

Monitors over a firewall

LRE 2021 R1

Installation Guide for Micro Focus SaaS Customers



Legal Notices

Disclaimer

Certain versions of software and/or documents (“Material”) accessible here may contain branding from Hewlett-Packard Company (now HP Inc.) and Hewlett Packard Enterprise Company. As of September 1, 2017, the Material is now offered by Micro Focus, 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.

Warranty

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

Restricted Rights Legend

Confidential computer software. Except as specifically indicated, valid license from Seattle required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 1993 - 2021 Micro Focus or one of its affiliates.

Contents

Contents	3
2 Document Purpose and Target Audience	4
3 How to use this guide	4
4 Terminology/Glossary	5
5 Start Here	6
5.1 Prerequisites	6
6 Installation	10
6.1 Checking for pre-installed components	10
6.2 Base installation	10
6.3 Installation of the latest patches	15
7 Configuration	16
7.1 MOFW Agent Configuration	16
7.2 Monitors Configuration	22
7.3 LRE Configuration	24
8 Troubleshooting	28
9 Using SiteScope with MOFW (Optional)	29
9.1 SiteScope Configuration	29
9.2 MOFW Configuration for SiteScope	30
10 Appendix	32
10.1 Configuring the MOFW Agent as either Service or Process	32
10.2 Reinstalling the Standalone Monitor Over Firewall Software	33
10.3 Applying the Latest Patch Upgrades	34
10.4 Test if the firewall is open for MOFW to SaaS Communication	34

2 Document Purpose and Target Audience

The "Monitors over a firewall - LRE 2021 R1 Installation Guide" assists customers in performing new Windows-based Monitor Over Firewall setups located in their 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 Micro Focus SaaS customers who are involved with operating performance tests within LRE 2021 or higher and/or installing and maintaining matching MOFW agents in their own network that are connected to Micro Focus 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 install later.

"6 Installation" walks through the actual installation of the MOFW software.

"7 Configuration" guides through the parameters to be configured after installation.

4 Terminology/Glossary

LoadRunner Enterprise (LRE)

The new name for Performance Center (PC).

Monitor Over Firewall

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

MOFW

Acronym for Monitor Over Firewall.

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/Advanced Settings/Agent Configuration”.

Agent Service (Agent)

A Windows service (called “LoadRunner Agent Service”) that runs on the MOFW host to connect it to Micro Focus 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 Micro Focus SaaS network that acts as a proxy to connect the customer’s injectors with LRE in the Micro Focus SaaS datacenters. Each MOFW has to be configured in the Agent Configuration once 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 Start Here

5.1 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.

5.1.1 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 Micro Focus SaaS

- The MOFW host needs to have *outbound* access to the public Micro Focus SaaS MI Listener DNS name, or alternatively, IP address.
- This access is typically for outgoing HTTP-based traffic on port 443 through the company firewall from the MOFW host to the public Micro Focus SaaS MI Listener DNS name, see later in chapter 5.
- No *inbound* ports must be opened in the company firewall from the MI Listener to the MOFW host.
- While we recommend using port 443 directly 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 injectors depends on the configuration of your network and firewall, to some extent determined by the security policies laid down by your IT organization.
- Hence, *we recommend that you contact your IT department or security team to determine if outbound traffic from the injector's network/injector hosts is allowed or can be allowed through the company's firewall on outbound port 443 towards a public DNS name (alternatively IP address) in Micro Focus SaaS's network, or if proxy access has to be used instead and is available.* Note that outbound traffic on port 443 towards specific DNS names/IP addresses is typically permissible in most cases, though sometimes the firewall must be opened first.

- The specific public DNS name (IP address) of the MI Listener will be obtained later in the process by request from Micro Focus SaaS, as described in chapter 2.

5.1.2 Host Hardware Requirements

This table provides hardware requirements for the MOFW.

Hardware component	Supported / Recommended
Processor	<ul style="list-style-type: none"> • 2 core CPU • 8 core CPU (Recommended)
Processor for UI level protocols*	<ul style="list-style-type: none"> • 8 core CPU • 16 core CPU (Recommended)
Memory (RAM)	<ul style="list-style-type: none"> • 8 GB • 16 GB (Recommended)
Memory (RAM) for UI level protocols*	<ul style="list-style-type: none"> • 16 GB • 32 GB (Recommended)
Available hard disk space	<ul style="list-style-type: none"> • 50 GB • 100 GB; SSD drive (Recommended)
Network card	1 GBit/s

5.1.3 Host OS and Software Requirements

Software component	Supported / Recommended
Operating system (See Windows Updates below)	<ul style="list-style-type: none"> • Microsoft Windows 8.1 64-bit* • Microsoft Windows 10 64-bit versions 1803, 1809, 1909, 2004, Enterprise LTSC 2019, 20H2 - (Recommended) • Microsoft Windows Server 2012 R2 64-bit* • Microsoft Windows Server 2016 64-bit** • Microsoft Windows Server 2019 64-bit** (Recommended)
Browser (used for recording and replaying protocols only)	<ul style="list-style-type: none"> • Microsoft Internet Explorer 11 (Recommended) • Microsoft Edge
Screen resolution***	<ul style="list-style-type: none"> • 1366x768 or higher • 1600x900 or higher (Recommended)

* Can only be used with Microsoft Internet Explorer 11.

** We recommend enabling Desktop Experience when using this operating system.

*** Controller is not supported on display monitors with 4K or higher resolution.

Please note that 32-bit Operating Systems are no longer supported.

Windows version	Required updates
<ul style="list-style-type: none"> • Windows 8.1 64-bit* • Windows 2012 R2 64-bit* 	Install the following pack of updates: <ol style="list-style-type: none"> 1. KB2919442 x64 or KB2970551 x64 (one of these two updates) 2. KB2919355 x64 3. KB2932046 x64 4. KB2959977 x64 (if applicable) 5. KB2937592 x64 6. KB2938439 x64 7. KB2934018 x64 8. KB2999226 x64

* The list of required updates might change due to Microsoft's update delivery policy or new Windows update releases. If you experience any issues, please contact Micro Focus Software Support.

5.1.4 *Software recommendations and 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).**
- In particular, do not install any web server such as IIS or other 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.

5.1.5 *Downloading required components*

At the time of writing of this document, the MOFW components required for an installation is only the basic Standalone Monitor Over Firewall LRE 2021 installer. The base installer can be located in the download section of your specific LRE instance as explained below. Alternatively, feel free to contact Micro Focus SaaS at the time of installation to determine the latest service packs and patches if required.

Important: Do ***not*** use installers obtained from other sources than your Micro Focus SaaS LRE instance or the Micro Focus SaaS team.

Standalone Monitor Over Firewall installer

This installer can be downloaded directly through the LRE application:

- Log on to the LRE application using your domain/project and user credential information.
- On the dashboard, top left, click the Dashboard icon:



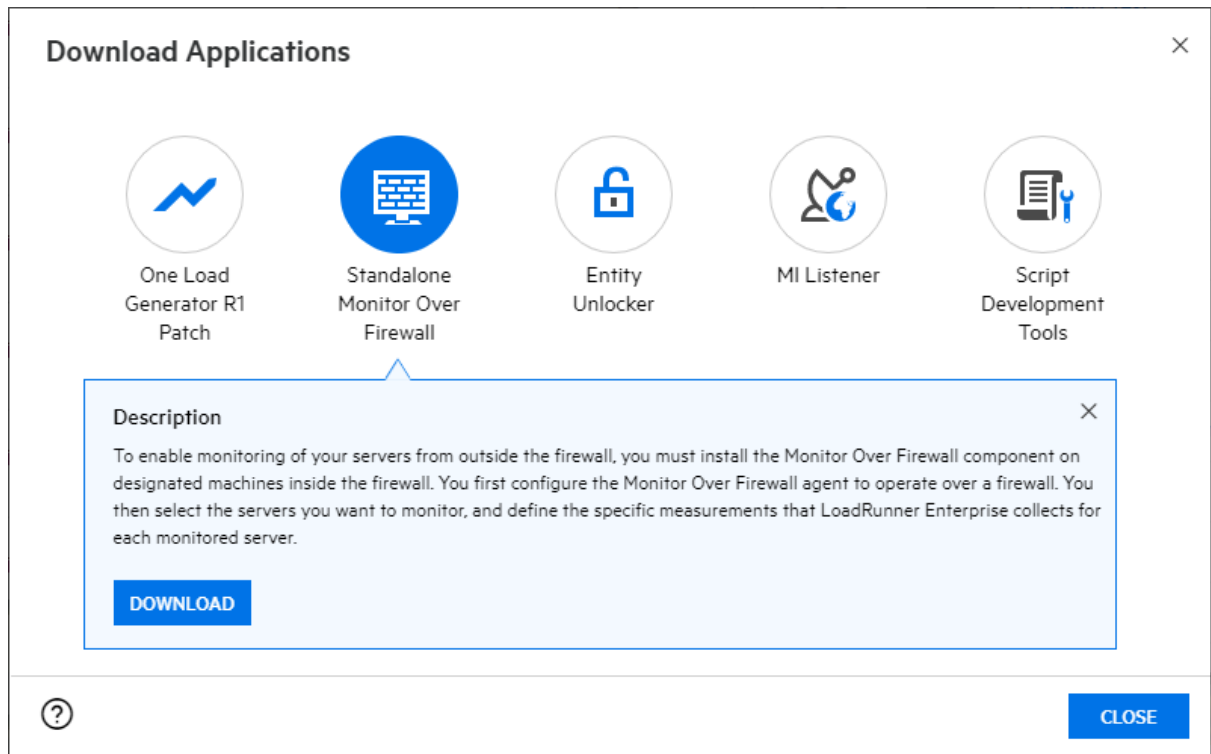
- Select "Download Applications":

MORE TOOLS

Controller Options >

Download Applications >

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



- As soon as the Windows file download dialog shows, save the file on your hard drive.

