LoadRunner Enterprise

Software Version: 2021-2021 R2

Installation Guide

Go to **HELP CENTER ONLINE**

http://admhelp.microfocus.com/lre/

Document Release Date: November 15, 2023 | Software Release Date: October 2021

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 products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus 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

Contains Confidential Information. Except as specifically indicated otherwise, a valid license is 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

Contents

Welcome to this guide

Welcome to the LoadRunner Enterprise Installation Guide

LoadRunner Enterprise, a cross-enterprise tool for planning and running multiple performance test projects across different geographic locations, stresses your applications to isolate and identify potential client, network, and server bottlenecks.

This guide describes how to install and set up LoadRunner Enterprise 2021 or any later minor release (they are all full installations).

> **Note:** If your organization has firewall restrictions that prevent you from using the online Help Center, you can download and deploy the Help Center on your local server. For details, see the Download Help Center instructions in the LoadRunner Enterprise Help Center.

Installation overview

Before you install

This chapter provides information that will help you prepare for the LoadRunner Enterprise component installations.

This chapter includes:

LoadRunner Enterprise components and data flow

This section describes the LoadRunner Enterprise system.

This section includes:

- "Architecture and components" below
- "Applications " on page 13
- "Communication paths" on page 13
- "Load considerations" on page 16
- "Clustered configuration" on page 18

Architecture and components

This section describes the architecture and components of LoadRunner Enterprise.

Architecture/Component	Description
Database server	The database server stores four types of schemas: • **Site Management schema.** Stores information related to each tenant in the system, including users and site management tasks. A row exists in this schema for each tenant you create. • **Site Administration schema.** Stores information related to the LoadRunner Enterprise system, such as domains, users, and site parameters. A row exists in this schema for each project you create. Irrespective of how you configure your system, there is always only one Site Administration schema. • **Lab Management.** Stores lab information related to managing lab resources (such as hosts and host pools), and for managing LoadRunner Enterprise assets (such as LoadRunner Enterprise server, licenses, and usage reports). There is always only one Lab Management schema. • **Project schemas.** Stores project information, such as entity data and user data. A separate schema exists for every project you create. The schemas can reside on an Oracle or on a Microsoft SQL server. **Note:** To improve system performance, it is advisable that the LoadRunner Enterprise server and the Database server be installed on separate machines and be connected over LAN.

Architecture/Component	Description
Project repository	Stores all files to be used by all the projects in the system. For example, scripts, run results, .xml files, templates, and attachments. By default the repository is located on the same machine as the application server, which is useful for smaller setups. For larger organizations however, or when working in a clustered environment, it is advisable to install the repository on a dedicated machine. When working in a clustered environment, the repository must be accessible by all nodes.
LoadRunner Enterprise Server	Hosts the LoadRunner Enterprise Web pages that enable you to design performance tests, configure monitors, reserve testing resources, run and monitor test runs, and analyze test results.
LoadRunner Enterprise Administration	The center for managing lab resources (such as hosts and host pools), and for managing LoadRunner Enterprise assets (such as LoadRunner Enterprise servers, licenses, projects, runs, timeslots, and usage reports). Also used for managing cloud settings when using cloud hosts in LoadRunner Enterprise, and automated maintenance of the system's key components to detect system failures.
LoadRunner Enterprise Hosts	Used to control performance tests, generate load, and analyze data. LoadRunner Enterprise hosts can be configured as Controllers, load generators, or data processors: • **Controller.** The manager of a performance test. The Controller receives scripts, runtime settings, and a list of load generators to use. The Controller issues instructions to the load generators including which scripts to run, how many Vusers to run per script, and scheduler settings. At the conclusion of the test run, the Controller collates the data. There is only one Controller per performance test. • **Load Generator.** Generate load by running virtual users (Vusers). The Controller dictates the manner in which they start and stop running. There can be any number of load generators for a given test. • **Data Processor.** Used for analyzing and publishing performance test results.

Applications

The following standalone applications integrate with your LoadRunner Enterprise system:

Application	Description
Analysis	Provides graphs and reports with in-depth performance analysis information. Using these graphs and reports, you can pinpoint and identify the bottlenecks in your application and determine what changes need to be made to your system to improve its performance.
MI Listener	Needed when running Vusers and monitoring applications over a firewall.
Monitors Over Firewall Agent	Used to monitor servers that are located over a firewall.
OneLG	A combined load generator installer for all of the LoadRunner family products.
TruClient Standalone	Installs TruClient as a standalone application. Install this tool to record Web applications with TruClient technology. You save the recordings to a script that can be used in a performance test run.
Virtual User Generator (VuGen)	Generates Vusers by recording actions that typical end-users would perform on your application. VuGen records your actions into automated Vuser scripts which form the foundation of your performance tests.

Use the diagram and table in the "Communication paths" below and "Load considerations" on page 16 sections to determine which machines to allocate for which performance testing tasks.

For example, you can combine a number of applications that have a light load on a single machine. For details on which standalone applications can be installed together, see the Support Matrix (System Requirements) in the LoadRunner Enterprise Help Center.

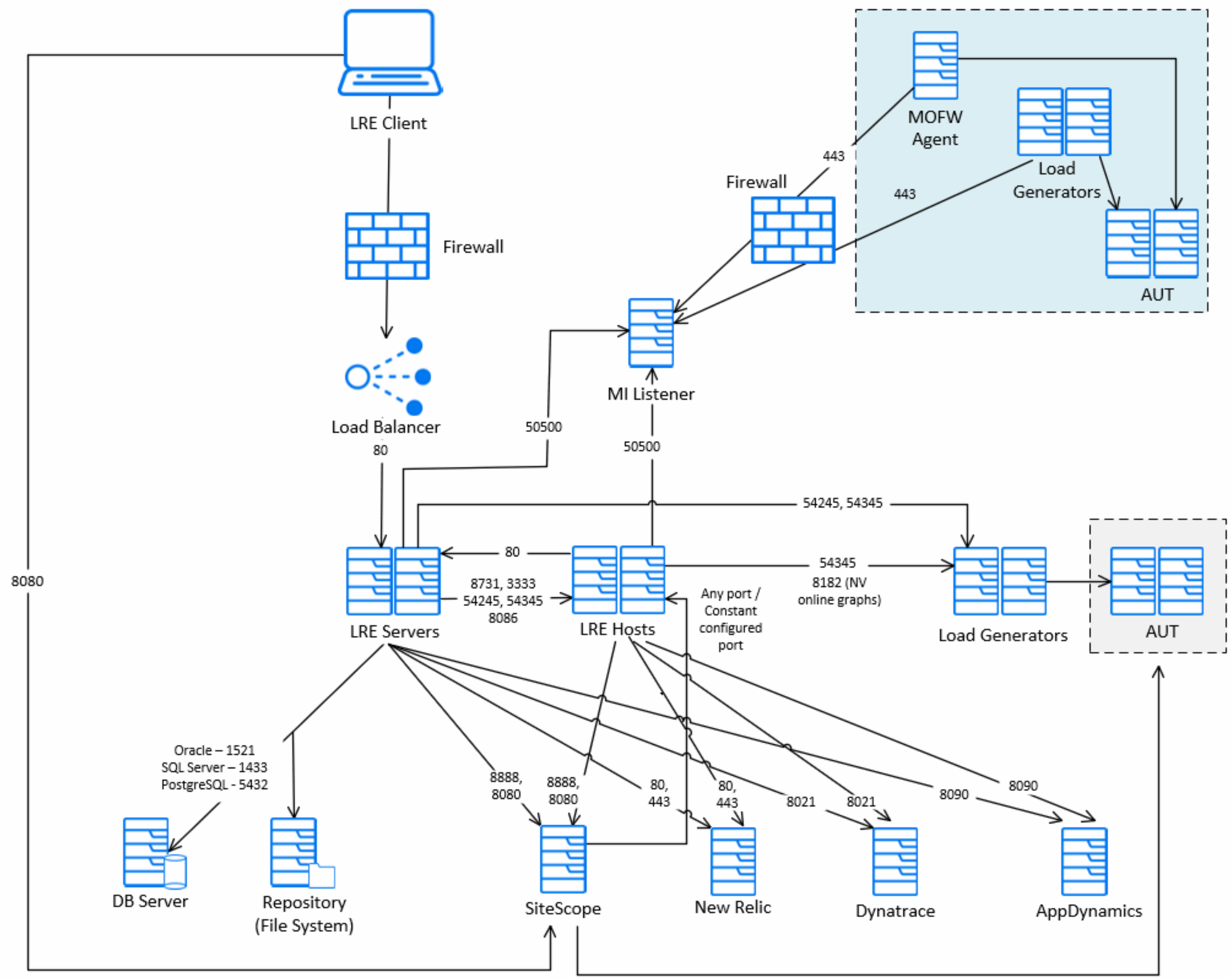
For information on installing the standalone applications, see "Install standalone components" on page 85.

