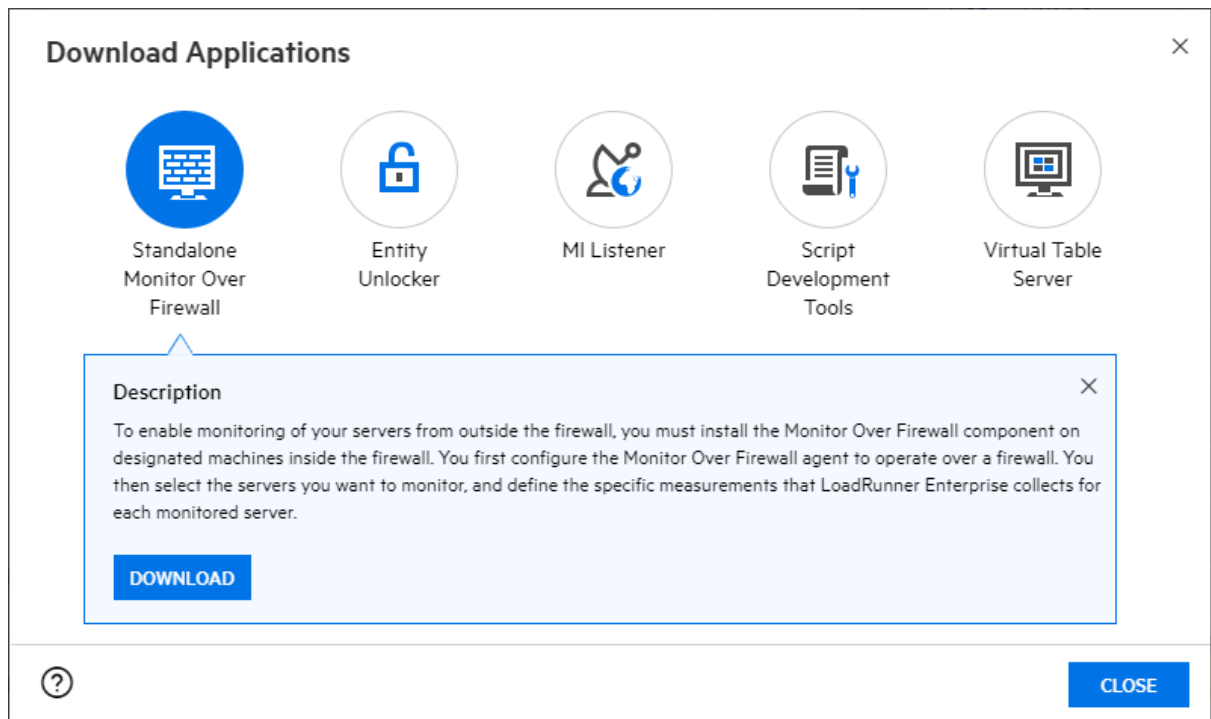
5.3 Downloading required components

The Standalone Monitor Over Firewall LRE installer is available in the download section of your LRE instance. Do not use installers obtained from other sources than your OpenText SaaS LRE instance or the OpenText SaaS team.

On the dashboard, top left, click the Dashboard icon and select “Download Applications”:



In the popup window, select “Standalone Monitor Over Firewall” and click “Download”:



LRE requires the matching LRE Standalone Monitor Over Firewall installation (no version difference), as present in the “Download Applications” dialog.

Install patches if and only if they can be found in that same “Standalone Monitor Over Firewall” section of your LRE instance you downloaded the main installer from.

6 Installation

The MOFW installation on the host is straight-forward, using the base installer obtained in the preparation phase earlier and running an automatic patch update as described later.

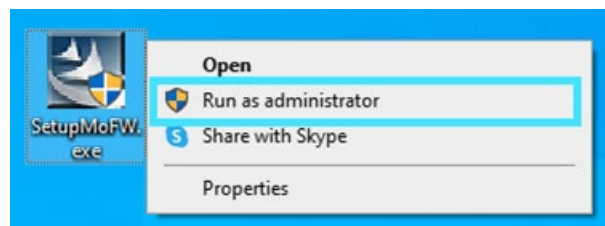
6.1 Checking for pre-installed components

Make sure that there are no previous versions of the MOFW software installed, and that no other LRE components such as VuGen, Analysis or Load Generator are installed. None of those components can exist on the machine where the Standalone Monitor Over Firewall is installed.

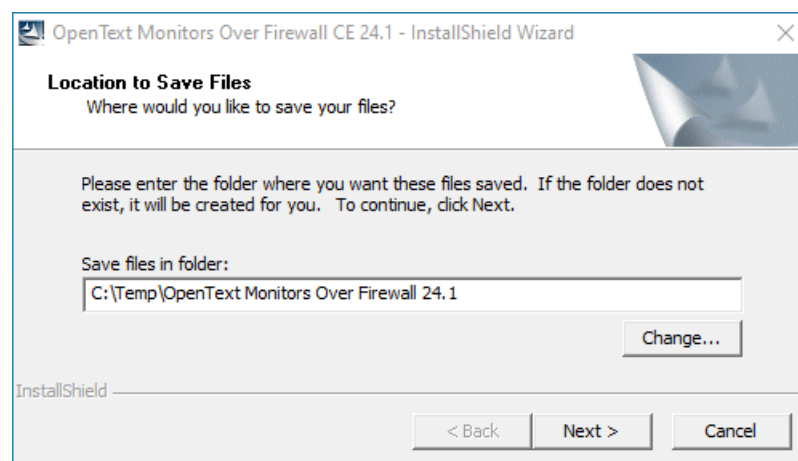
You can check for pre-installed components through the Windows Control Panel/Add or Remove Programs and uninstall them if present.

6.2 Base installation

After making sure that no previous load generator software is present, start the installation by starting your “SetupMoFW.exe” installer **using a local or domain administrator login, then Run as administrator**:

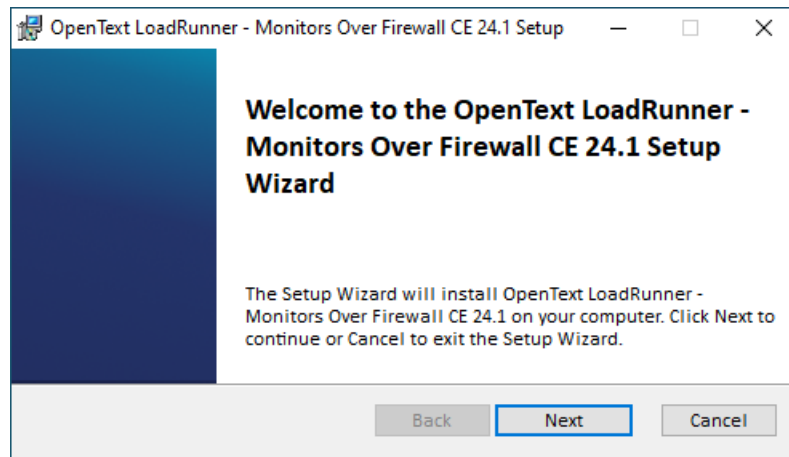


Accept the default location or select a temporary location for the installer to decompress the files:

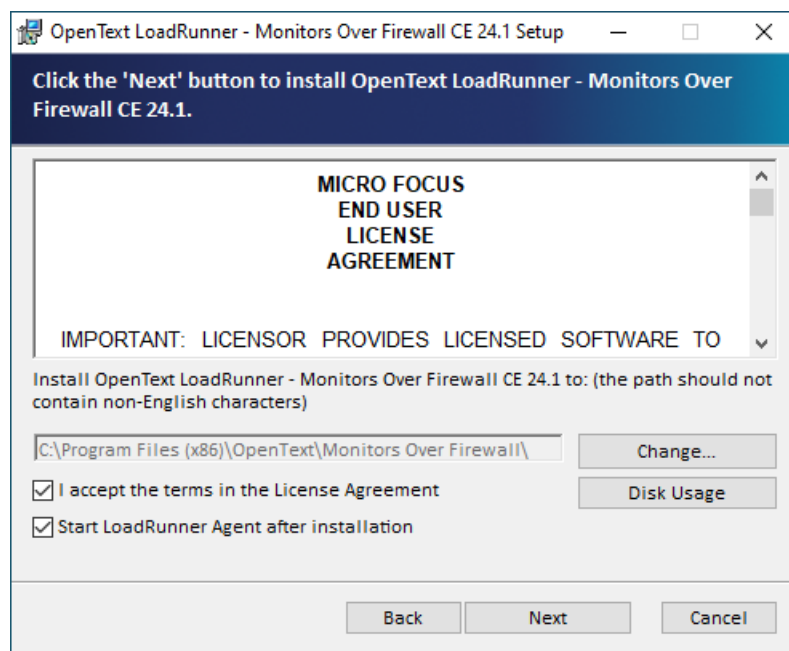


Accept any requests to install prerequisite programs that have been determined to be missing.

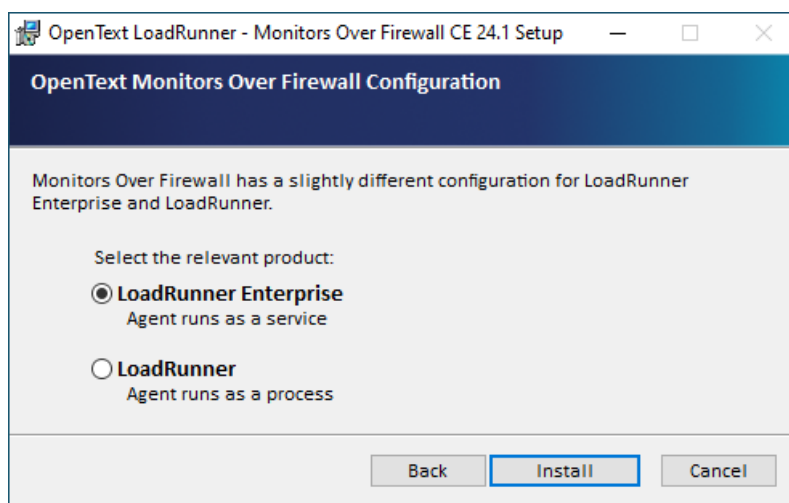
Once the prerequisite installation has completed, click “Next”.



Accept the License Agreement terms and to start the Agent after the installation.



Select the "LoadRunner Enterprise" product:

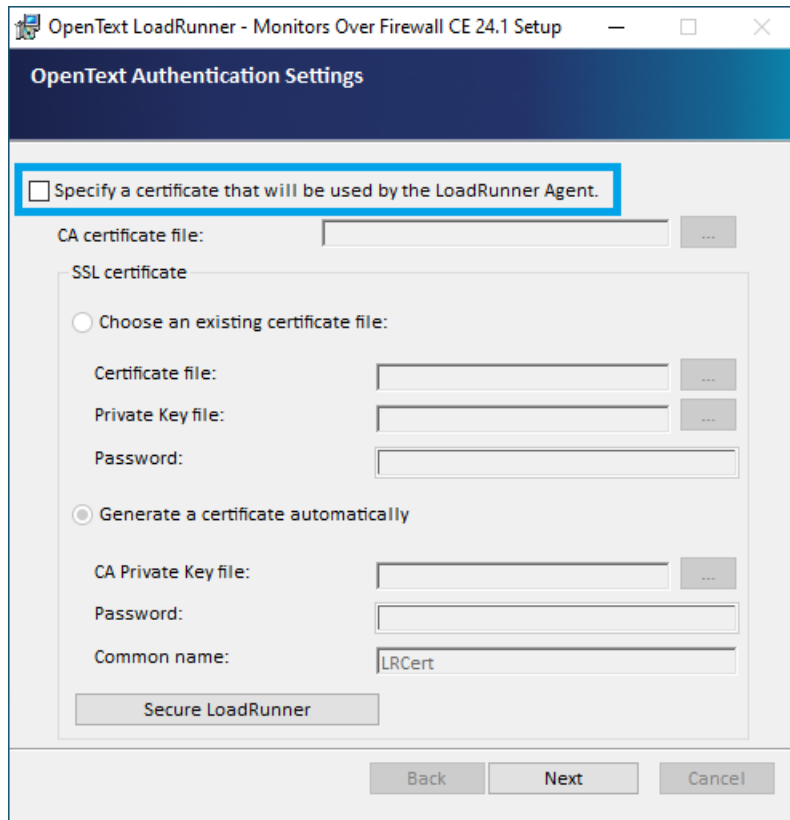


We recommend choosing “LoadRunner Enterprise” since this leads to installing the MOFW Agent as a service, providing permanent availability whenever the host is up and running.

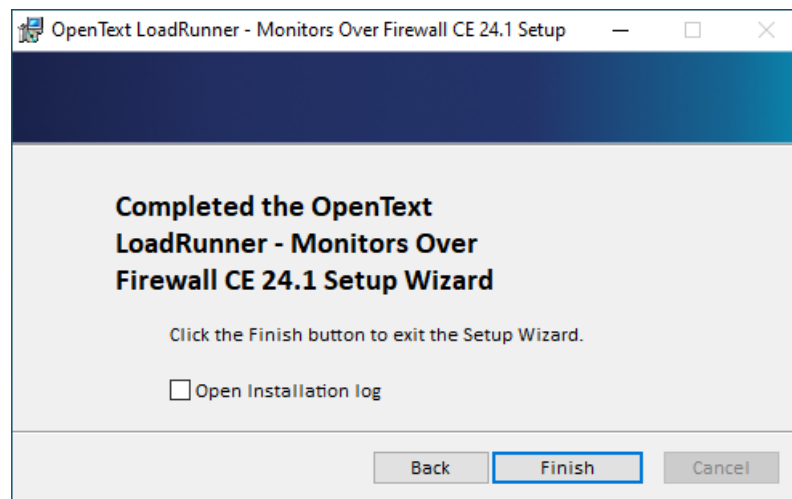
Continue with “Install” to finish the installation.

After the installation, make sure to **uncheck** “Specify a certificate that will be used by the LoadRunner Agent” unless you have exchanged certificates with OpenText, then follow the instructions from our operations team.

By unchecking this box, preinstalled default certificates are still used for SSL communication.



Click “Next” and the installation is complete. Click “Finish” to end the installation process and proceed to the next phase.



6.3 Installation of the latest patches

Patches are to be installed if and only if present in the Downloads section of your LRE instance.

7 Configuration

Once the MOFW has been successfully installed as per the previous chapters, the MOFW Agent must be configured to connect successfully to the MI Listener and then which server counters the MOFW Agent will collect and finally add the MOFW to our testing setup in LRE.

7.1 MOFW Agent Configuration

You will first need to configure the MOFW Agent on the MOFW host machine.

7.1.1 Prerequisite #1: Agent Configuration parameters

You will need the following information.

- The **MI Listener Name**.
 - This is the public DNS name of the specific MI Listener in the OpenText SaaS network that the MOFW will communicate with.
 - An example: `almrwc1645p-mil1.saas.microfocus.com`
- The **Local Machine Key**.
 - The Local Machine Key is composed of

`<mofwname>`

 - Please note that the Local Machine Key for an MOFW has no location part like a Load Generator, so there are no underscores ‘_’ used in the name.