Version matching

LRE 2021 requires the matching LRE 2021 Standalone Monitor Over Firewall installation (no version difference), as present in the “Download Applications” dialog.

Patch installers

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.

At the time of writing, no patches are required for the LRE 2021 Standalone Monitor Over Firewall.

6 Installation

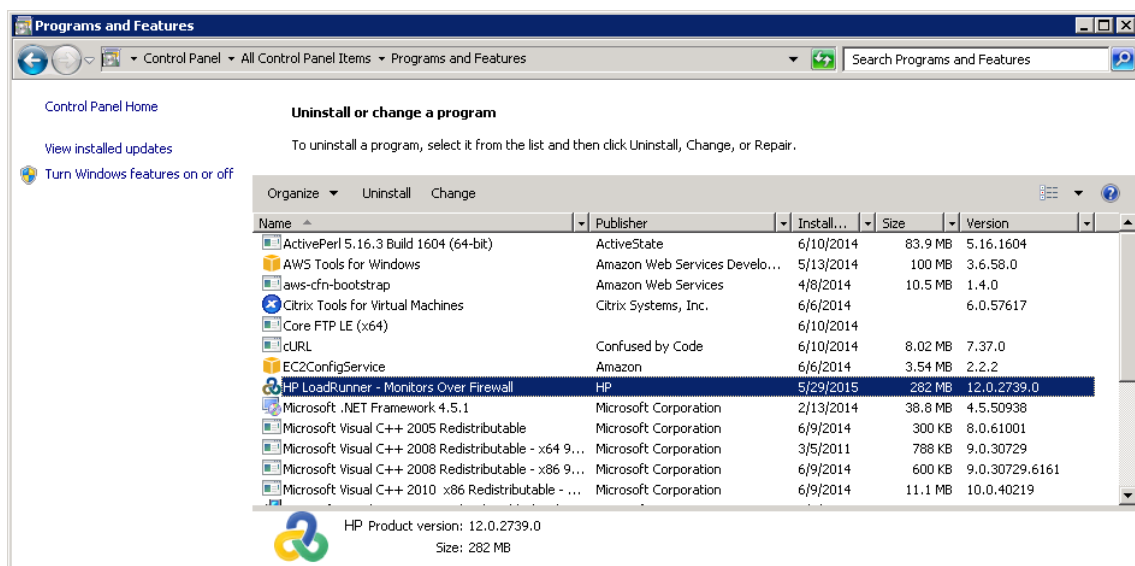
The MOFW installation on the host is straight-forward, using the base installer obtained in the preparation phase earlier and running an automatic patch update as described later.

6.1 Checking for pre-installed components

The installation of the Standalone Monitor Over Firewall requires that no previous versions of the MOFW software is present, and that no other LRE components such as VUGen, Analysis or IOFW are installed. None of those components are allowed to exist on the machine where the Standalone Monitor Over Firewall is installed.

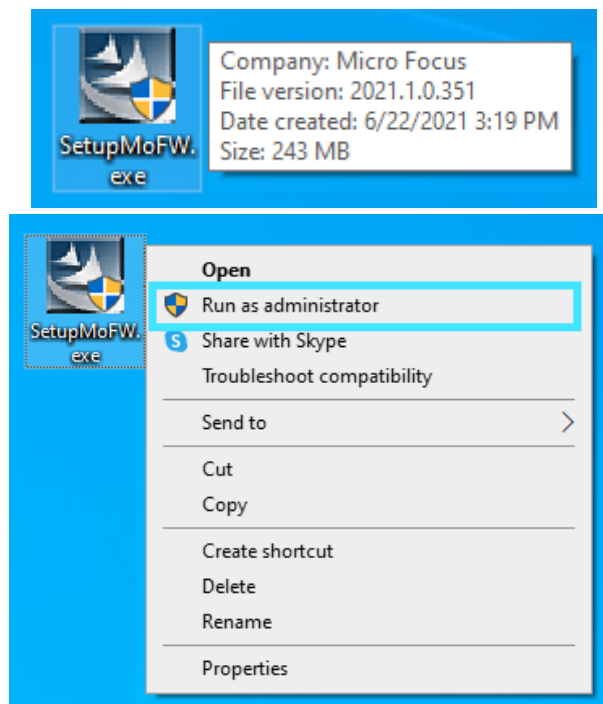
Hence, as a first step, make sure that no old versions of LoadRunner, IOFW or MOFW are present, and uninstall them in case. You can check for pre-installed components through the Windows Control Panel/Add or Remove Programs.

In the example below, an older installation of MOFW is already present, including its patches. Hence, before a desired installation, the “Monitors Over The Firewall” program would have to be removed, in turn automatically removing the patches as well.

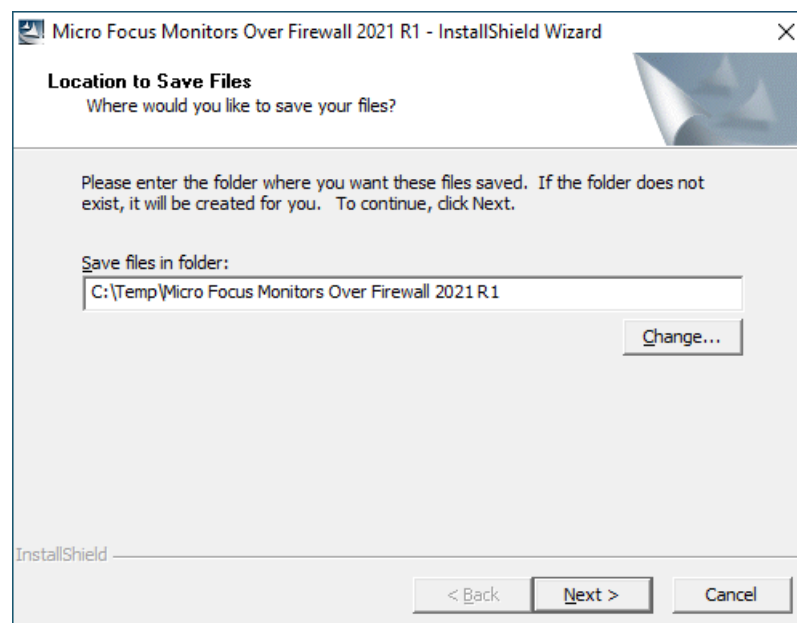


6.2 Base installation

- 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:**



- Find a temporary location for the installer to decompress the files, or accept the default location:

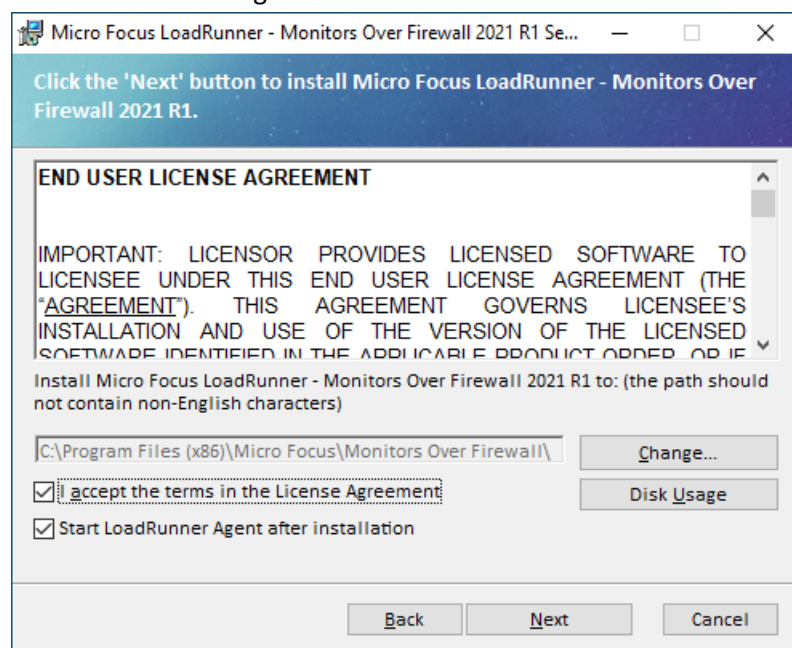


- The installer will decompress the necessary files into the given folder.
- Accept any host reboot requests. Any reboot should also restart the installer automatically. If not, open "setup.exe" inside the temporary installation folder to kick off the installation.
- Accept any requests to install prerequisite programs that have been determined to be missing.
- This may include components such as the .Net Framework 4.6.2 installers, MS Visual Studio C++ redistributables, latest Windows updates, and more.