Communication paths

When installing LoadRunner Enterprise, it is important to consider the communication paths between the various components, and their resource demands.

When running a performance test, components share information with LoadRunner Enterprise via a distinct system of communication. Understanding which components communicate with one another and the method of communication is essential for configuring your system.

The following diagram illustrates the LoadRunner Enterprise communication paths in an advanced deployment:



Note:

- To view other deployment options that can be used for configuring LoadRunner Enterprise on-premises or on the cloud, see LoadRunner Enterprise Deployments in the LoadRunner Enterprise Help Center.
- If the installation cannot use a default port because it is already in use, you can change the port. For details, see "Unable to install a LoadRunner Enterprise component if the default port is in use" on page 159.
- You cannot have a firewall between the LoadRunner Enterprise server, LoadRunner Enterprise hosts (used as Controllers), and MI Listener.
- Port 8182 from LoadRunner Enterprise host to load generators is relevant when running NV emulation for viewing NV related graphs during online. If the port is closed, graphs are still available in the offline results and Analysis report.

- Connections from APM tools to the AUT are not displayed in the diagram. Each AUT tool uses its own ports, which can be found in the corresponding product’s documentation.
- When using a load balancer for LoadRunner Enterprise servers:
  - The load balancer needs to be configured for sticky sessions based on the HTTP cookie **ASP.Net_SessionId**.
  - You need to configure WebSocket on the load balancer. However, if you have SSL configured on the load balancer only (and not on LoadRunner Enterprise servers), you need to terminate SSL for WebSocket on the load balancer.

The following table displays the connection ports that must be opened for the incoming traffic on the various LoadRunner Enterprise components:

Component	Ports
LoadRunner Enterprise Server	HTTP (80) * **
LoadRunner Enterprise Host	HTTP (8731) TCP (3333, 54245, 54345) 8182 for LoadRunner Enterprise hosts used as Load Generators to see online graphs for NV emulation information. If the port is closed, you can still see NV information in the offline results. 8731 for LoadRunner Enterprise server to communicate with the Load Testing Operator service that orchestrates the test. 8086 for LoadRunner Enterprise server/host to get online/offline analysis data. The port should be open for outgoing communication from the LoadRunner Enterprise server, and for incoming communication for the LoadRunner Enterprise host (for an internal database). For an external database, the port should be open for both incoming and outgoing communication from the LoadRunner Enterprise server and LoadRunner Enterprise host. 54345 for LoadRunner Agent Service. Enables the Controller to connect to this host when it acts as a Load Generator. 54245 for LoadRunner Remote Management Agent Service. Enables LoadRunner Enterprise server to perform lab maintenance operations on this host. 3333 for LoadRunner Data Collection Agent. Enables LoadRunner Enterprise to control the machine routing table during test execution, based on the definitions set in Target IPs in the project settings. It also enables getting resource utilization metrics while a test is running.

Component	Ports
Database	TCP 1433 (SQL), 1521 (Oracle) **, 5432 (PostgreSQL) **
Repository	NetBIOS
Standalone Load Generator	TCP (54245, 54345) 8182 to see online graphs for NV emulation information. If the port is closed, you can still see NV information in the offline results.
Cloud-based Load Generator	As defined in the Cloud Network Settings dialog box. For details, see Initial cloud settings in the LoadRunner Enterprise Help Center.
MI Listener	HTTP/TCP for load generator only: 443 ** TCP for LoadRunner Enterprise server and host (used as a Controller) only: 50500
Application under test	Any; HTTP (Random)
SiteScope - Topology	HTTP (8080) *
SiteScope - Monitor Profiles	HTTP (8888) *

* HTTPS is also supported on this component.

** Default values that can be changed during configuration.

Load considerations

The following table provides some basic installation considerations for each LoadRunner Enterprise component:

Machine	Quantity in the system	Load Considerations
LoadRunner Enterprise Server	At least one. Also supports cluster configuration. For details, see "Clustered configuration" on the next page.	Heavy load. To balance the load, you can install and configure external load balancers to work with LoadRunner Enterprise. For additional load balancing support, you can install multiple LoadRunner Enterprise Servers.
LoadRunner Enterprise Hosts: Controller, Load Generator, and Data Processor	At least one of each.	Controller has heavy load. Load generator has medium load. Data processor has medium to high load. It is recommended to designate spare Controllers and load generators for fault-tolerance and high availability purposes. **Note:** • You can configure a host as a Controller + Load Generator, but this is not recommended because running Vusers consumes a lot of resources. Running Vusers on the Controller host is only appropriate for performance tests that have a very small number of Vusers. • You can configure a host as a Controller + Data Processor, but this is not recommended because data processing might consume high amounts of CPU and resources.
MI Listener	At least one, if you are monitoring over a firewall.	Medium load. • Standalone installation is required. • Cannot exist on a machine running IIS.
Monitor Over Firewall machine	At least one, if you are monitoring over a firewall.	Light load. Standalone installation is required.
SiteScope (optional)	One	Light load.

> **Tip:** You should also consider the communication paths between the various components when installing LoadRunner Enterprise, and their resource demands. This information helps you configure your system to evenly distribute the load, and prevent overloading any particular resource. For details, see "Communication paths" on page 13.

Clustered configuration

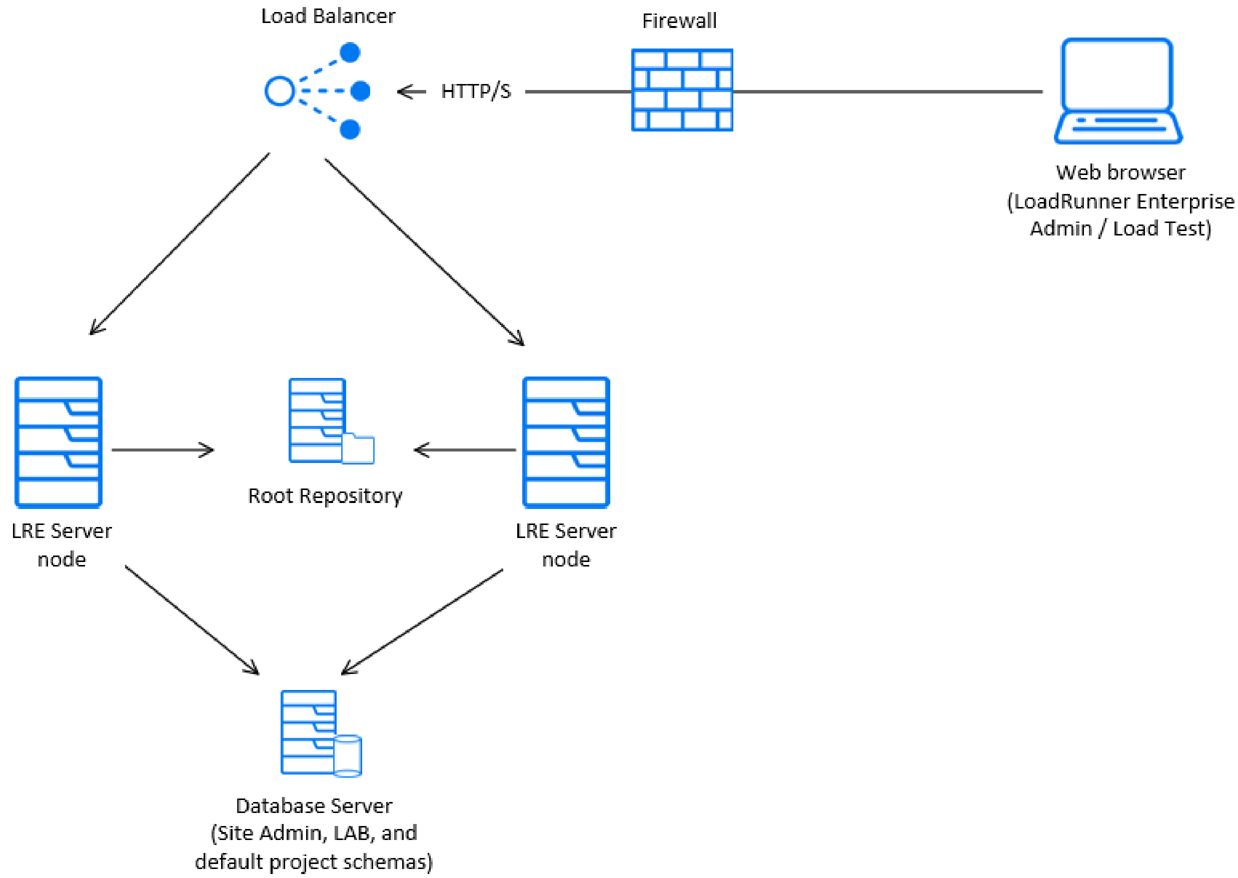
LoadRunner Enterprise can be run on a single node cluster. A cluster is a group of application servers that run as if they were a single system. Each application server in a cluster is referred to as a node.