Policy for selecting a valid MOFW Local Machine Key

A valid MOFW Local Machine Key must meet the following criteria:

- Only alphabetical and numeric characters as well as dashes ‘-’ are allowed.
- The name must start with a letter.
- We encourage the use of numbers if prefixed with names.
- MOFW names must be unique (across the LRE instance). Hence, the name must be descriptive, contain organization-specific information and should not be generic.
- We recommend starting the name with an abbreviation of the company name, but also to include the term “mofw” to avoid confusion with the load generator names.

Here some typical examples of valid MOFW names for customer “Sample Industries, Inc.”:

`“sii-mofw01”, “siwestmofw01”, “siinyork-mofw”`

7.1.2 Prerequisite #2: Outbound Network Access from the MOFW to the MI Listener

As mentioned in the prerequisites chapter under “Network requirements between the MOFW Agent and OpenText SaaS”, to function properly, the MOFW host must have network access to reach the MI Listener from your network. Network access can be provided through one of two means:

Case A: Direct communication on port 443

The firewall between the MOFW and the internet must be open for **outbound communication on port 443 against the MI Listener DNS name** (or, less preferable, IP address).

If the firewall is not open, you need to open a firewall request to your security team.

Note that the firewall rule should not be bidirectional, since there are no incoming connections from the MI Listener. Only outbound connections on port 443 should be allowed.

At this point, make sure to test if the firewall is open from your MOFW using the simple telnet test described in the Appendix.

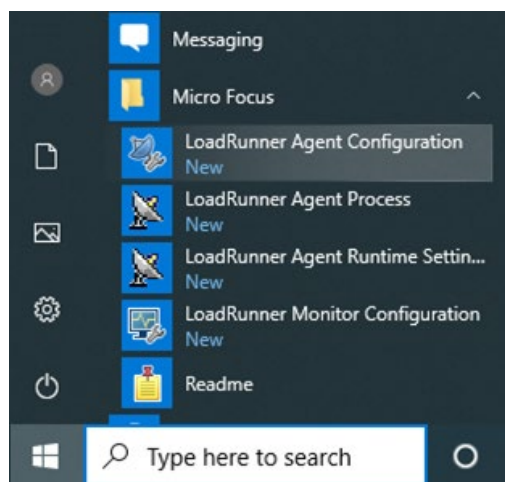
Case B (alternate): Proxy Communication

If a proxy is required to reach the internet, please contact your IT or security team to provide the proxy configuration details, such as the proxy DNS name/IP address and its port. Proxy credentials and/or protocol information may be required as well.

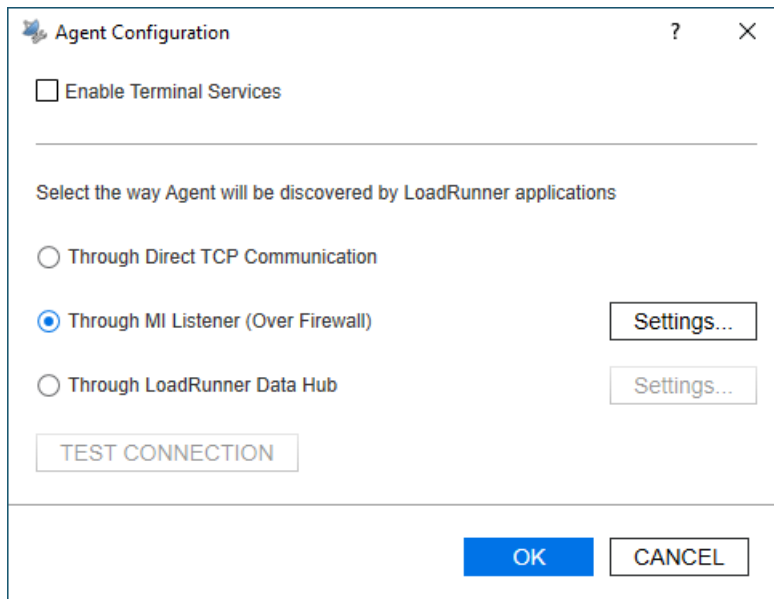
Alternatively, you may also log on to the MOFW host, open a browser and check its settings if a proxy is active and which parameters are used. If a proxy is present in the browser and browsing to the internet works, in most cases you should be able to use the same proxy settings for the MOFW configuration as well, but always check with your network team.

7.1.3 Agent Configuration

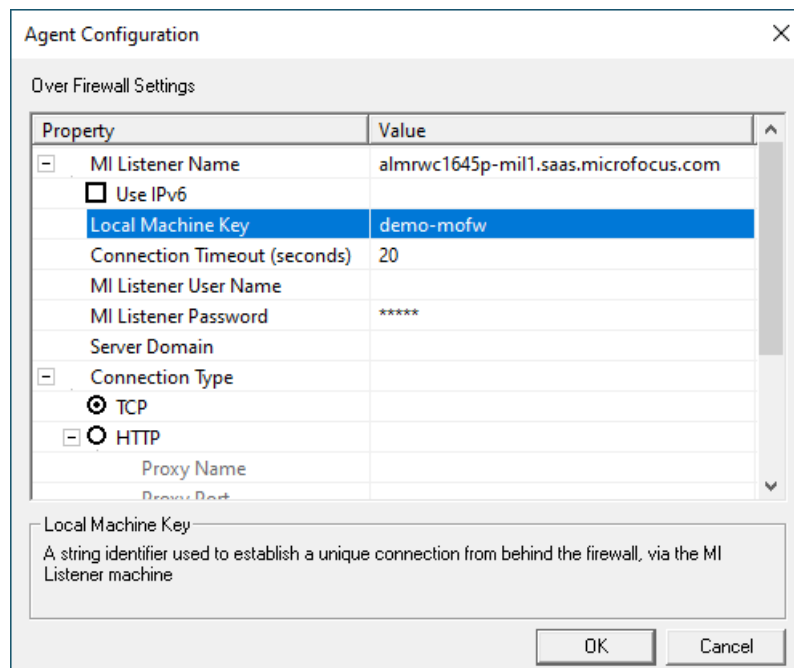
To configure the agent, go to: *Start / Micro Focus / LoadRunner Agent Configuration*



Select the “Through MI Listener (Over Firewall)” checkbox and click “Settings”:



Enter the MI Listener Name, as provided to you by OpenText SaaS, and the Local Machine Key.



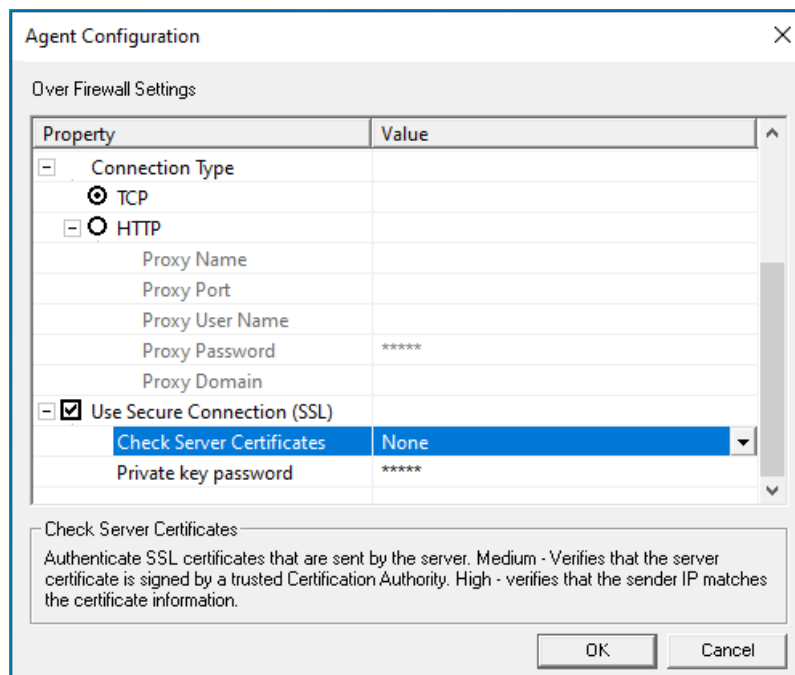
In this **example**, the public DNS name of the MI Listener Name is:

`almrwc1645p-mil1.saas.microfocus.com`

The Local Machine Key is the name only, without any location string. Example:

`demo-mofw`

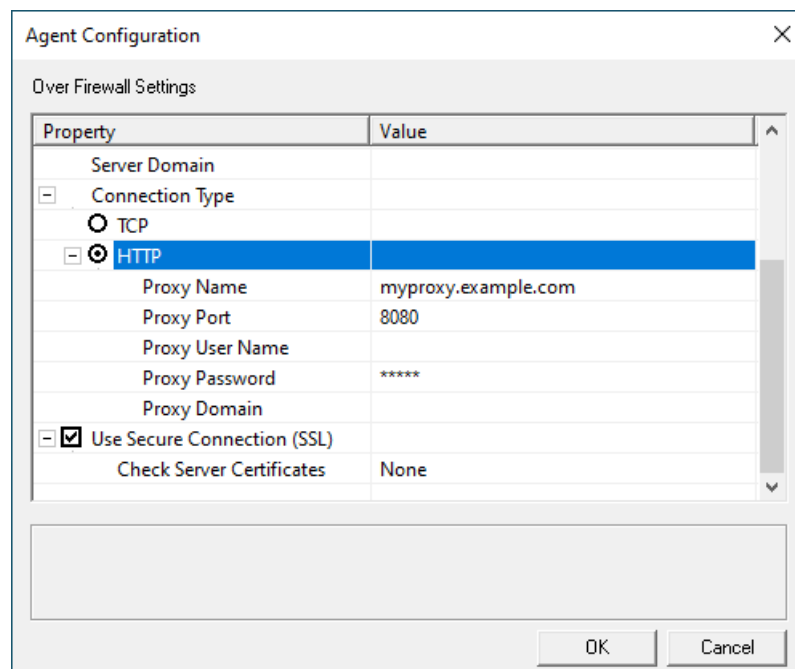
Finally check the **Use Secure Connection (SSL)** box to enable SSL communication between the MOFW and the MI Listener and set **Check Server Certificates** to **None**. The latter is due to the certificate is offloaded on the load balancer and not on the MIL. It is also possible to not use SSL, so if you run into issues, please try without SSL as well.



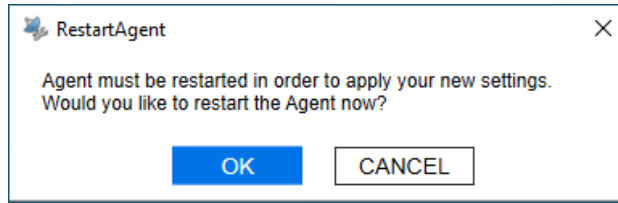
For proxy configurations only (case B above):

Enter the proxy parameters as provided by your IT or security team. This typically includes at least Proxy Name and Proxy Port, sometimes also credential information.

Check also the “Use Secure Connection (SSL)” box and set the “Check Server Certificates” to “None”.



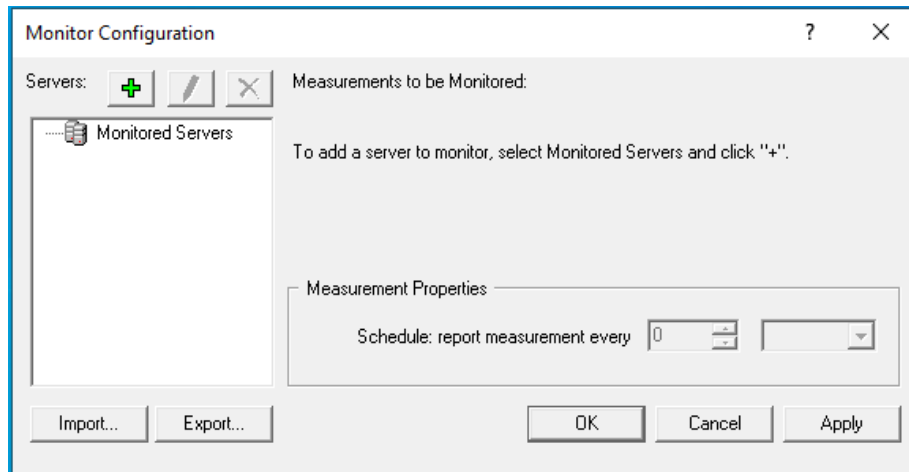
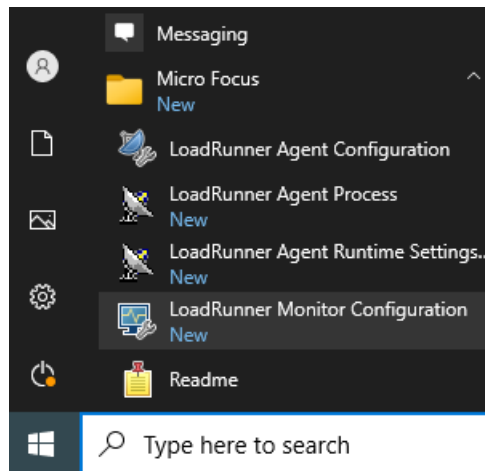
Click “OK” twice and you will be asked to restart the agent:



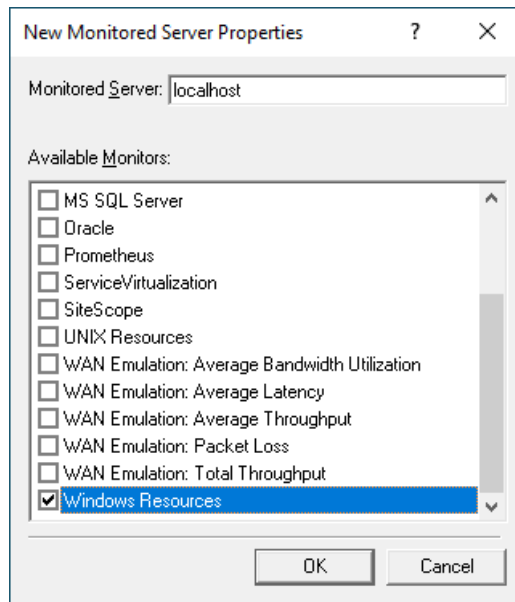
The Agent Configuration is now complete. Next, we need to configure the monitors.