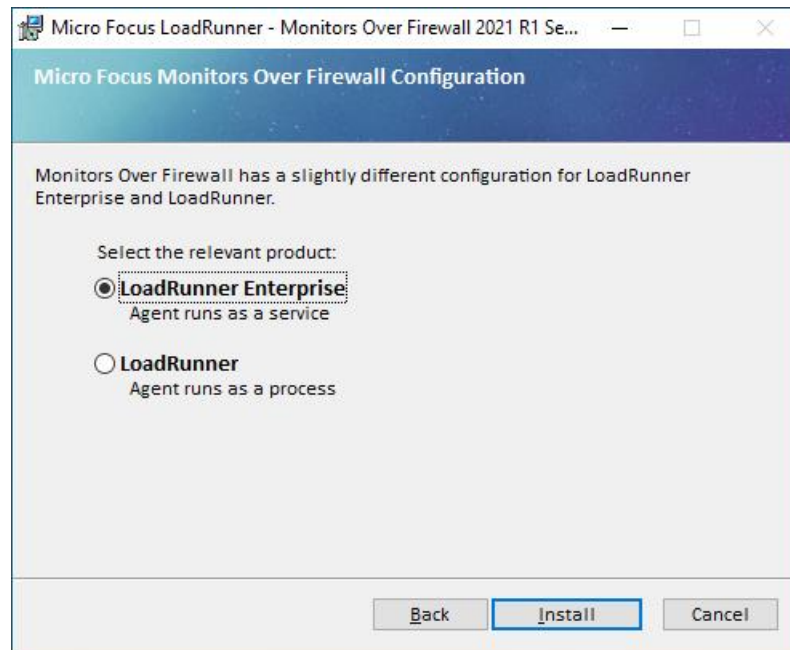
- Depending on the Operating system, when installing the .net framework, you may be asked to reboot the host (otherwise the installation may not yet get recognized by the Standalone MOFW installer). In that case, accept the restart and start the MOFW installer again.
- At the end of the installation of a prerequisite component, depending on the component, the Standalone MOFW installer will either continue by itself:
 - Or you may be required you to restart the Standalone MOFW installer again,
 - Or you may have to accept system restarts after being prompted to. In this case, you will have to start the MOFW installer again once the restart has completed.
- Once the prerequisite installation has completed, in the MOFW installer, follow the instructions on the screen and provide the requested information. First click “Next”.



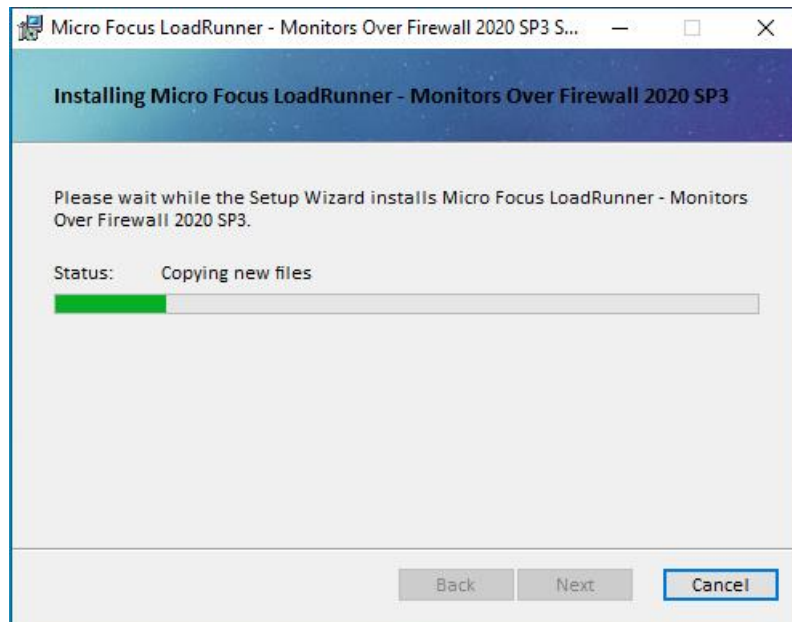
- You will now see the license dialog.



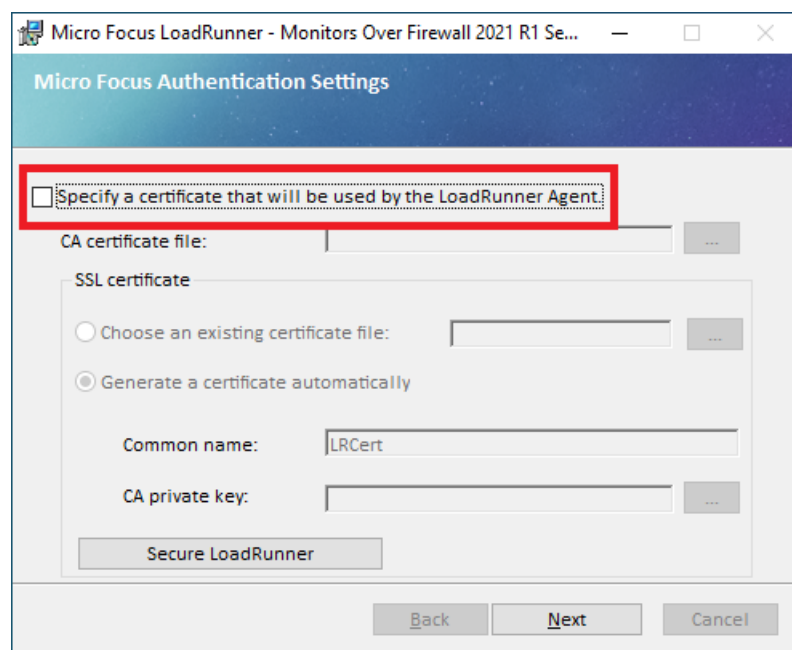
- Check available disk space using the “Disk Usage” button and select a different installation folder if necessary.
- Select “Start LoadRunner Agent after installation” and accept the terms in the license agreement and hit “Next”.
- Next, select the “LoadRunner Enterprise” product:



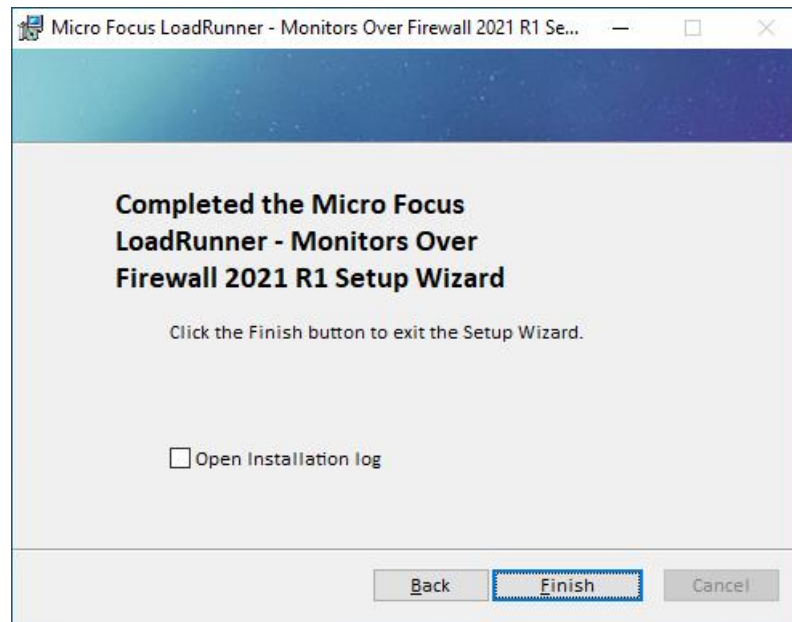
- In SaaS, **we recommend choosing “LoadRunner Enterprise”**. This leads to installing the MOFW Agent as a service, providing permanent availability whenever the host is up and running.
 - Selecting “LoadRunner” instead would require that before starting a load test session, the MOFW Agent process will have to be started manually after logging into the host (and typically, also stopping the process testing has finished).
 - In case that an MOFW Agent was installed in one way and needs to be changed to the other, please consult Appendix 10.1, “Configuring the MOFW Agent as either Service or Process” for instructions.
- Continue with “Install”. Now the installation is in progress.



- After installation, uncheck the flag “Specify a certificate that will be used by the LoadRunner Agent.”



- Finally, 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. At the time of writing this document, there are no patches available.