Clusters provide mission-critical services to ensure maximum scalability. The load balancing technique within the cluster is used to distribute client requests across multiple application servers, making it easy to scale to an infinite number of users.

Take the following into consideration when setting up a clustered environment:

- All nodes must have access to the database server on which you configure the system.
- All nodes must have access to the repository. For example, if the repository is located on the first node in the cluster, all other nodes must have access to the first node. If you install the repository on a dedicated machine, each node must have access to that machine.
- The load balancer must be configured with session persistency. Set the persistency to **sticky session enabled** or **destination address affinity**, depending on the load balancer.

The following diagram illustrates a clustered LoadRunner Enterprise system configuration:



Prerequisites for clustering

You can install LoadRunner Enterprise on a single node or as a cluster. This section describes the prerequisites for installing LoadRunner Enterprise as a cluster on a Windows environment.

- Check with your system administrator whether you are installing LoadRunner Enterprise on a single node or as a cluster.
- If you are installing LoadRunner Enterprise on cluster nodes, verify which machine to use as the first node to start the installation and the number of machines you should use. This depends on the number of users and availability considerations.
- When creating a common repository for the cluster nodes, the folder must be shared with the domain user used for configuring the cluster nodes.
- The LoadRunner Enterprise account should be set with a domain user that has the correct permissions for setting a cluster environment; the IUSR_METRO user does not have permissions on a remote repository or on the IIS web server of the first node and on hosts.
- Install each cluster node with the same domain user.
- Configure each node with the same Site Administration and Lab database schema names (not just the same database server).

This is important because when a node is installed in cluster mode, the Lab schema name is not read from the common repository. For example, if node A is installed with schema names **LRE_ADMIN_MYSCHEMA** and **LRE_LAB_MYSCHEMA**, when node B is installed, the schema names will automatically be populated in the Configuration wizard with **LRE_ADMIN_MYSCHEMA** and **LRE_DEFAULT_LAB_DB**.

Therefore, you need to manually change the Lab database schema name from **LRE_DEFAULT_LAB_DB** to **LRE_LAB_MYSCHEMA**.

- You must use the same communication passphrase on all nodes.

For details on installing LoadRunner Enterprise as a cluster, contact Micro Focus support.

System component considerations

The LoadRunner Enterprise system includes several components. This section provides pre-installation considerations for each of the components.

For system requirement details for each component, see the Support Matrix (System Requirements).

LoadRunner Enterprise Server	**General:** • Uninstall any 12.6x or earlier installations of the LoadRunner Enterprise Server (formerly Performance Center Server) from your machine. Also make sure that Network Virtualization was uninstalled, or uninstall it manually. • To install a LoadRunner Enterprise Server, you must have full local administrative rights on the designated machine. • You can install LoadRunner Enterprise 2021.x as a full installation, or over an existing LoadRunner Enterprise 2020.x installation. If installing as a full installation, we recommend installing the LoadRunner Enterprise Server on a clean machine with a new image. • To install a LoadRunner Enterprise Server, you must have full local administrative rights on the designated machine. • The LoadRunner Enterprise Server requires a specific Windows user to be defined on the machine. When using the default user or a custom local user, the user will be created on the machine and will be added to the Administrator group. Ensure that there is no security system in place that will prevent creating the user or that will remove the user from the Administrators group. For details on how to create this user, see "Install and configure LoadRunner Enterprise servers and hosts" on page 47. • Microsoft Windows Script Host should be version 5.6 or later. To verify the version number, navigate to the **<Windows installation directory>\Windows\system32** directory. Right-click **wscript.exe** and select **Properties**. In the **Version** tab, verify the file version number. **IIS:** • Before you install the LoadRunner Enterprise Server, you must install Microsoft Internet Information Services (IIS 8.0/8.5/10). **Note:** For better security, we recommend you follow the Microsoft IIS security best practices to harden your IIS web server. • You must allow LoadRunner Enterprise file extensions in IIS. To do so, open IIS Manager. Under the IIS section for the LoadRunner Enterprise Server application, open **Request Filtering**. Click **Edit Feature Settings** and clear the **Allow unlisted file name extensions** option so only file extensions that are explicitly defined are used. Add the following to the list of allowed file extensions: .html, .js, .css, .map, .aspx, .ascx, .ash, .asmx, .eot, .otf, .ttf, .woff, .woff2, .json, .svg, .svc, .xml, .png, .jpg, .jpeg, .gif, .axd, .ico, and . (to include paths with no extension). • During installation, some IIS features are updated on all LoadRunner Enterprise Servers using IIS. • The following features are **enabled**: Active Server Pages, ASP.NET 4.5 (IIS 8.0/8.5), ASP.NET 4.6 (IIS 10), Metabase, Static content, IIS 6.0 Management Compatibility, and Dynamic Compression.

	• The following feature is **disabled**: URL Authorization **Oracle:** • Ensure that the Oracle client installed on the LoadRunner Enterprise server is at least the same version as on the Oracle server, and that connectivity is established with the Oracle server. • Only a 64-bit Oracle client installation is required. • If you install the Oracle client after installing the LoadRunner Enterprise Server, you **must** restart the machine after installing the Oracle client. • Oracle Monitoring: When defining Oracle monitors, install the LoadRunner Enterprise Server in a directory whose path does not include any of the following characters: ( ) : ; * \ / " ~ & ? { } $ % | < > + = ^ [ ]. For example, on a 64-bit machine, do not install the LoadRunner Enterprise Server in the default installation directory (**C:\Program Files (x86)**....), as this path includes illegal characters.
LoadRunner Enterprise Host	• To install a LoadRunner Enterprise Host, you must have full local administrative rights on the designated machine. • The LoadRunner Enterprise Host requires a specific Windows user to be defined on the machine. This user is configured when adding the Host to LoadRunner Enterprise Administration. When using a default user or a custom local user, the user will be created on the machine and added to the Administrator group. Ensure that there is no security system in place that will prevent creating the user or that will remove the user from the Administrators group. For details on how to create this user, see "Install and configure LoadRunner Enterprise servers and hosts" on page 47. • LoadRunner Enterprise supports the InfluxDB time series database for storing data externally. The InfluxDB time series database is installed as part of the LoadRunner Enterprise Host installation.
Standalone Load Generator (Windows)	You cannot install the Standalone Load Generator on the same machine as the LoadRunner Enterprise Server or LoadRunner Enterprise host.
Standalone Load Generator (Linux)	You can install the Standalone Load Generator on Linux to run Vusers. The Linux Vusers interact with the Controller that is installed on a Windows machine. For details, see "Install Load Generator on Linux" on page 87.
MI Listener	• The MI Listener must be installed on a standalone machine. • The MI Listener cannot be installed on a machine running IIS.

Monitor Over Firewall Machine	The Monitor Over Firewall agent must be installed on a standalone machine.
SiteScope Server	• SiteScope is used for monitoring applications. • Refer to the *SiteScope Deployment Guide* for minimum requirements.

Windows system locale considerations

The Windows system locale (Culture and UI Culture) of the user running the LoadRunner Enterprise environment (IUSR_METRO unless changed) must match the localized version of your LoadRunner Enterprise software. When working with a non-localized version of LoadRunner Enterprise, the locale must be set to English (EN-xx). Since the LoadRunner Enterprise user is created and configured when the machine is added to the LAB project, the system locale needs to be verified after completing all of the configuration steps.

For more details on setting the Windows system locale, see Software Self-solve knowledge base article KM01215254.

Required services

Before you install LoadRunner Enterprise components, check that the services defined in the table below are running on each component machine and that the startup type for each service is defined as **Automatic**.

> **Note:** The default settings for running the services on the operating system may differ from one version to another. You should go through all of the services on each machine to ensure that the required services are running.