7.2 Monitors Configuration

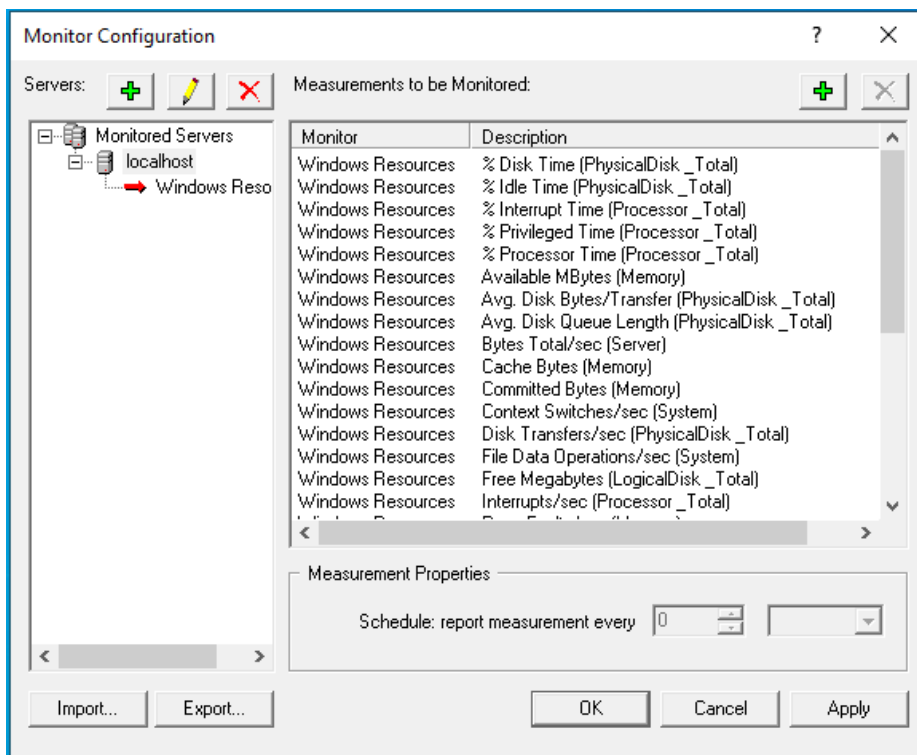
Open the LoadRunner Monitor Configuration from the start menu:



In the Monitor Configuration window, click on the upper left green '+' button to add the servers that will be monitored. Specify the server properties such as the server IP or hostname and the type of counters that will be captured.

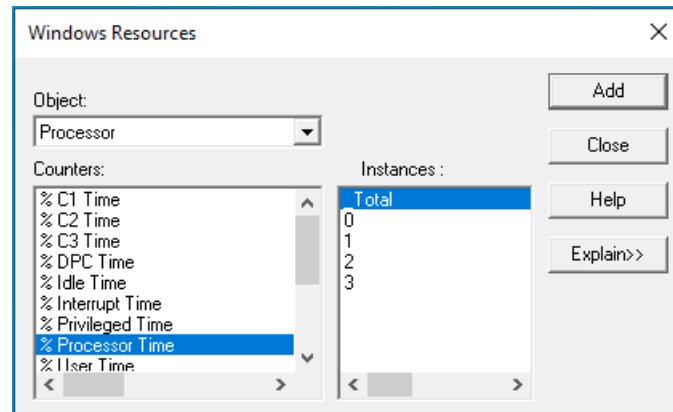


The Monitor Agent has a predefined list of server types and counters that could be captured by the product. It can also connect to OpenText SiteScope which is a more advanced monitoring tool. Once the server and a monitor type have been defined click OK and a default set of counters will be populated.

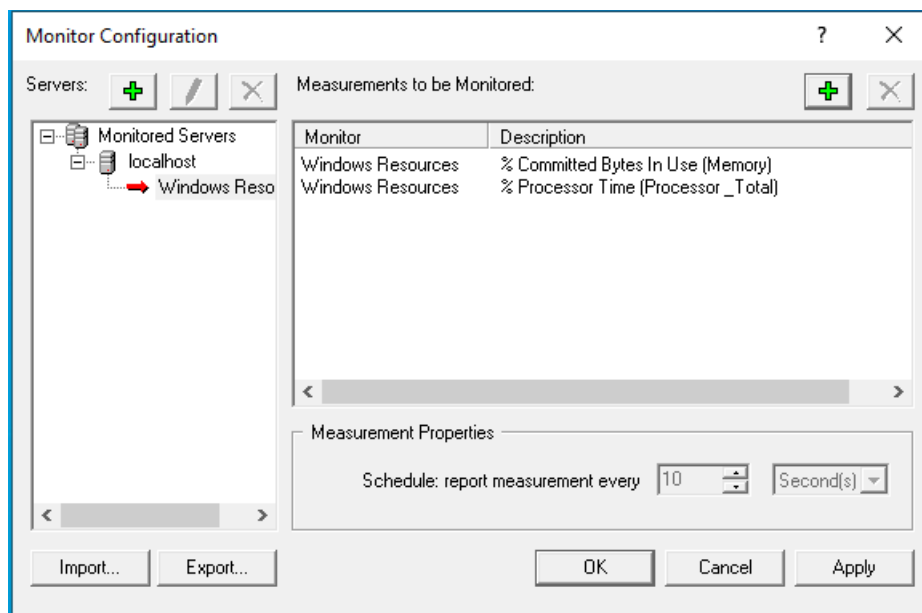


It is important to realize that the default set of counters might include counters that aren't available on the specific operating system that is being monitored, since different OS have slightly different counters. Due to that, best practice is to remove all the default counters and only add those of interest and that are confirmed to exist. To do that, highlight all the counters and click the delete button marked with a red 'x'.

To add the counters of interest, select the green + button on the right and select the name of the monitor type.



Select the object of interest and which counter to monitor, click the Add button for each and once done, click the Close button. This will bring you back to the Monitor Configuration window, and you will see your selected measurements once you've highlighted the monitor.

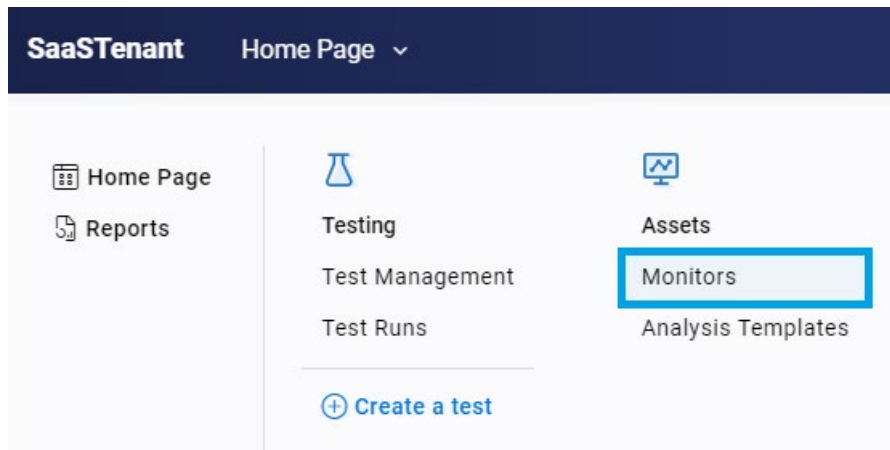


Click the OK button and the window will close, and the setup on the MOFW host is done.

7.3 LRE Configuration

To enable the MOFW Agent to report monitor measurements to a running performance test, we need to add the MOFW to our testing setup.

Log onto the LRE application and got to Assets -> Monitors:



Click the “New Monitor Profile” button.

Select Monitor Profile Type: “Monitor Profile Over Firewall”.

Enter a name (which isn’t related to the Local Machine Key).

Select the MI Listener, which is displayed using the short name.

Enter the Local Machine Key that was used in the Agent Configuration.

The image shows a dialog box titled "New Monitor Profile" with a close button (X) in the top right corner. The dialog has a dark header with "SaaS Tenant" and "Monitors & Analysis templates" with a dropdown arrow. The main content area is white and contains the following elements: "Select Monitor Profile Type:" followed by two radio button options. The first option is "Monitor Profile" with a monitor icon and a radio button. The second option is "Monitor Profile Over Firewall" with a monitor icon and a radio button that is selected. Below the options are four input fields: "Name *" with the value "My MOFW", "MI Listener *" with the value "LREFRA002P-M02" and a dropdown arrow, "Machine Key *" with the value "demo-mofw", and "Description" with an empty text area. At the bottom right, there are two buttons: "OK" (blue) and "CANCEL" (white with a grey border).