7 Configuration

Once the MOFW has been successfully installed as per the previous chapters, we now need to configure the MOFW Agent to connect successfully to the MI Listener, then configure 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**.
 - An example: almrwc1645p-mil1.saas.microfocus.com
 - This name is typically the public DNS name, and in some cases the public IP address, of the specific MI Listener in the Micro Focus SaaS network that the injectors will communicate with.
- 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 (IOFW) 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 all of the following criteria:

- Only alphabetical and numeric characters as well as dashes ‘-’ are allowed.
- We encourage the use of numbers, if prefixed with names.
- The name must start with a letter.
- MOFW names must be unique (across the LRE site). Hence, the name must be descriptive, contain customer-specific information and cannot be generic (“mofw01”, “mofw” are not valid examples).
- We recommend starting the name with an abbreviation of the customer 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”, “siiwestmofw01”, “siinyork-mofw”

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

As mentioned in the prerequisites chapter under “Network requirements between the MOFW Agent and Micro Focus SaaS”, in order to function properly, MOFW hosts need to have network access to

reach the MI Listener from your network. Network access can be provided through one of two means:

Case A (typical, preferred): Direct communication on port 443, and Firewall Request

In order for this to work, the firewall between the MOFW and the internet needs to be open for outbound communication on port 443 against the MI Listener DNS name (or, less preferable, IP address).

At this point, make sure to test if the firewall is open from your MOFW, using the simple test described in Appendix 10.4.

In case the firewall is not open yet, you will need to file a specific firewall request to your security team to open the firewall for:

Outbound communication for the specific host IP addresses of the MOFW host (or their subnet) on port 443 towards the MI Listener DNS name(s) or MI Listener IP address provided by Micro Focus SaaS.

Note that the firewall rule does not need to be bidirectional, as incoming connections can still be blocked safely without functional impact on LRE. Only outbound connections on port 443 need to be allowed.

Make sure to repeat the test in Appendix 10.4 after the firewall rule has been implemented.

Case B (alternate): Proxy Communication

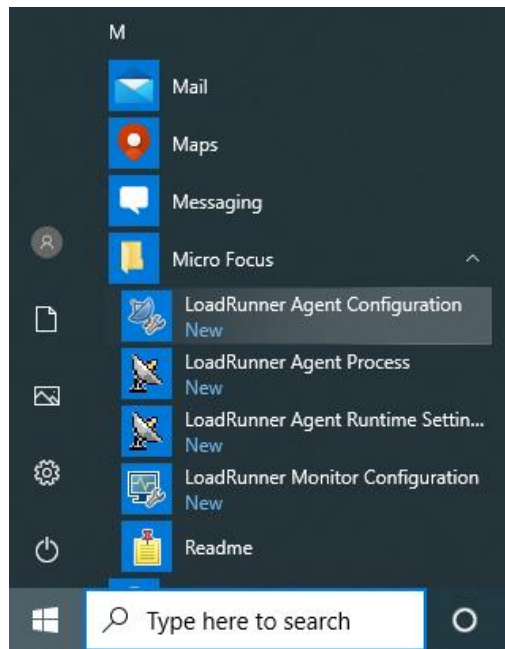
In this case, please contact your IT or security team to provide proxy configuration details, mainly the proxy's DNS name or IP address, and its port. Proxy credentials and/or protocol information may be required as well.

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.

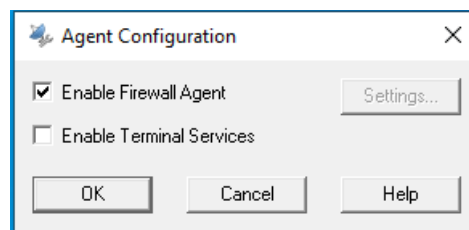
7.1.3 Agent Configuration

To configure the agent, start the agent through:

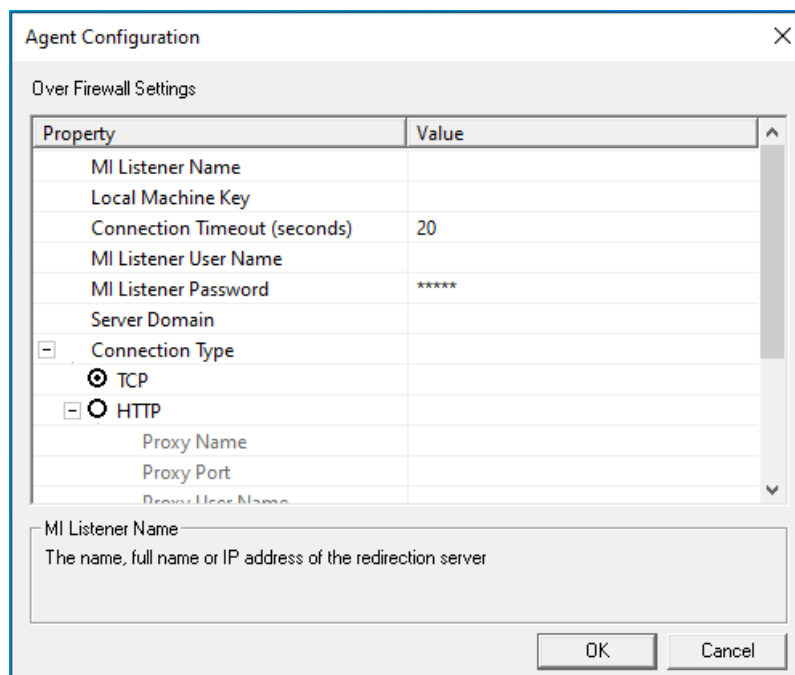
Start/Micro Focus/LoadRunner Agent Configuration



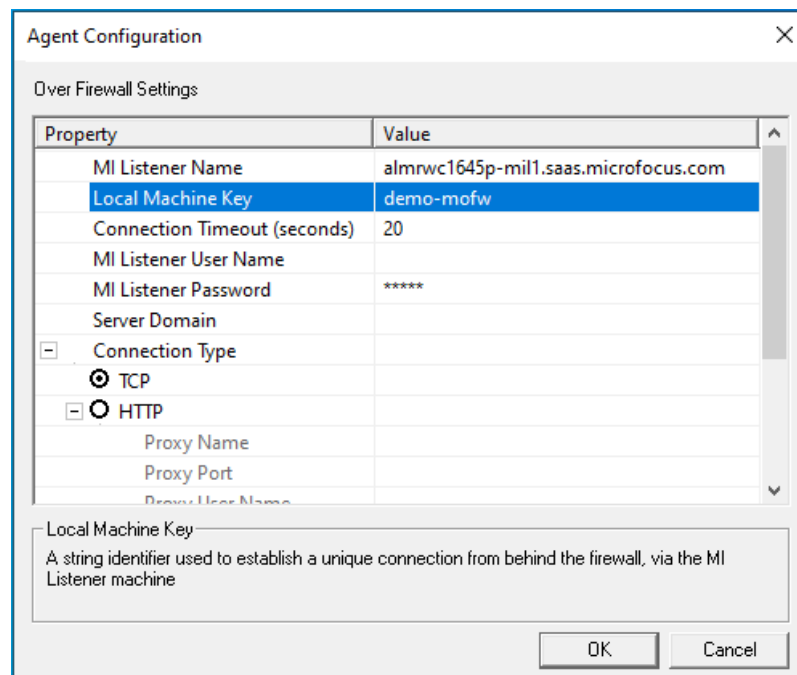
Select the “Enable Firewall Agent” checkbox:



Click “Settings”. The “Agent Configuration” dialog appears:



Enter the MI Listener Name, and the Local Machine Key.



The image shows a screenshot of the 'Agent Configuration' dialog box, specifically the 'Over Firewall Settings' tab. The dialog has a title bar with a close button. Below the title bar, there is a section titled 'Over Firewall Settings'. Inside this section is a table with two columns: 'Property' and 'Value'. The table contains the following entries:

Property	Value
MI Listener Name	almrwc1645p-mil1.saas.microfocus.com
Local Machine Key	demo-mofw
Connection Timeout (seconds)	20
MI Listener User Name	
MI Listener Password	*****
Server Domain	
Connection Type	
<input checked="" type="radio"/> TCP	
<input type="radio"/> HTTP	
Proxy Name	
Proxy Port	
Proxy User Name	

Below the table, there is a section titled 'Local Machine Key' with a description: 'A string identifier used to establish a unique connection from behind the firewall, via the MI Listener machine'. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

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

`almrwc1645p-mil1.saas.microfocus.com`

The Local Machine Key is the name only, no location string:

`demo-mofw`

Do note that the MI Listener will be different depending on the LRE instance.

Local Machine keys have to be spelled exactly as provided, and have the format:

`<mofwname>`

Finally check the **Use Secure Connection (SSL)** box to enable SSL communication between the MOFW and the MI Listener, which is required due to security concerns, 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.