Machine	Services
All LoadRunner Enterprise servers and hosts	• IPsec Policy Agent (for TCP/IP security) • Remote Procedure Call (RPC) • Windows Management Instrumentation (for LoadRunner Enterprise health check) • Windows Event Log (optional— used for debugging) • COM+ services (Event System and System application) • System Event Notification (for COM+)

Machine	Services
LoadRunner Enterprise servers	• IIS Admin Service (Microsoft Service) • Workstation • TCP/IP NetBIOS Helper • World Wide Web Publishing Service (Microsoft Service) • Distributed Transaction Coordinator (MSDTC)
LoadRunner Enterprise hosts	• Remote Registry Service (requires for host monitor)

LoadRunner Enterprise prerequisite software

Before you can install LoadRunner Enterprise, some prerequisite software must be installed on your machine. During installation, LoadRunner Enterprise checks whether the prerequisite software is installed on your machine. LoadRunner Enterprise enables you to automatically install missing software from the LoadRunner Enterprise installation package.

The following table provides a list of the prerequisite software and how LoadRunner Enterprise detects whether the software is installed.

> **LoadRunner Enterprise 2021 and 2021 R1 only:**
>
> - If Visual C++ 2017 Redistributable is already installed Visual C++ 2015 Redistributable will not be installed. Visual C++ 2017 Redistributable should be compatible in most cases. For more details, see the Microsoft documentation.
> - If installation of Visual C++ 2015 Redistributable Update 3 fails, install KB2999226 manually.

Prerequisite Software	Machines	Means of detection
.NET Framework 4.8	- All LoadRunner Enterprise server and host machines - Standalone VuGen - Standalone Load Generator - Standalone Analysis	Searches the registry key for the `Release` value. Its expected value should be greater than 528040: `HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full` **Note:** .NET Framework 4.8 replaces the .NET Framework 4.6.2 and earlier files. If there are any applications that are using the .NET Framework 4..6.2 or earlier files and are running during the installation of .NET Framework 4.8, you may need to restart your machine. If you are prompted to restart the machine, restart it before continuing the installation.
.Net core hosting 3.1.3	LRE server	Check for the registry key: `\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Updates\.NET Core\Microsoft .NET Core 3.1.3 - Windows Server Hosting (x86)`
Microsoft Data Access Components (MDAC) 2.8 SP1 (or later)	- All LoadRunner Enterprise server and host machines - Standalone VuGen - Standalone Analysis - Standalone Load Generator	Searches the registry key: `HKLM\Software\Microsoft\Data Access`

Prerequisite Software	Machines	Means of detection
Microsoft Core XML Services (MSXML) 6.0	• All LoadRunner Enterprise server and host machines • Standalone VuGen • Standalone Analysis • Standalone Load Generator	Queries the existence and version of: `%systemroot%\system32\msxml6.dll`

Prerequisite Software	Machines	Means of detection
Microsoft Visual C++ Redistributable for Visual Studio: • 2015 (LRE 2021 and 2021 R1) • 2015–2019 (LRE 2021 R2)	• All LoadRunner Enterprise server and host machines • Standalone VuGen • Standalone Analysis • Standalone Load Generator	Queries the MSI manager for the GUID: `{65E5BD06-6392-3027-8C26-853107D3CF1A}` In addition, the following Windows updates need to be manually installed: • **Windows Server 2012:** Required Updates: ◦ Update for Universal C Runtime in Windows (Also known as UCRT or KB2999226. See https://support.microsoft.com/en-us/kb/2999226.) • **Windows 8.1 or Windows Server 2012 R2:** Required Updates: ◦ March 2014 servicing stack update for Windows 8.1 and Windows Server 2012 R2 (See: https://support.microsoft.com/en-us/kb/2919442. Includes the KB2919442 update.) ◦ Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update: April 2014 (See https://support.microsoft.com/en-us/kb/2919355. Includes the following updates: KB2932046, KB2937592, KB2938439, KB2934018, KB2959977, KB2919355) ◦ Update for Universal C Runtime in Windows (Also known as UCRT or KB2999226. See https://support.microsoft.com/en-us/kb/2999226.) • **Windows 10:** No updates required

Prerequisite Software	Machines	Means of detection
Microsoft Visual C++ Redistributable for Visual Studio: • 2015 x64 (LRE 2021 and 2021 R1) • 2015–2019 x64 (LRE 2021 R2)	• All LoadRunner Enterprise server and host machines • Standalone VuGen • Standalone Analysis • Standalone Load Generator	Queries the MSI manager for the GUID: `{36F68A90-239C-34DF-B58C-64B30153CE35}`
Microsoft Windows Installer 3.1	• All LoadRunner Enterprise server and host machines • Standalone VuGen • Standalone Analysis	Looks for one of the following: • Registration of the WindowsInstaller. Installer.com object version 3 or later • MSI.dll version 3 or later in the %systemroot%
Internet Information Services (IIS)	LoadRunner Enterprise server	`HKLM\SOFTWARE\Microsoft\InetStp` Looks for both Major and Minor numbers. Supports following versions: • 8.0 (Windows Server 2112) • 8.5 (Windows Server 2012 R2) • 10.0 (Windows Server 2016 with Desktop Experience)
Strawberry Perl 5.10.1	• Standalone VuGen	Queries the MSI manager for the GUID: `{C977182F-221A-337A-B681-963808E0023A}`

Prerequisite Software	Machines	Means of detection
Windows Imaging Component (WIC)	• All LoadRunner Enterprise server and host machines • Standalone VuGen • Standalone Analysis • Standalone Load Generator	Queries the version of: `%systemroot%\system32\WindowsCodecs.dll`

Pre-installation prerequisites and considerations

This section includes pre-installation prerequisites and considerations for all LoadRunner Enterprise components.

Permission requirements	To install and configure a LoadRunner Enterprise server or LoadRunner Enterprise host, you must have full local administrative rights on the designated machine.
Planning the environment	• **Separate machines.** The LoadRunner Enterprise server and the LoadRunner Enterprise host cannot be installed on the same machine. • **LoadRunner installations**. You cannot install LoadRunner Enterprise components on machines with existing LoadRunner Professional installations. Before installing LoadRunner Enterprise, ensure that you have removed all versions of LoadRunner Professional from the machine. • **Load considerations.** Before you begin installing, you should decide which machine is to be used for what purpose. Consider the expected load on each machine when determining which components to install on which machines. For details, see "Load considerations" on page 16. • **Dedicated host machines.** We strongly recommend that you install LoadRunner Enterprise hosts on dedicated machines that do not contain, or provide access to sensitive information; and that you do a thorough security review of the network topology and access levels in your testing environment.

Disable UAC and DEP	To install LoadRunner Enterprise, you must first disable User Access Control (UAC) and Data Execution Prevention (DEP). For details on how to disable UAC, see: http://gallery.technet.microsoft.com/Registry-Key-to-Disable-UAC-45d0df25. For details on how to disable DEP, see https://community.microfocus.com/t5/LoadRunner-User-Discussions/How-to-TurnOff-Disable-DEP-completely/td-p/618234.
Not FIPS compliant	LoadRunner Enterprise server and host components are not FIPS complaint and cannot operate on a FIPS enabled Windows machine without additional configuration. For details on how to work with LoadRunner Enterprise on a FIPS enabled Windows machine, see Software Self-solve knowledge base article KM01420828.
Network considerations	• **Map network drive.** If the LoadRunner Enterprise installation directory is located on a network drive, it is recommended to map the network drive before you run the installation. For details, see "Unable to run the LoadRunner Enterprise component installation from a network drive" on page 158. • **Add to Trusted Sites.** To enable running the installation from a network location, make sure that the network location path is added to the Trusted Sites of the machine on which you are running the installation.
Remote Desktop connection	If you are installing a LoadRunner Enterprise server or LoadRunner Enterprise host using a Remote Desktop connection (RDP), you must connect using the Console session.
VMWare	LoadRunner Enterprise is certified to work with VMWare ESX/ESXi 5.0 and higher. Due to the rapidly evolving architectures provided by Virtualization vendors, as long as the third party vendor guarantees full compatibility of the virtualized environment with the LoadRunner Enterprise approved system requirements for physical hardware, then LoadRunner Enterprise will function as designed.
Standalone applications	For installation of standalone applications, you must manually install the prerequisite software. For the list of required prerequisites, see "LoadRunner Enterprise prerequisite software" on page 24. For details on installing the prerequisites in silent mode, see "Install LoadRunner Enterprise silently" on page 76.
Language settings	Ensure that the operating system and the database are both configured for the same language. If not, some texts displayed in LoadRunner Enterprise will be corrupted. For example, if you are working with German, ensure that you are working on a German operating system, and that the database is configured for German.