Click OK. Now that we have the MOFW registered in the system, we can add it to the tests that should utilize it.

Select a test in the Test Management module and open it by clicking the Edit Test button. Select the Assets tab.

SaaS Tenant Testing ▾ 1 ? ▾ | DEFAULT | LRE_Demo ▾ | 8 ▾

Test Management > Test Id 175 | **Demo Test** Last Modified Apr 23, 2024, 1:29:39 PM

Groups and Workload **Assets (0)** SLA Disruption Events SAVE TEST RUN TEST

Analysis Template Default Analysis M... 0 →

Monitors (0)

Assign Monitors Remove ↻ Help

ID	Type	Name	Description
----	------	------	-------------

Click the Assign Monitors button and navigate to the MOFW in the tree and add it.

Add Monitors ×

Select monitor or monitors folder

🗑️ ↻ 🔍

Resources

My MOFW Demo

SELECT SELECT & CLOSE CLOSE

SaaS Tenant Testing ▾ 1 ? ▾ | DEFAULT | LRE_Demo ▾ | 8 ▾

Test Management > Test Id 175 | **Demo Test** Last Modified Apr 23, 2024, 1:29:39 PM

Groups and Workload **Assets (1)** SLA Disruption Events SAVE TEST SAVE AND RUN

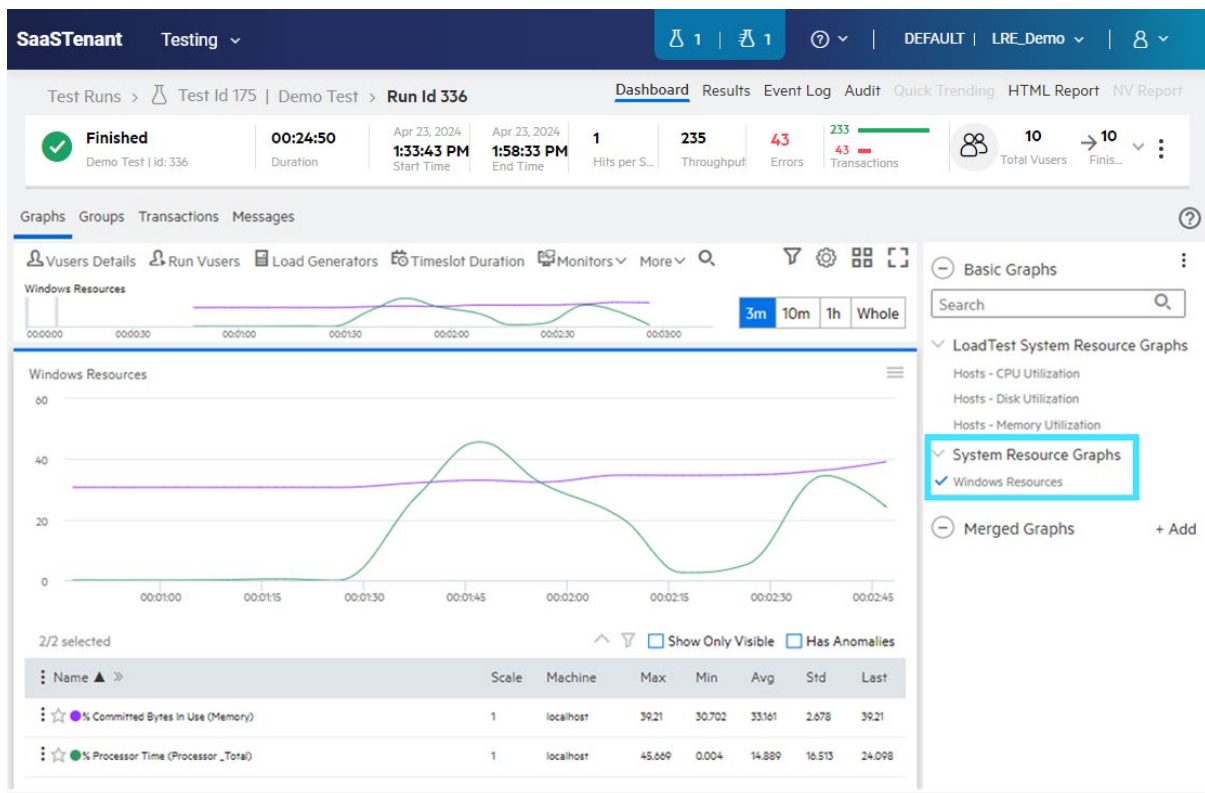
Analysis Template Default Analysis M... 0 →

Monitors (1)

Assign Monitors Remove ↻ Help

ID	Type	Name	Description
1114	Monitors Over Firewall	My MOFW	

Once the test is running, although no Vusers need to be in a running state, the selected monitor measurements will start reporting after some time, but keep in mind that this might take up to a few minutes.



8 Troubleshooting

In case the MOFW Agent is not working or running as expected, basic technical troubleshooting on your end will be required. Should the recommended steps in the "*Load generators over a firewall - Troubleshooting Guide*" not suffice to resolve any technical issues, please open a support case and our team will reach out to you to help you resolve the matter.

Please add at least the following information to the case to ensure fastest possible resolution:

- A short description of the issue, including any observations you find helpful that you may have made while troubleshooting the issue yourself.
- If applicable, which steps from the guides have already been attempted?

Note that during the troubleshooting process, the OpenText SaaS engineer may find it necessary to conduct a live remote diagnosis session on the MOFW host.

9 Using SiteScope with MOFW (Optional)

While the MOFW agent can connect to multiple servers and upload metrics to LRE, a more scalable solution is to use the MOFW agent together with SiteScope.

To use SiteScope with LRE you will still need the MOFW agent, so begin by configuring the MOFW agent as described above and then configure the MOFW agent to work with SiteScope.

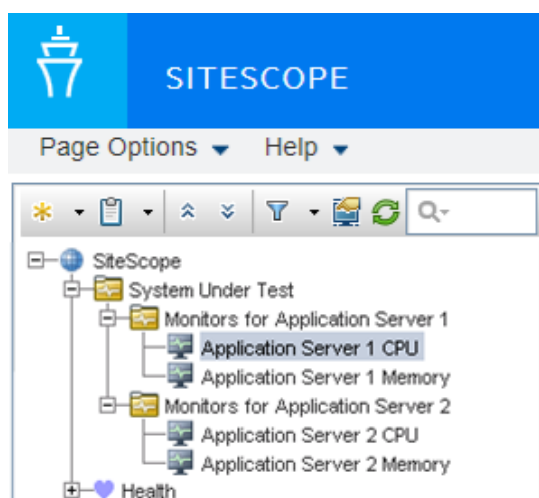
You can install SiteScope on the same host as the MOFW installation.

Please make sure that your SiteScope installation is compatible with your version of LRE.

- Install SiteScope according to installation instructions.

9.1 SiteScope Configuration

After opening the URL <http://localhost:8080/SiteScope/> you should be presented with the SiteScope GUI, where you will first need to create a SiteScope group with a working SiteScope monitor attached. Please refer to the SiteScope specific documentation on how to do this in detail. In this example we've added two groups with two monitors in each group.



Do make sure that the Monitor has a green status indicating that data is being collected.