Agent Configuration

Over Firewall Settings

Property	Value
<input type="checkbox"/> Connection Type	
<input checked="" type="radio"/> TCP	
<input type="radio"/> HTTP	
Proxy Name	
Proxy Port	
Proxy User Name	
Proxy Password	*****
Proxy Domain	
<input checked="" type="checkbox"/> Use Secure Connection (SSL)	
Check Server Certificates	None
Private key password	*****

Check Server Certificates:
Authenticate SSL certificates that are sent by the server. Medium - Verifies that the server certificate is signed by a trusted Certification Authority. High - verifies that the sender IP matches the certificate information.

OK Cancel

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.

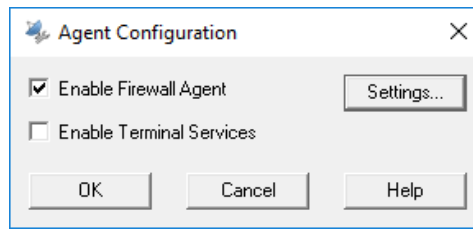
Agent Configuration

Over Firewall Settings

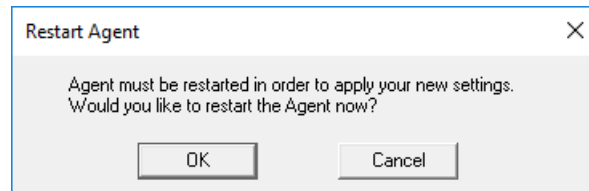
Property	Value
<input type="checkbox"/> Connection Type	
<input type="radio"/> TCP	
<input checked="" type="radio"/> HTTP	
Proxy Name	myproxy.example.com:8080
Proxy Port	
Proxy User Name	
Proxy Password	*****
Proxy Domain	
<input checked="" type="checkbox"/> Use Secure Connection (SSL)	
Check Server Certificates	None
Private key password	*****

OK Cancel

Click "OK" when done. The small "agent configuration" popup reappears.



Click “OK” again. You will be asked to restart the agent:

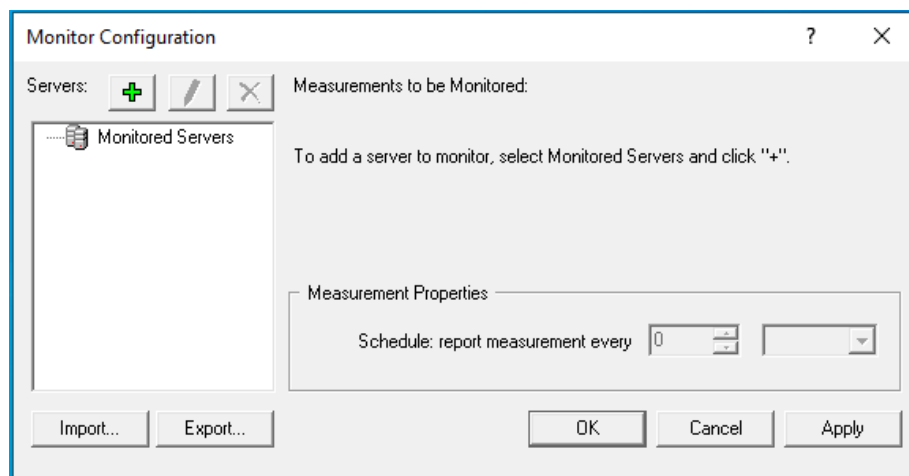
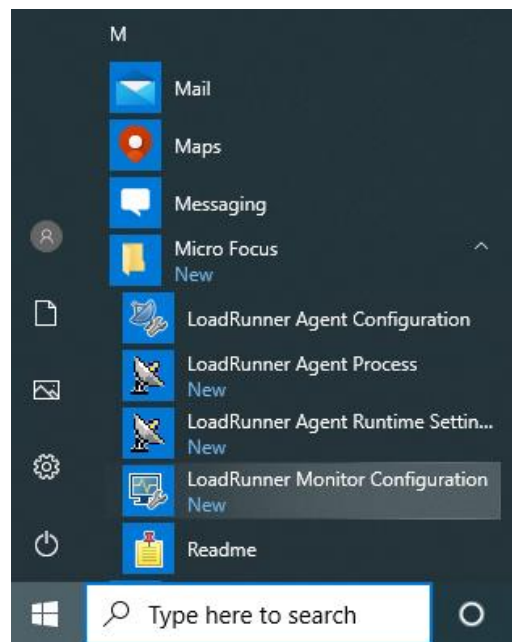


Confirm with “OK”.

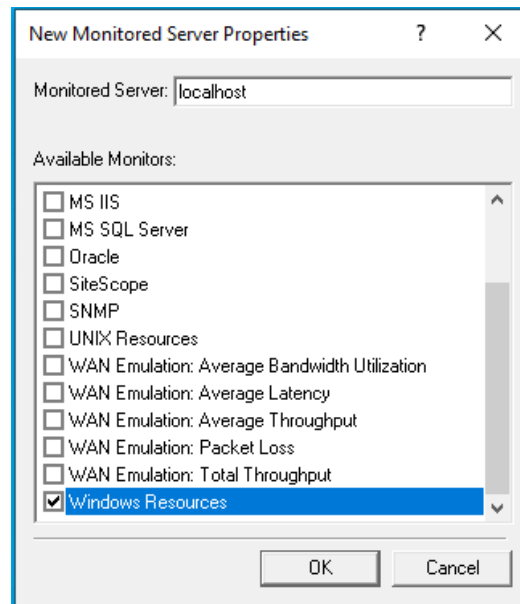
The agent configuration is now complete. Next we need to configure the monitors.

7.2 Monitors Configuration

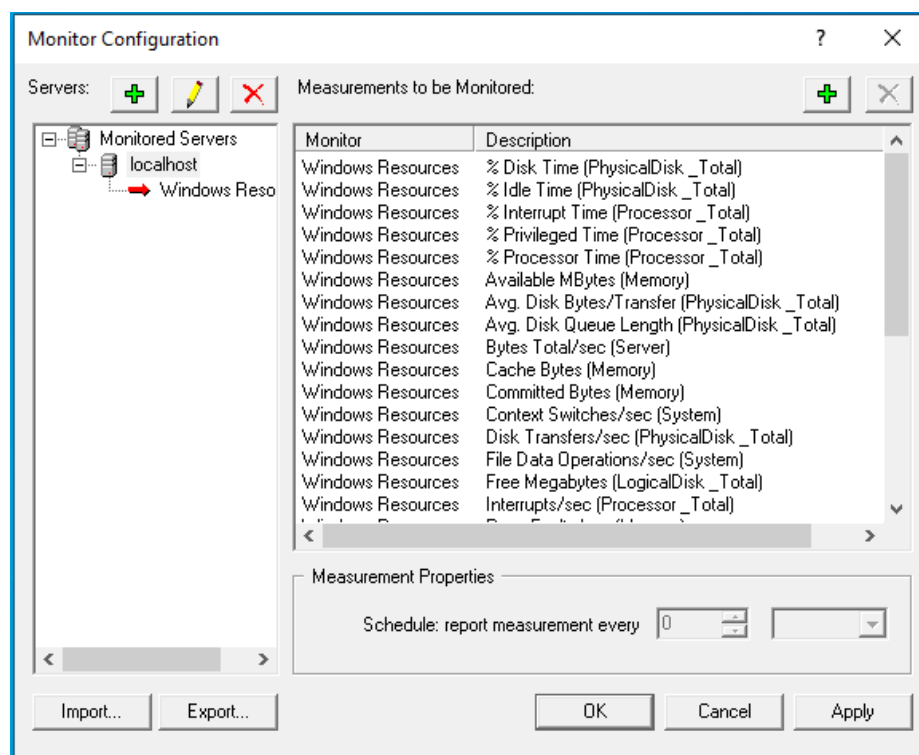
The next step is to configure which server counters the MOFW Agent will be collecting. Open the Monitor Configuration from the start menu:



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.