Database prerequisites

This section provides an overview of the prerequisites for connecting LoadRunner Enterprise to an Oracle, Microsoft SQL, and PostgreSQL database server.

> **Note:** Make sure you create the LoadRunner Enterprise database user before you start the LoadRunner Enterprise installation process.

Oracle Database servers

This section includes:

- "Oracle Database Admin user requirements" below
- "Oracle client requirements" below
- "Oracle Database considerations: Specify an Oracle user profile" on the next page
- "Oracle Database considerations: Add additional Oracle grants" on page 34

Oracle Database Admin user requirements

- To connect LoadRunner Enterprise to an Oracle database server, the installing database user must have sufficient permissions to perform certain administrative tasks in Oracle. These tasks include creating the project user schema and copying data between projects.
- If you are unable to use the Oracle system user due to security reasons, we recommend that your database administrator create a LoadRunner Enterprise database administrative user, for example **lre_admin_db**, with the specific privileges required to install LoadRunner Enterprise.

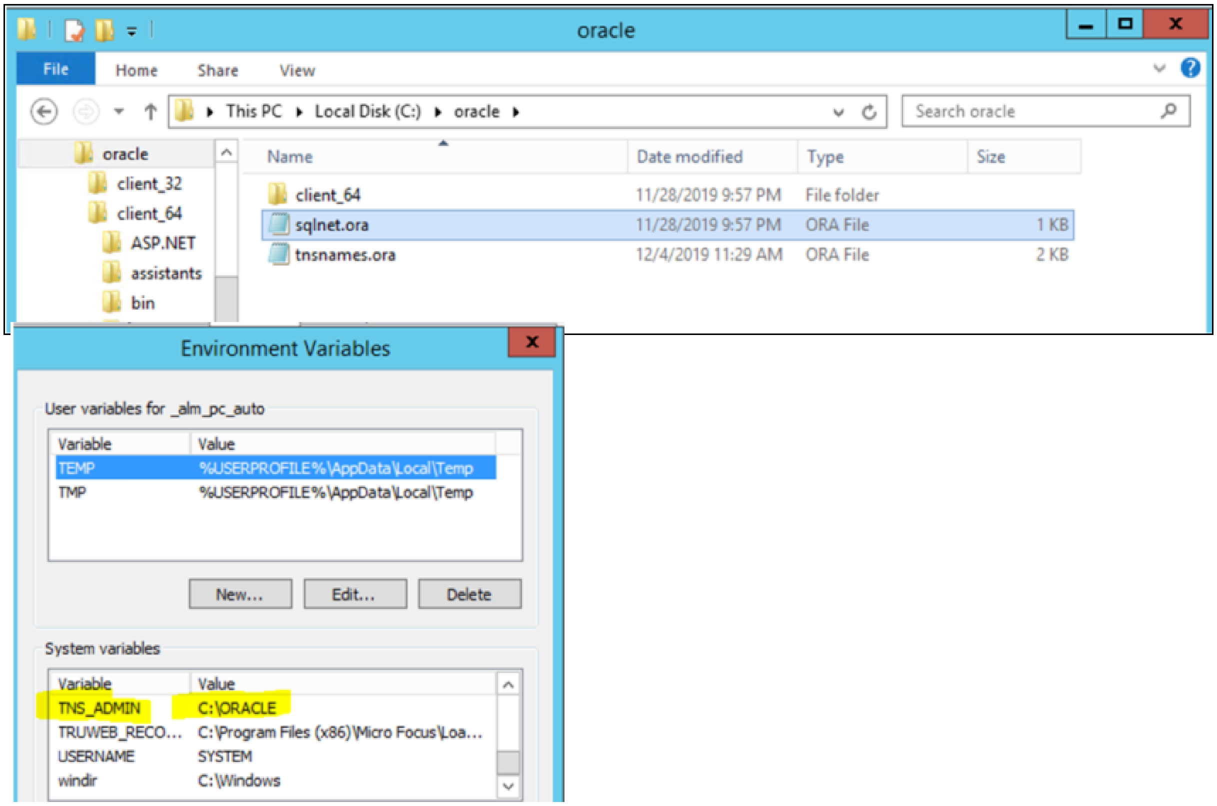
  Your database administrator can create a LoadRunner Enterprise database administrative user using a script, see this KB article. This script creates the LoadRunner Enterprise database administrative user with the recommended grants required on the database.

  If you are using a container database (CDB), all scripts for creating the LoadRunner Enterprise database user must be run while directly connected to the CDB. Those scripts should be run by a user with SYSDBA system privileges.

  > **Note:** When using CDB, the script invokes the "CONTAINER=Current" parameter.

Oracle client requirements

- The Oracle clients should be installed on the LoadRunner Enterprise server with **Administrator** installation type, and connectivity must be successfully established with the Oracle server.
- The **tnsnames.ora** file should contain the net service configuration that has the information to access the Oracle database server.
- Only a 64-bit Oracle client installation is required.



Name	Date modified	Type	Size
client_64	11/28/2019 9:57 PM	File folder	
sqlnet.ora	11/28/2019 9:57 PM	ORA File	1 KB
tnsnames.ora	12/4/2019 11:29 AM	ORA File	2 KB

User variables for _alm_pc_auto

Variable	Value
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

Variable	Value
TNS_ADMIN	C:\ORACLE
TRUWEB_RECO...	C:\Program Files (x86)\Micro Focus\Loa...
USERNAME	SYSTEM
windir	C:\Windows

To install the Oracle clients:

a. Create a root folder for the Oracle clients (`c:\oracle` in the example).

b. Install the Oracle client 64-bit version within a new dedicated folder (`client_64` in the example) under the root folder.

c. Copy the relevant **tnsnames.ora** and **sqlnet.ora** files into the Oracle clients root folder.

d. Set the **TNS_ADMIN** environment variable for the Oracle clients root folder (see the example above).

e. Restart the machine.

f. Install LoadRunner Enterprise. See "Install and configure LoadRunner Enterprise servers and hosts" on page 47.

Oracle Database considerations: Specify an Oracle user profile

Since every project created in LoadRunner Enterprise is a user in Oracle, and each user created needs to be connected to a profile, you can specify a profile for your project to use in the configuration. This profile is added to the user when the Oracle user is created.

1. On the LoadRunner Enterprise server, stop the LoadRunner Backend Service.
2. Copy the following:

```
"SiteParameters": {
   "OracleDbUserProfileForNewProject": {
   "Value": "",
   "Description": "Add the db profile that will be used when creating a new oracle user, value is a string",
   "IsSystem": true,
   "IsVisible": false
   }
}
```

3. Depending on the type of environment you are using:
   - For a clustered environment: To affect all cluster nodes, paste the copied section to the remote **appsettings.json** file under the repository (for example, **pc-repo\SqlEnvironment\system_config\**).
   - For a single node: To affect this node only, paste the copied section to **appsettings.json** in the **<LoadRunner Enterprise server installation>\LRE_BACKEND\** folder.

> **Note:** Do not make any changes to the default configuration file, **appsettings.defaults.json**.

4. Add the user profile you want to use to the **OracleDBUserProfileForNewProject** value.

   Make sure that you define the user profile in the same way that it is defined in the database—with or without quotes. When defined with quotes in the database, you must use the escape character (\ ) in the configuration file.

   Examples:

   Profile created without quotes:

```
"SiteParameters": {
   "OracleDbUserProfileForNewProject": {
   "Value": "myprofile",
   "Description": "",
   "IsSystem": true,
   "IsVisible": false
   }
}
```

Profile created with quotes (use escape character):

```
"SiteParameters": {
   "OracleDbUserProfileForNewProject": {
   "Value": "\"myprofile\"",
   "Description": "",
   "IsSystem": true,
   "IsVisible": false
   }
}
```

5. Make sure the JSON file is valid and save your changes.

Oracle Database considerations: Add additional Oracle grants

You can customize the LoadRunner Enterprise configuration file by adding additional Oracle grants to a user if the default grants are not sufficient.

1. On the LoadRunner Enterprise server, stop the LoadRunner Backend Service.
2. Copy the following:

```
"SiteParameters": {
   "OracleDbUserExtraGrants": {
   "Value": "",
   "Description": "Add extra grants to each user created by the app, separate each grant with ';' omit the word 'GRANT' and 'to', will added by the app.",
   "IsSystem": true,
   "IsVisible": false
   }
}
```

3. Depending on the type of environment you are using:
   - For a clustered environment: To affect all cluster nodes, paste the copied section to the remote **appsettings.json** file under the repository (for example, **pc-repo\SqlEnvironment\system_config\**).
   - For a single node: To affect this node only, paste the copied section to **appsettings.json** in the **<LoadRunner Enterprise server installation>\LRE_BACKEND\** folder.