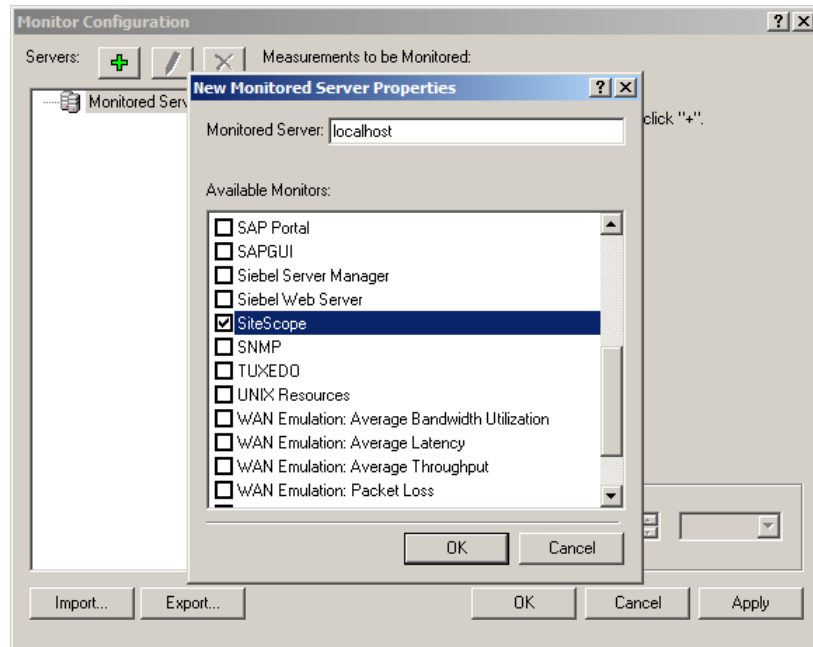
Name	Status	Type	Target	Summary
Selected node				
localhost CPU		CPU	SiteScope Server	0% avg, cpu1 0%,
Counters (3 out of 3)				
utilization				0%
utilization cpu # 1				0%
utilization cpu # 2				0%

9.2 MOFW Configuration for SiteScope

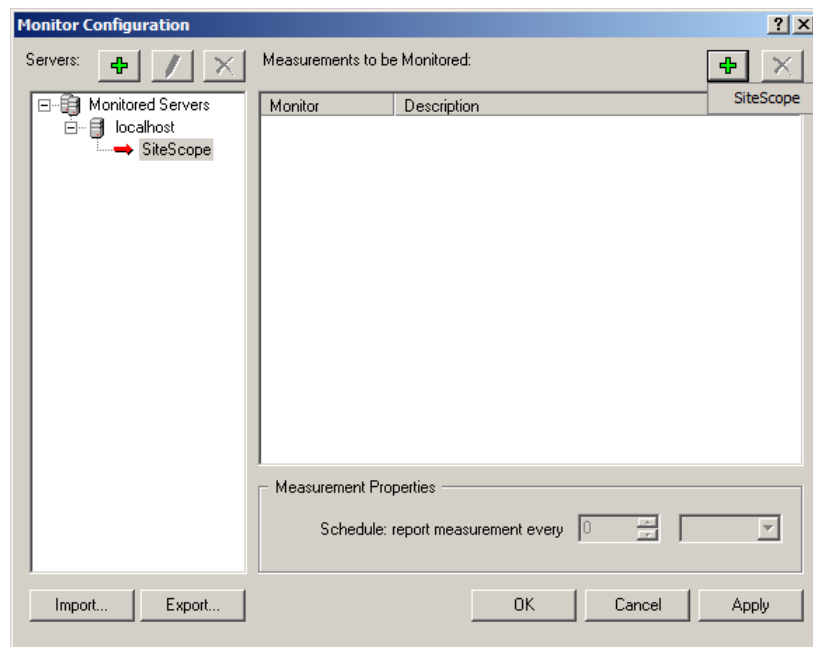
Now we need to use the “Monitor Configuration” tool of the MOFW to tell LRE about the SiteScope setup we have created. This is done similarly to the steps in the “Monitor Configuration” chapter

earlier in this document. Any differences are noted below.

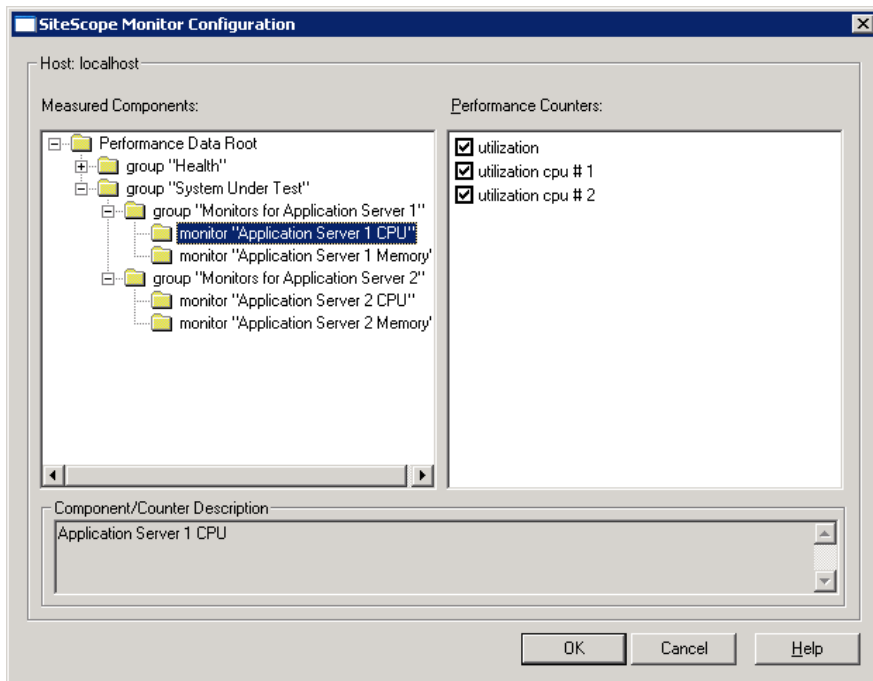
First we start the Monitor Configuration as before. Next, we bind SiteScope to the MOFW by registering a server “localhost” (or the network/host name of the host wherever the SiteScope application resides), and by adding a “SiteScope” monitor:



Now we add the monitors from SiteScope to MOFW. We first click on “+” to add monitors:



Next, we add all monitors (or a subset we chose) that we registered in SiteScope, by opening the tree for each desired monitor in each group and selecting each desired metric (performance counter) through checkboxes:



Now we click "OK" twice to close the Monitor Configuration tool. Assuming that all other steps earlier in this document were taken to register the MOFW inside of LRE and inside a load test, the monitoring setup is now complete.

10 Appendix

10.1 Configuring the MOFW Agent as either Service or Process

The MOFW agent can be run either as a service or as a process.

The MOFW agent can be run either as a service or as a process. OpenText SaaS recommends running the agent as a service, since the Agent then becomes available after the host is started.

NOTE: It is crucial that the Agent only runs through one of these two means, not both, at the same time. Otherwise, operational errors will occur.

As a service, the 'LoadRunner Agent Service' service runs automatically even if the user does not log in to the system. The user can login to the machine and go to Administrative Tools -> Services -> 'LoadRunner Agent Service' to verify or change which user account is running the service, since this might affect the user's rights to pass through proxies. The service should run under administrative privileges, or user "IUSR_METRO".

While installing, make sure to have administrative privileges (domain or local).

As a process, the Agent runs through 'magentproc.exe' from the <MOFW>\launch_service\bin folder. This requires a user to login to the machine to start this Agent and stay logged in during the use of the MOFW. The Agent will run with the same user rights as the logged in user.

After installing the MOFW Agent, the user can switch the Agent to run as either service or process by performing the following steps.