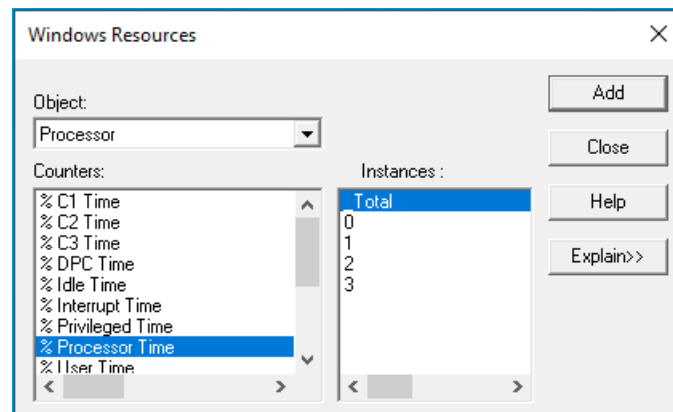


The Monitor Agent has a predefined list of server types and counters that could be captured by the product. It also has the ability to connect to Micro Focus SiteScope which is a more advanced monitoring tool. Once the server and a monitor type have been defined click OK and a default set of counters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

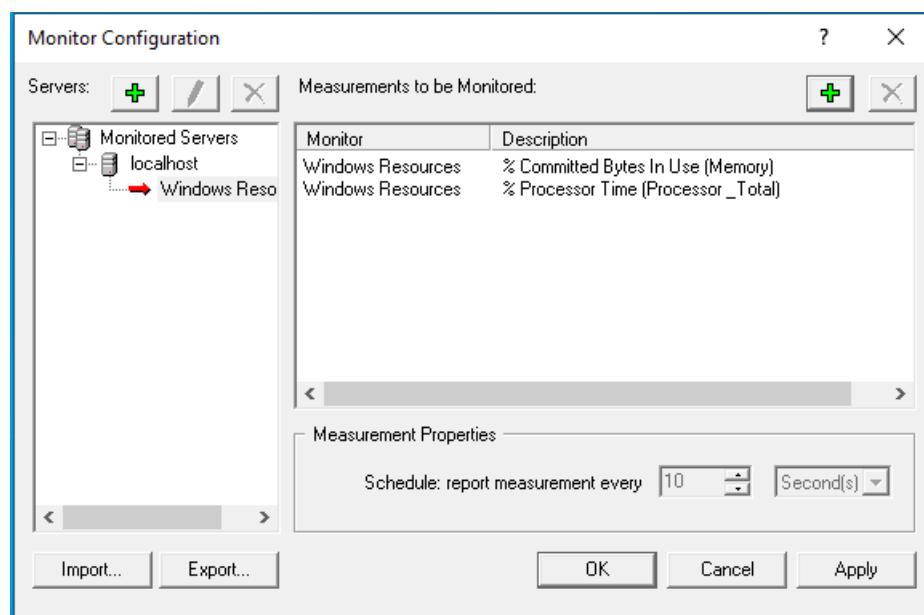


It is important to realize that the default set of counters might include counters that aren't available on the specific operating system that is being monitored, since different OS have slightly different counters. Due to that, best practice is to remove all the default counters and only add those of 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.

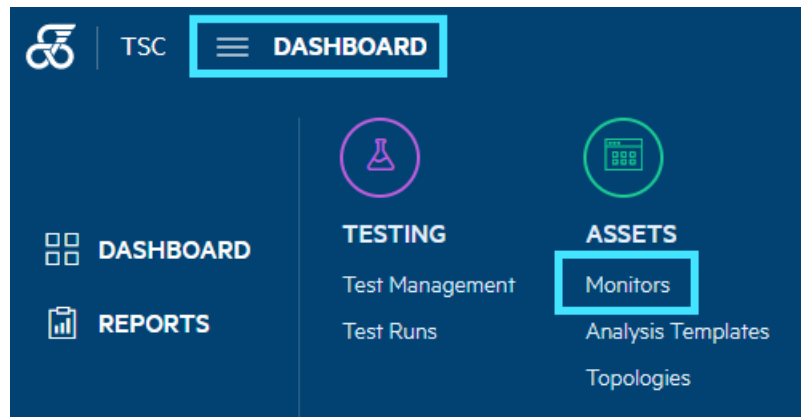


Click the OK button and the window will close, and the setup on the MOFW host is done.

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. It is important to remember that since we're using monitors on the other side of a firewall, we can't use the normal Monitor Profiles in LRE so we have to add the MOFW as a Resource.

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



- (Optional) Create a folder for the MOFW.
- Click the “New Monitor Over The Firewall Button” button.
- Enter a display name (which isn’t related to the Local Machine Key)
- Select Type: Monitor Over Firewall
- Enter the Local Machine Key that was used in the Agent Configuration
- Select the MI Listener (in most cases, there is only one MI Listener available for monitoring; keep that default. Note that the MI Listener name here may not reflect the public DNS name.)
- Click OK.

Create New Monitor Over Firewall

* Name:

* MI Listener:

* Machine Key:

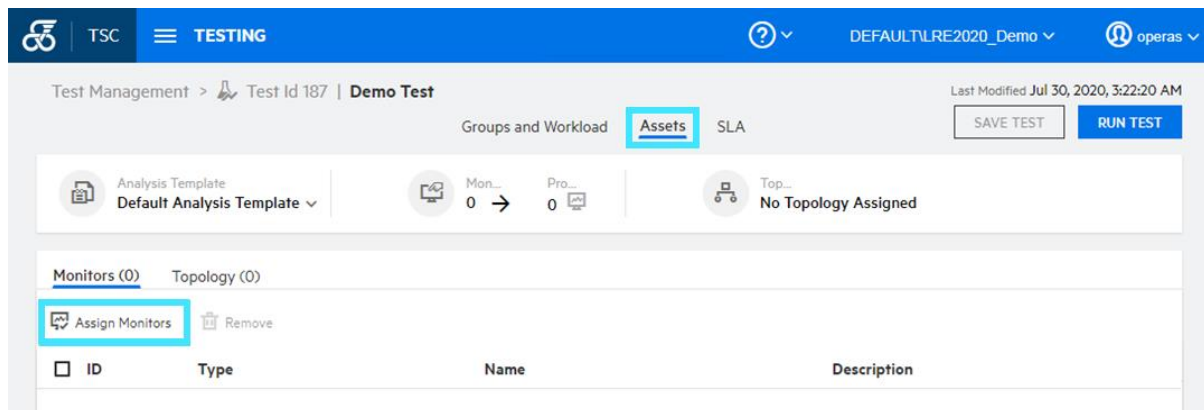
Description:

Messages

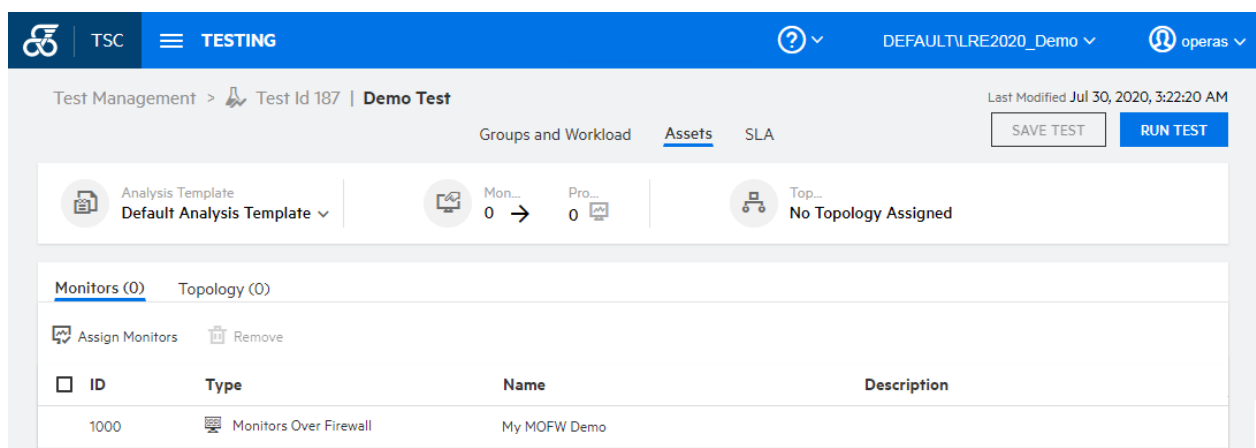
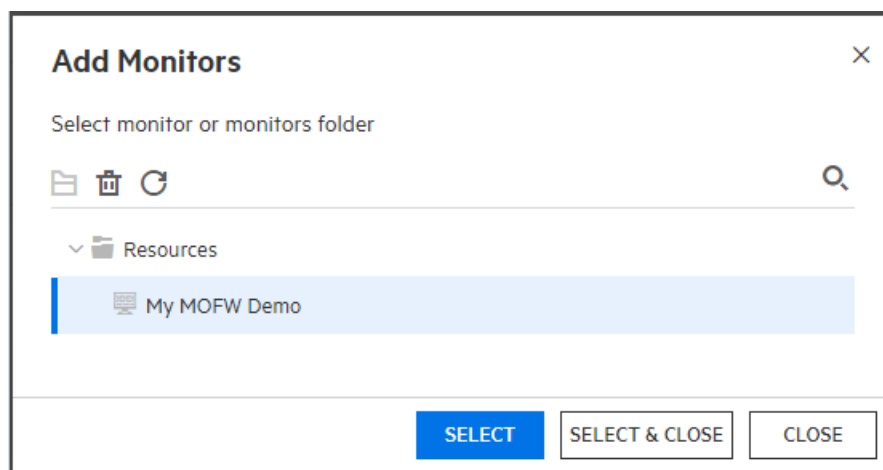
OK Close

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.



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



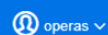
Once the test is running, although no Vusers need to be in a running state, the selected monitor measurements will start reporting after some time, but keep in mind that this might take up to a few minutes.



TSC

TESTING

DEFAULT/LRE2020_Demo ▾



Test Runs > Test Id 187 | Demo Test > Run Id 17

Dashboard

Results

Event Log

Audit

HTML Report

NV Report



Pending

Demo Test | Id: 17

00:03:14

Elapsed Time

Stopped

Scheduler st...