Note: Do not make any changes to the default configuration file, **appsettings.defaults.json**.

4. Add any specific grants that you want to give to a user to the **OracleDBUserExtraGrants** value.

   Separate each grant with a semi-colon (;) and omit the words "GRANT" and "to" since they will be added automatically.

   Example:

```
"SiteParameters": {
   "OracleDbUserExtraGrants": {
   "Value": "EXECUTE ON SYS.DBMS.LOB",
   "Description": "",
   "IsSystem": true,
   "IsVisible": false
   }
 }
```

5. Make sure the JSON file is valid and save your changes.

Microsoft - SQL Database servers

Prerequisites

- To connect LoadRunner Enterprise to a Microsoft SQL database server, the installing database user must have sufficient permissions to perform certain administrative tasks in SQL.
  - **For SQL Authentication:** An admin database user with "dbcreator" level permissions and a user with "public" permissions.
  - **For Windows Authentication:** A domain user with "dbcreator" permissions. LoadRunner Enterprise must be configured with this service user.
- Collation for the SQL database server should be set to **SQL_Latin1_General_CP1_CI_AS**.

PostgreSQL Database servers

Prerequisites

To connect LoadRunner Enterprise to a PostgreSQL database server, the installing database user must either be:

- A PostgreSQL **superuser** with "CreateDatabase" and "CreateRole" permissions, or
- A PostgreSQL **non-superuser** with the following permissions:

```
Rolcanlogin = true
Rolcreatedb = true
Rolcreaterole = true
Rolconnlimit = -1
```

Notes and limitations

- Migrating projects from 12.6x versions of LoadRunner Enterprise on Oracle or Microsoft SQL to LoadRunner Enterprise 202x on PostgreSQL is not supported.
- If you try to install two environments (such as staging and production or a multi-tenant environment) on the same PostgreSQL database server, they will overrun each other.

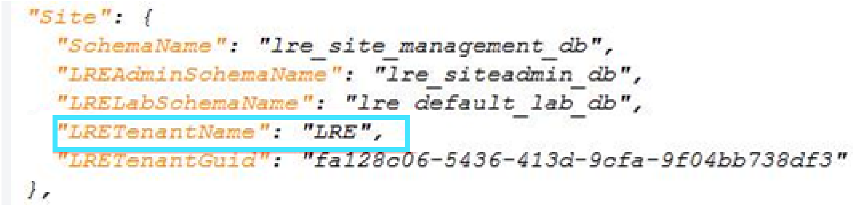
  Resolution: Set up a separate PostgreSQL database server for each environment.

  a. The first environment can be configured by running the LoadRunner Enterprise Configuration wizard. For details, see "Configure a LoadRunner Enterprise server or host" on page 51.

  b. For the second environment, you must change the LRE tenant name.

     i. Open the **appsettings.defaults.json** file located in the **<LR Enterprise server installation>\LRE_BACKEND** folder.

     ii. In the 'Site' section, change the **"LRETenantName"** value to one that is to different to the values on all the other environments.



```
"Site": {
  "SchemaName": "lre_site_management_db",
  "LREAdminSchemaName": "lre_siteadmin_db",
  "LRELabSchemaName": "lre default_lab_db",
  "LRETenantName": "LRE",
  "LRETenantGuid": "fa128c06-5436-413d-9cfa-9f04bb738df3"
},
```

- The first time you install LoadRunner Enterprise, and for every time zone change you make on the LoadRunner Enterprise server or database, make sure that you align the time zone from the operating system with the time zone in **postgresql.conf** on the database server machine. Failure to do so will result in the **Active Reservation/Timeslot ID** column being empty in the Hosts grid when you run a test.

  To align the time zone:

  a. On the database server machine, open pgAdmin. Open **lre_<tenant-name>_tenant_db** or any LoadRunner Enterprise related DB file.

     Open a new script and run:

     ```
     SELECT now()
     ```

     Check if there are any differences between the time displayed in the query result and the time of the operating system.

  b. Check the time zone set in PostgreSQL by running:

```
SHOW timezone
```

Check the time zone on the operating system to verify that a different time zone is set. If the time zones are the same then you have a different issue and there is no need to continue with these steps.

c. Navigate to **<postgresql-install-dir>/<version-of-pg>/data** and open the **postgresql.conf** file. Search for the "timezone" section. You should find the following line:

```
timezone = '<Continent>/<City>'
```

d. Go back to pgAdmin and run the following:

```
SELECT name, abbrev, utc_offset, is_dst FROM pg_timezone_names ORDER
BY utc_offset;
```

This should give you a table of all available values that you could put in the **postgresql.conf** file. Select the name that matches the operating system time zone. Replace the value in **postgresql.conf** with the chosen value, and save the file.

e. In pgAdmin run:

```
SELECT pg_reload_conf();
```

Followed by:

```
SHOW timezone
```

Followed by:

```
SELECT now()
```

It should now display the correct (OS) time zone and time.

f. Run a test and check for **Active Reservation/Timeslot ID** in the Hosts grid. The problem should be resolved.

Installation package details

You can find information and components for the installation as follows:

Support Matrix	Provides information on supported operating systems, technologies, and integrations. For details, see Support Matrix (System Requirements).
Standalone installations (for example, for the load generator)	Found in the installation package's **Standalone Applications** folder. For details, see "Install standalone components" on page 85.

Additional components (such as the Citrix Agent and so on)	Found in the installation package's **Additional Components** folder. For details, see "Install additional components" on page 97.

Pre-installation project migration steps

Project migration pre-installation activities

If you are migrating performance tests from Performance Center, this chapter presents migration considerations to be taken into account before installing LoadRunner Enterprise.

This chapter includes:

Pre-installation project migration considerations

Review and perform the following before migrating existing projects to LoadRunner Enterprise.

- To work with Performance Center/ALM projects in LoadRunner Enterprise, you will first need to upgrade your projects to Performance Center 12.6x (ALM 12.60) before you can migrate them to the latest version of LoadRunner Enterprise. For details, see "Upgrade existing Performance Center/ALM projects to LoadRunner Enterprise" below.
- In addition, review the Support Matrix (System Requirements) in the LoadRunner Enterprise Help Center to make sure you meet the requirements for working with the LoadRunner Enterprise version being used.
- Review the list of features that are not available or fully implemented in this release. For details, see Unsupported features in the LoadRunner Enterprise Help Center.
- Before beginning the installation, back up the projects, the database, and the repository. For details, see "Back up projects in existing ALM installation" on the next page.

> **Note:** During the migration process, data is taken from ALM in read-only mode so no changes should occur on the database level.

- Migrating projects from one database type in ALM 12.60 to another database type in LoadRunner Enterprise is not supported.

Upgrade existing Performance Center/ALM projects to LoadRunner Enterprise

The following table describes how to upgrade and migrate projects from Performance Center/ALM to LoadRunner Enterprise. Note that not all projects can be migrated directly to LoadRunner Enterprise.

From version:	To LoadRunner Enterprise
Performance Center 12.6x	Projects in ALM 12.60 can be migrated directly to LoadRunner Enterprise 202x, provided the LoadRunner Enterprise system user has access to the location where the Performance Center/ALM 12.6x repository (source for migration) is stored. For migration details, see "Project migration pre-installation activities" on the previous page.
Performance Center 11.52 - 12.5x	The Performance Center/ALM repository must be moved to the location of the ALM 12.6x repository. Projects must first be upgraded to ALM 12.60. For details, see the ALM 12.60 Installation and Upgrade Guide. **Note:** You must first upgrade **LAB_PROJECT**, and then any Performance Center template projects, before migrating Performance Center projects.
Performance Center 11.00	Projects must first be upgraded to ALM 11.52, and then to ALM 12.60. For details, see the ALM 11.52 Installation and Upgrade Guide. **Note:** You must first upgrade **LAB_PROJECT**, and then any Performance Center template projects, before upgrading Performance Center projects.

Back up projects in existing ALM installation

Back up all your projects in the existing ALM installation that you plan to migrate. We strongly recommend that you deactivate projects before backing them up.

If you must back up while your project is still active, you must back up the database before the file system. We also recommend backing up the file system as soon as possible after backing up the database. To back up and restore data from active projects, see this KB article.

> **Note:**
>
> - Before you run the migration process, perform a full backup of your projects that includes the project database schema and the project repository.
> - **Version Control:** Version control enabled projects cannot be backed up while there are checked out entities. All entities must be checked in to the corresponding version of Quality Center or ALM. To determine if there are checked out entities, see this KB article.