To run the MOFW Agent as a service (recommended by OpenText SaaS for permanent setups):

1. Remove the "LoadRunner Agent Process" shortcut from the Start -> Program Files -> Startup group if present, to avoid the process from starting when the computer is rebooted.
2. Launch the command prompt using **Run as Administrator** and go to <MOFW>\launch_service\bin. (If started erroneously as a non-administrative user, the installed service will not work properly later).
3. Type in: `magentservice.exe -install<enter>`
 - Note: If you want to set a different account:
Type in:
`magentservice.exe -install <user_domain>\<user_name> <password>`
4. Go to the Window's Services view and change its properties to start it as "Automatic".
5. If you wish to modify the login details after installation of Agent Service, do the following:
 - Go to Start -> Control Panel -> Administrative Tools -> Services and look for the LoadRunner Agent Service.
 - Right-click and select Properties->Log On and change the information from there.

To run the MOFW Agent as a process (if needed):

1. Launch the command prompt using **Run as Administrator** and go to <MOFW>\launch_service\bin

2. Uninstall LoadRunner Agent Service by typing in:
`magentservice.exe -remove<enter>`
3. Verify that the service 'LoadRunner Agent Service' is no longer running.
4. Start the MOFW Agent process by running `magentproc.exe` from
`<MOFW>\launch_service\bin`
5. If desired to start the process automatically after login, add a shortcut to the `magentproc.exe` into the Start -> Program Files -> Startup group.

To run the MOFW Agent service under a different account:

If an installed MOFW Agent service runs under incorrect credentials that do not have proper administrative permissions, you can correct this by uninstalling and reinstalling the service:

1. Launch the command prompt using **Run as Administrator** and go to
`<MOFW>\launch_service\bin`
2. Uninstall LoadRunner Agent Service by typing in:
`magentservice.exe -remove<enter>`
3. Type in `"magentservice.exe -install <user_domain>\<user_name> <password>"`
4. Go to the Window's Services view and change its properties to start it as "Automatic".

10.2 Reinstalling the Standalone Monitor Over Firewall Software

In some cases, it may be required to reinstall the Standalone Monitor Over Firewall software completely, e.g. if the installation got corrupted. Please see steps for reinstallation below.

Note: With some older versions of the MOFW software, it has been possible to install multiple standalone components on the same host. That is no longer supported, meaning that **ONLY** the MOFW software can be installed on the host.

Uninstalling and reinstalling the MOFW:

- Make a note of the Agent Configuration parameters.
- Obtain the Standalone Monitor Over Firewall software by downloading it from the LRE application ("Standalone Monitor Over Firewall"), using the "Download applications" button.
- Make sure your Windows account on the MOFW has administrative privileges.
- Now uninstall the existing Standalone Monitor Over Firewall software.
- Reinstall the latest Standalone Monitor Over Firewall software using *administrative* privileges (e.g. by right-clicking on the installer and selecting "run as administrator"), and during the setup choose the "LoadRunner Enterprise" and "as a service" (in contrast to as a process) options.
- In the Agent Configuration application, enter the configuration parameters as previously, and restart the agent as requested. This typically includes at least the MI Listener Name and the Local Machine Key.
- Verify through the Windows "services" view that the service is now present in Windows.
- Allow the host to restart.
- Make sure that the service is running.

10.3 Applying the Latest Patch Upgrades

- Any patches for your Standalone Monitor Over Firewall installations that are required to match your LRE instance will be available to download from your LRE instance, certified for use by OpenText SaaS.
- Patches are required if and only if shown in your download section.

10.4 Test if the firewall is open for MOFW to SaaS Communication

MOFWs can connect to the MI Listener in OpenText SaaS LRE in one of two ways: Either directly through your company's firewall through outbound port 443 (recommended), or through a proxy in your network.

In many cases, outbound communication on port 443 is already permitted, for example for browsing the internet from the host, though in cases of higher security, even outbound communication may be blocked by default.

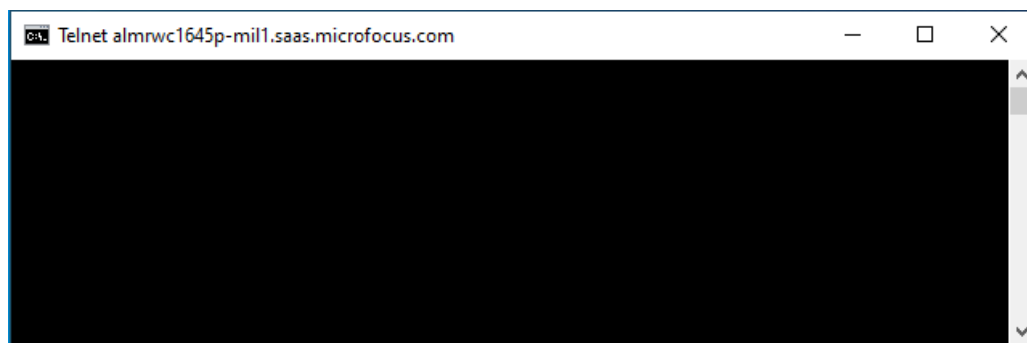
Log in to the selected MOFW, e.g. through Remote Desktop Client (RDP).

Open a Windows command shell (e.g. by Start/Run, typing "cmd").

Enter `telnet <MI Listener DNS name> 443` and check the response.

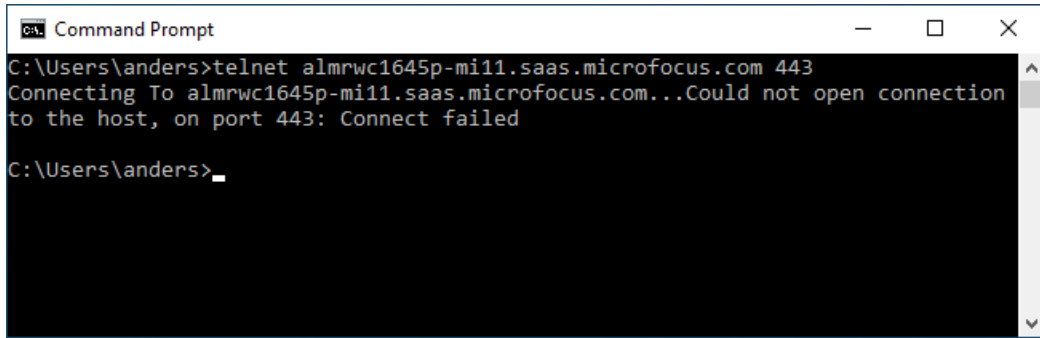
Example: `telnet almrwc1645p-mil1.saas.microfocus.com 443`

Case 1: If the response looks like this (blinking cursor on empty window):



Then the firewall is open from the MOFW host to the MI Listener on port 443, as it needs to be for direct communication. You can click the "X" close icon to close the window and log off.

Case 2: If the response looks like this ("could not open connection ..."):

A screenshot of a Windows Command Prompt window. The title bar reads "Command Prompt". The command prompt shows the following text:

```
C:\Users\anders>telnet almrwc1645p-mi11.saas.microfocus.com 443
Connecting To almrwc1645p-mi11.saas.microfocus.com...Could not open connection
to the host, on port 443: Connect failed

C:\Users\anders>_
```

Then the firewall is not open and needs to be opened by your IT Security team unless you use a proxy configuration instead. Please contact your IT Security Team to open the firewall from the list of IP addresses of MOFW hosts you use to the MI Listener DNS name/IP address outbound on port 443. Note that the firewall rule should not be bidirectional, since there is no incoming communication from the MI Listener. Only outbound connections on port 443 need to be allowed.

Case 3 – If the telnet test cannot be performed:

We recommend asking your IT Security team to check if the firewall is open outgoing from the MOFW IP address(es) to the MI Listener DNS name (or if given alternatively, the MI Listener IP address) on port 443.