0.00

Hits per Sec

0

Errors

0

Transactions



10

Total Vuse...

→ 10

Not Sta...

0

Active

0

Finished

⋮

STOP RUN

Graphs Groups Transactions Messages



Users Details



Run Users



Load Generators



Timeslot Duration



Monitors ▾



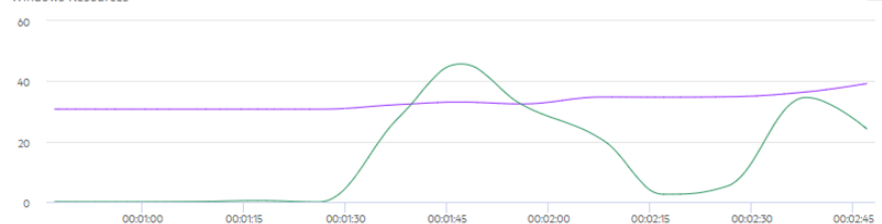
More ▾

Windows Resources



3m 10m 1h Whole

Windows Resources



2/2 selected



Show Only Visible



Has Anomalies

Name ▲ ▾

Name ▲ ▾	Scale	Machine	Max	Min	Avg	Std	Last
☆ % Committed Bytes in Use (Memory)	1	localhost	39.21	30.702	33.161	2.678	39.21
☆ % Processor Time (Processor_Total)	1	localhost	45.669	0.004	14.889	16.513	24.098

8 Troubleshooting

In case that 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 *"Monitors over a firewall - LRE 2021 R1 Installation Guide"* not suffice to resolve any technical issues, please inform us through the still open support case. Our team will reach out to you to help you resolve the matter directly.

Please add at least the following information to the existing 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 Micro Focus SaaS engineer may find it necessary to conduct in your presence a live remote diagnosis session on the MOFW host.

9 Using SiteScope with MOFW (Optional)

While the MOFW agent can connect to most servers and upload metrics to LRE, a more reliable and 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. Now you need to modify the MOFW agent to work with SiteScope.

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

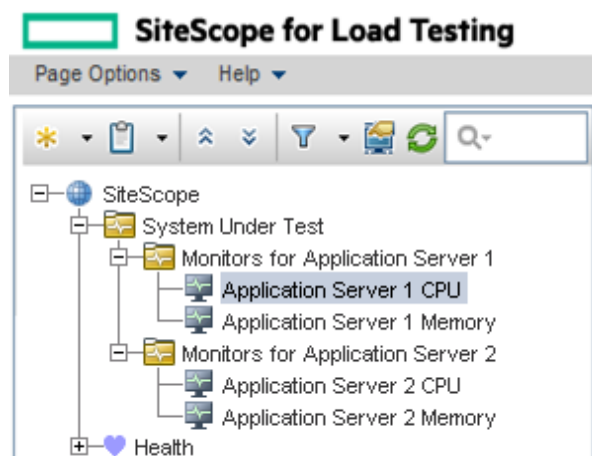
NOTE: LRE 2021 R1 supports integration with SiteScope 2019.11, 2020.05 and 2020.10 only.

- Install SiteScope according to installation instructions.

9.1 SiteScope Configuration

After browsing in Internet Explorer to 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.



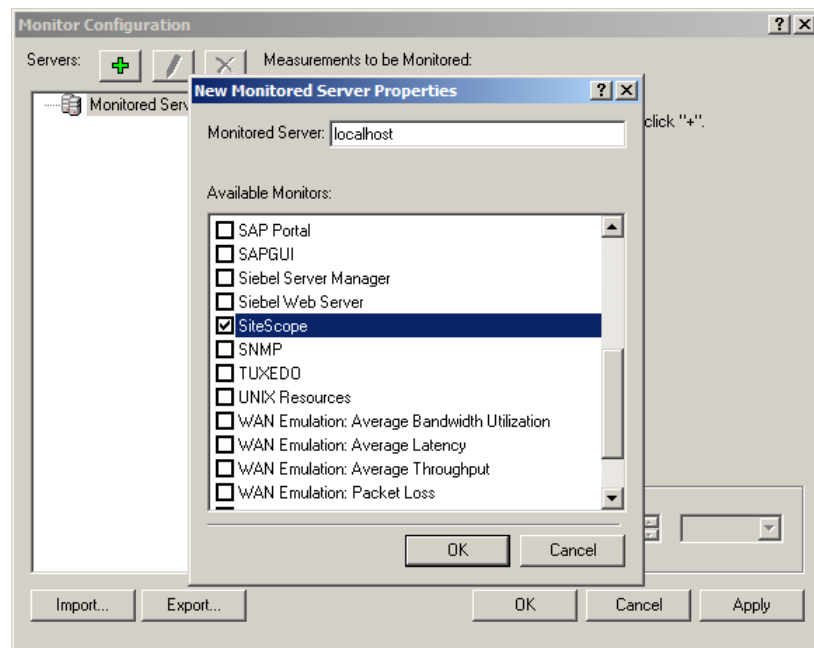
Do make sure that the Monitor has a green status indicating that data is being collected.

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%

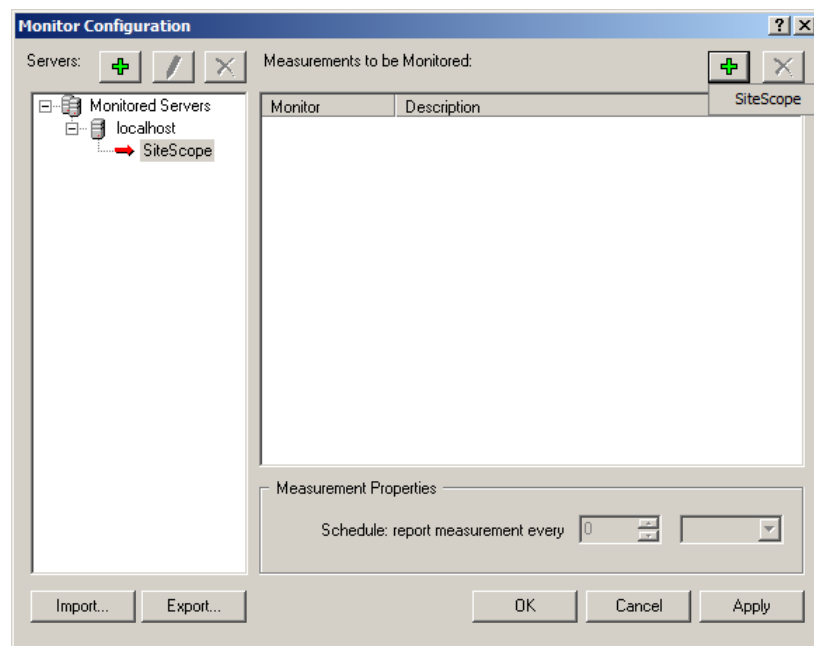
9.2 MOFW Configuration for SiteScope

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.

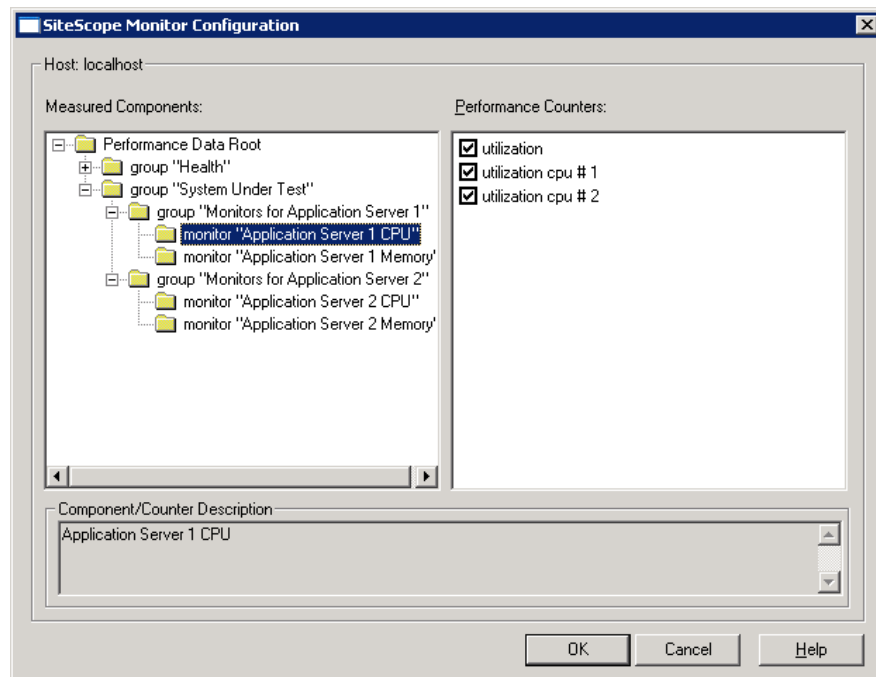
First we start the Monitor Configuration as before. Next, we bind SiteScope to the MOFW by registering a server “localhost” (or the network/host name of the host wherever the SiteScope application resides), and by adding a “SiteScope” monitor:



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 service or as a process.