To back up the project database schema on the database server:

- **Microsoft SQL database.** To back up the project database schema on the database server, see this KB article.

- **Oracle database.** To back up the project database schema on the database server, see this KB article.

Overview of migration process

Migrating projects from Performance Center to LoadRunner Enterprise requires the following steps:

1. **Upgrading Performance Center projects to ALM 12.60 (pre-installation)**

   For details on upgrading Performance Center projects to ALM 12.60, see Upgrading Projects to a New Version in the ALM Help Center.

2. **Migrating the Site Admin and LAB schemas from ALM (during installation)**

   During the installation process, you need to migrate the configuration data that was stored in ALM Site Admin and LAB to LoadRunner Enterprise.

   For details, see "Configure Site Admin and LAB schema migration." on page 57

   > **Note:** You can also perform this step post-installation from the Configuration wizard, provided you specify a new Site Admin and LAB schema for LoadRunner Enterprise (if you use the existing schemas nothing will happen). For details, see "Post-installation configuration steps" on page 73.

3. **Migrating the project data (post-installation)**

   After installing LoadRunner Enterprise, you need to migrate project data and the file repository from existing projects to LoadRunner Enterprise using the migration tool in LoadRunner Enterprise Administration.

   Project data which includes scripts, attachments, run results, .xml files, and templates is migrated from ALM Site Admin and LAB to the LoadRunner Enterprise server.

   For details, see Migrate projects to LoadRunner Enterprise in the LoadRunner Enterprise Help Center.

Installation and configuration

Install LoadRunner Enterprise

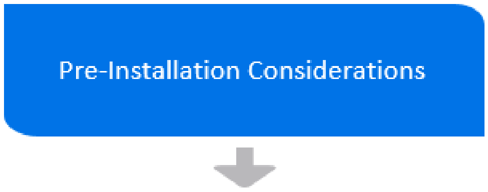
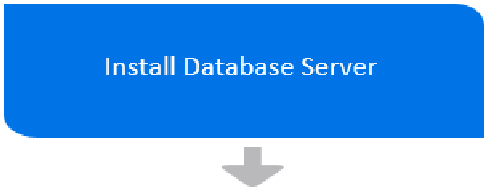
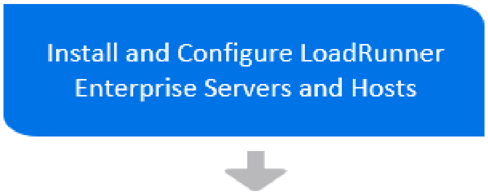
This chapter describes how to install LoadRunner Enterprise 2021 or any later minor release (they are all full installations).

> **Note:**
>
> - You can install LoadRunner Enterprise 2021.x as a clean installation, or over an existing LoadRunner Enterprise 2020.x installation; the installation process, which is the same for both, is described below. You can also migrate projects in ALM 12.60 directly to LoadRunner Enterprise 2021.x. For details, see "Project migration pre-installation activities" on page 40.
> - When upgrading from Performance Center 12.6x or LoadRunner Enterprise 2020, you need to request (and upload) new licenses to work with the upgraded LoadRunner Enterprise version. For details, see Set LoadRunner Enterprise license keys in the LoadRunner Enterprise Help Center.
> - If you are using host attributes in your tests and you plan to upgrade to LoadRunner Enterprise 2021 R2, you must upgrade your environment as follows to avoid losing host attribute data (you can ignore this note if you are installing LoadRunner Enterprise 2021 R2 as a clean installation).
>
>   a. Perform the installation steps in the LoadRunner Enterprise Setup Wizard (stop when the Configuration Wizard opens). For details, see "Install a LoadRunner Enterprise server or host" on page 48.
>
>   b. Download and run LoadRunner Enterprise 2021 R2 Hotfix 1 (**LRE2021_R2_Hotfix_01.2022.1.zip**) available from the Micro Focus FTP server or by contacting Micro Focus support.
>
>   c. Run the LoadRunner Enterprise Server Configuration Wizard. .For details, see "Configure a LoadRunner Enterprise server or host" on page 51.
>
>   After configuration is complete, host attributes from previous versions are displayed in LoadRunner Enterprise Administration in the Host Details page and Assign/Manage Host Attributes.

This chapter includes:

Installation flow

This section describes the steps required to install LoadRunner Enterprise.

	Before beginning the actual installation procedure, check that you meet the prerequisite criteria for working with LoadRunner Enterprise. For details, see "Before you install" on page 10.
Project Migration Pre-Installation Considerations	If you plan to work with projects from an earlier version of LoadRunner Enterprise (formerly Performance Center), follow the "Project migration pre-installation activities" on page 40.
	Install the Database server. For details, see "Database prerequisites" on page 31 and "LoadRunner Enterprise configuration options" on page 102.
 Install and Configure LoadRunner Enterprise Servers and Hosts	1. Install and configure LoadRunner Enterprise servers and hosts. For details, see "Install and configure LoadRunner Enterprise servers and hosts" on page 47. 2. Configure LoadRunner Enterprise in LoadRunner Enterprise Administration. For details, see "Post-installation configuration steps" on page 73.

Install Standalone Components	• Install standalone applications that provide advanced features for working with LoadRunner Enterprise. For details, see "Install standalone components (Windows)" on page 84. • To install a load generator on Linux, see "Install Load Generator on Linux" on page 87. • To install the load generator through a Docker container, see "Deploy Dockerized load generators on Linux" on page 88 / "Deploy Dockerized load generators on Windows" on page 93.
Perform Additional Tuning and Configuration	• Perform additional tuning and configuration settings to get the most out of LoadRunner Enterprise. For details, see "LoadRunner Enterprise configuration options" on page 102. • You can set LoadRunner Enterprise to run Vusers and monitor servers over a firewall. For details, see "Working with firewalls" on page 121.
Verify Installation	• Perform a post-installation verification. For details, see "Post installation verification" on page 100. • For installation troubleshooting details, see "Troubleshooting installation issues" on page 153.
Migrate Projects	After the installation is successful, you can migrate existing projects from LoadRunner Enterprise 12.6x (ALM 12.60) to LoadRunner Enterprise. You migrate projects from LoadRunner Enterprise Administration. For details, see Migrate projects to LoadRunner Enterprise in the LoadRunner Enterprise Help Center.

Upgrade LoadRunner Enterprise

LoadRunner Enterprise versions 2021 and later are full installations that can be installed over any LoadRunner Enterprise 2020 or later installation.

To upgrade all components in your installation, follow the installation process as described in "Install and configure LoadRunner Enterprise servers and hosts" on the next page. The installation process detects the older version, and gives you the option to upgrade.

Note: For silent upgrade, see "Installing an upgrade in silent mode" on page 82.

Before upgrading to a later version

- We recommend creating a back up of your Site Admin and Lab DB schemas before you start to safeguard against any unexpected changes during the upgrade process. For details, see Back up projects in the LoadRunner Enterprise Help Center.
- If you are upgrading to a new version of LoadRunner Enterprise and you have more than one LoadRunner Enterprise server installed, you must perform the following on all LoadRunner Enterprise servers:
  a. Stop IIS and the LoadRunner Backend Service and the LoadRunner Alerts Service.
  b. Install the latest version of LoadRunner Enterprise. For details, see "Install and configure LoadRunner Enterprise servers and hosts" below.

Patch installation (for 2021 R1 only)

After installation of 2021 R1, you must install the relevant patch package on your LoadRunner Enterprise host machines:

- Full LoadRunner Enterprise host installation machines: Install LRP_2021_R1_Patch
- OneLG load generator machines:
  - Windows OS: OneLG_2021_R1_Patch
  - Linux OS: LinuxLG_2021_R1_Patch

Install and configure LoadRunner Enterprise servers and hosts

This section describes how to install and configure LoadRunner Enterprise servers and hosts.

- "Install a LoadRunner Enterprise server or host" on the next page
- "Configure a LoadRunner Enterprise server or host" on page 51

> **Note:**
>
> - Review the LoadRunner Enterprise installation flow before you begin the installation. For details, see "Installation flow" on page 45.
> - If you are upgrading from an earlier version of LoadRunner Enterprise, review the upgrade instructions in "Upgrade LoadRunner Enterprise" on the previous page.
> - If you are migrating 12.6x or earlier projects from Performance Center, follow the instructions in "Project migration pre-installation activities" on page 40.