The MOFW agent can be run either as service, or process. Micro Focus SaaS recommends running the agent as a service for most (permanent) setups, as the Agent becomes ready immediately after the host is started, then idling with minimal system resources.

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 have an effect on 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 <LG>\launch_service\bin folder. This requires a user to login to the machine in order 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 Micro Focus 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 <LG>\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 <LG>\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 <LG>\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 <LG>\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 redo the Standalone Monitor Over Firewall software installation completely, e.g. if the installation got corrupted. Please see steps for reinstallation below.

Note for multi-component installation

With some previous 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:

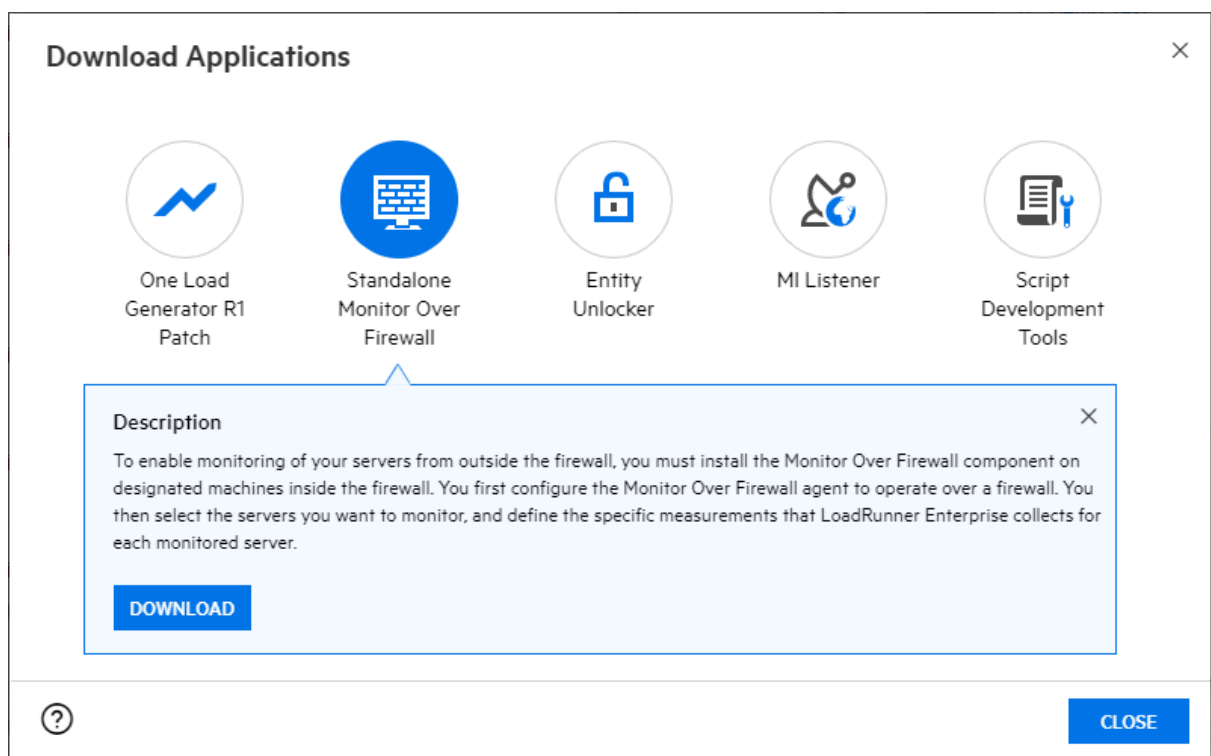
- Make a note of the Agent Configuration parameters.
- Obtain the Standalone Monitor Over Firewall software by downloading it from the LRE application ("Standalone Monitor Over Firewall"), using the "Download applications" button.
- Make sure your Windows account on the MOFW has administrative privileges.
- 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 are available for download from your LRE instance, certified for use by Micro Focus SaaS.**
- Regarding the installation order of patches, please follow any instructions provided in the download section itself.
- Alternatively, feel free to contact Micro Focus SaaS to inquire about the latest proper patch levels and installers.
- At the time of writing, for LRE 2021 R1, no SaaS-certified patches for Standalone Monitor Over Firewall are required. Patches are required if and only if shown in your download section.

Accessing Micro Focus SaaS Standalone Load Generator installers in LRE:



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

MOFWs can connect to the MI Listener in Micro Focus SaaS LRE in one of two ways: Either directly through your company's firewall through outbound port 443 (typical setup), or through a proxy in your network (less typical setup). If both possibilities are given, direct communication is to be preferred over proxy communication.

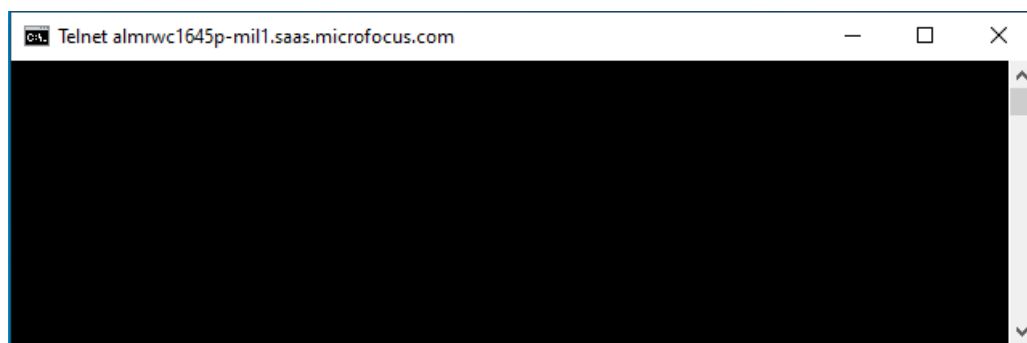
The following chapter describes how to test if the company's firewall is open for an MOFW to communicate outbound to its MI Listener through port 443.

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

Steps:

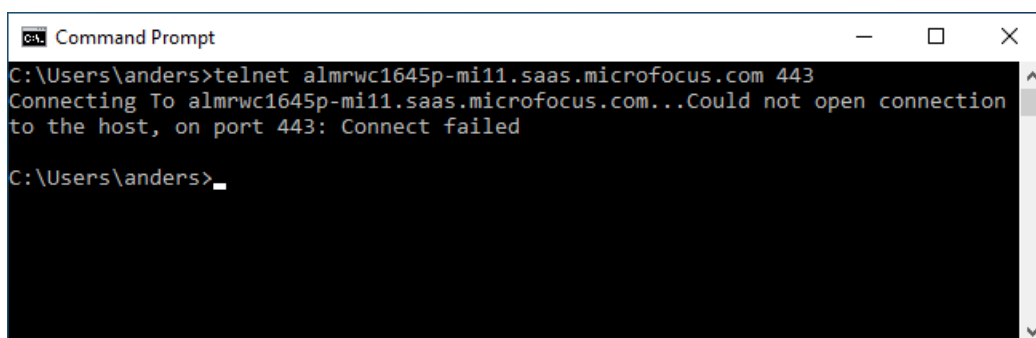
- Log in to the selected MOFW, e.g. through Remote Desktop Client (RDP).
- Open a Windows command shell (e.g. by Start/Run, typing "cmd").
- Enter `telnet <MI Listener DNS name> 443` and check the response.
- The MI Listener DNS name is provided by Micro Focus SaaS and needs also to be entered identically in the Agent Configuration's "MI Listener" field (see cause 2.2.2).
E.g. for MI Listener "almrwc1645p-mil1.saas.microfocus.com", the command is:
`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.
- Test completed.

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



- Then the firewall is not open and is in need to be opened by your IT Security team, unless you used 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 does not have to be bidirectional, as incoming connections can still be blocked safely without functional impact to LRE. Only outbound connections on port 443 need to be allowed.
 - Test completed.
- **Case 3 – telnet is not enabled:**
- If the response instead indicates that telnet is not enabled on this computer, then you can try enabling the telnet feature on the MOFW through Windows, as long as not forbidden by your IT organization or prevented by Windows security policy. Enabling telnet works slightly differently in various versions of Windows, though it is typically done through “Start/Control Panel/Programs and Features” or similar. E.g. on Windows 7, select “Start/Control Panel/Programs/Programs and Features/Turn Windows Features on or off” and make sure that the “telnet” checkbox is checked. After installation, repeat the test above.

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.
- As an alternative, you may try to open a browser on the MOFW host. Check in the browser settings if a proxy is configured. If not, browse an extranet URL of your choice that starts with “<https://>”. If you can access that site without proxy, in most cases it means that port 443 is open to ANY public DNS names and IP addresses (unless the specific site has been white-listed for you), and hence the MOFW should be able to reach the MI Listener also.