Install a LoadRunner Enterprise server or host

1. **Launch the LoadRunner Enterprise installer.**

   Download the installer package, and run **setup.exe**.

2. **Select an installation option.**

   The setup program starts and displays the installation menu page.

   Select **LoadRunner Enterprise** or **LoadRunner Enterprise Host**.

   > **Note:** If a particular host machine is to be used as a load generator only, we recommend that you install the Standalone Load Generator because the installation requires less disk space, and it is less time-consuming to move the load generator's setup files (compared to the LoadRunner Enterprise Host). For details on installing the Standalone Load Generator, see "Install standalone components (Windows)" on page 84. To install a load generator on Linux, see "Install Load Generator on Linux" on page 87.

3. **If necessary, install prerequisite software.**

   Some prerequisite software must be installed on the machine before installing the LoadRunner Enterprise component. If any of the prerequisite software is not already installed on the machine, the prerequisite software dialog box opens.

   Click **OK** and follow the on-screen instructions to install the prerequisite software before continuing with the LoadRunner Enterprise component installation. You cannot continue with the LoadRunner Enterprise component installation unless all the prerequisite software is installed.

   For a full list of prerequisite software, see "LoadRunner Enterprise prerequisite software" on page 24.

   > **Note:**
   >
   > - If you are prompted to restart the machine after installing the prerequisite software, you must do so before continuing with the installation. After rebooting the machine, run **setup.exe** again to continue with the installation. If the installation continues from where it left off before rebooting, we recommend starting the setup again—the installer will detect the installed prerequisites and continue with the installation.
   > - When installing a LoadRunner Enterprise server, if Microsoft Internet Information Services (IIS) 8.0/8.5/10 is listed on this page, it is required that you close the installation, install IIS, and restart the installation.

4. **If an earlier version is installed on your machine.**

   The installation process detects the older version, and gives you the option to upgrade or exit the installation.

5. **Start the installation.**

- For LoadRunner Enterprise Server: The LoadRunner Enterprise Setup Wizard opens, displaying the Welcome page. Click **Next**.
- For LoadRunner Enterprise Host: The LoadRunner Setup Wizard opens, displaying the Welcome page. Select **LoadRunner Enterprise Host**, and click **Next**.

6. **Review the License agreement.**

   To accept the terms of the license agreement, select **I accept the terms in the License Agreement**.

   For LoadRunner Enterprise Host only:

   - If you plan to integrate LoadRunner Enterprise with Silk Performer, select **Install Silk Agent after installation**. For details, see Silk Performer scripts in the LoadRunner Enterprise Help Center.
   - To help us improve the quality, reliability, and performance of LoadRunner Enterprise, select **Participate in LoadRunner improvement program**. This enables us to collect anonymous information about your software and hardware configuration, and about how you use LoadRunner Enterprise. Click **More Details** in the user interface for more information.

   > **Caution:** Participating in the improvement program creates unnecessary overhead on the host machine and is not recommended.

   Click **Next**.

7. **Select a destination folder.**

   Specify the location in which to install the LoadRunner Enterprise component. By default, LoadRunner Enterprise is installed to `C:\Program Files (x86)\Micro Focus\LoadRunner Enterprise\`.
   To choose a different location, enter the location or click the **Change** button, select a location, and click **OK**.

   > **Note:**
   >
   > - When upgrading from LoadRunner Enterprise 2020 SP2 or SP3, the location field is read-only.
   > - (LoadRunner Enterprise Host only). To reduce problems due to the Microsoft Windows API path limitation, choose a short name for your installation directory path. For example: "`C:\LREHost`".

   Click **Next**.

8. **Start the installation process.**

   The wizard prompts you to confirm the details and start the installation. To review or change any settings, click **Back**.

   Click **Install** to start the installation. The wizard displays the installation progress.

   Upon completion of the LoadRunner Enterprise installation, click **Next**, and continue with the steps in the Configuration wizard as described below.

9. **Upon completion of the installation, determine whether to install Network Virtualization (NV).**

   Upon completion of the installation, the **Finish** page opens.

   To view the installation log files, click the **Open Installation Log** link. The files are also available on the LoadRunner Enterprise server or host from **<installation folder>\orchidtmp\Configuration\configurationWizardLog_pcs.txt**.

   To install NV, choose one of the below options, or click **Do not install** to skip NV installation (you can install NV manually at a later time).

   - **Typical.** Automatically launches a non-interactive NV installation, using the default NV settings.
   - **Custom.** Automatically launches an interactive NV installation, enabling you to set the installation folder, data folder, and port to be used, and select which NV components to install.

   > **Note:**
   >
   > - The LoadRunner Enterprise installation is complete, regardless of the selected NV installation option.
   > - If you are installing NV on a LoadRunner Enterprise server, the NV for LoadRunner Enterprise installation will be launched.
   > - If you are installing NV on a LoadRunner Enterprise host, both the NV for Controller and the NV for Load Generator installations will be launched (one after the other).
   > - If you choose to install NV automatically, you must disable Windows SmartScreen before proceeding with the NV installation. To do so, open HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer in the Registry Editor, and change the Value data for "SmartScreenEnabled" to "Off". You do not need to disable SmartScreen when installing NV manually.
   > - Upgrading from Performance Center 12.6x to LoadRunner Enterprise 2021.x (for LoadRunner Enterprise host only): If NV for Controller and NV for Load Generator co-exist on the machine, and you select Custom mode installation, then you are unable to modify Setup configuration settings.
   >   **Resolution:** Exit the wizard and uninstall the NV components. Then reinstall them by manually running the NV installation. See the installation section in the Network Virtualization for LoadRunner Help.
   > - The NV installation log files are available from **C:\Temp\NV_Logs**.

   Upon completion of the LoadRunner Enterprise installation (and NV installation if selected), click **Next**, and continue with the steps in the Configuration wizard as described below.

Configure a LoadRunner Enterprise server or host

1. **Prerequisite (LoadRunner Enterprise 2021 R2 only).**

   If you plan configuring the LoadRunner Enterprise server and IIS to work with a secure (SSL) connection, we recommend making sure that a server certificate has been imported and a corresponding HTTPS binding is created for the site before running the Configuration Wizard.

2. **Start the LoadRunner Enterprise configuration.**

   After completing the LoadRunner Enterprise installation, click **Next**. The Welcome page of the Configuration wizard opens.

   Click **Next** to start the configuration process.

3. **Create the LoadRunner Enterprise service user (LoadRunner Enterprise server only).**

   LoadRunner Enterprise requires that a system user is created for use by the LoadRunner Enterprise server, hosts and the Load Generator standalone machines.

   a. In the **LRE Service User** page, specify a user to run the service.

      - If you select **Use Default Credentials**, LoadRunner Enterprise is configured with the LoadRunner Enterprise system user, IUSR_METRO, and adds it to the machine's Administrators group.
      - To define your own system user for the LoadRunner Enterprise environment, clear the **Use Default Credentials** check box, and enter the domain, user, and password. Enter credentials using one of the following formats: domain\username or username@domain.

      > **Note:**
      >
      > - You can use a local or a domain user. When using a local user, if the user does not exist on the LoadRunner Enterprise server machine, the installer will create it.
      > - When using a local user, if the user name does not exist or is not in the Administrators group, it will be added to the Administrators group.
      > - When using a domain user, make sure that the domain user is a member of the Administrators group.
      > - You must have a domain user set in the Configuration wizard when setting the repository path to a network location.
      > - The LRE Service user you set here must have permissions for the file repository (see Configure the repository).
      > - After adding the LoadRunner Enterprise server to the project, the LoadRunner Enterprise user will be saved to that database. Each subsequent LoadRunner Enterprise server or host added, will be configured with that user.
      > - After a LoadRunner Enterprise server is added, you can use the System Identity utility (**<LRE server installation directory>/bin/IdentityChangerUtil.exe**) to change the user. For details, see the System Identity Utility Window in the LoadRunner

> Enterprise Help Center.
>
> - Once you succeed in creating the user and configuring the server, the next time you launch the Configuration wizard, this page will not be displayed.

b. Click **Next**.

4. **Configure the repository.**

a. In the **Repository** page, click the **Browse** button to navigate to, or enter the path of the new LoadRunner Enterprise repository.

> **Note:**
>
> - Make sure you select a path where you have full read and write permissions.
> - The user account that was set in the **LRE Service User** page must have permissions for the file repository (see Create the LRE Service User).
> - To work with cluster nodes, make sure that all nodes have access to the file repository path and that the path is UNC. All nodes in the cluster must have the same string for the repository path.
> - The length of the file repository path cannot exceed 200 characters.
> - The file repository path cannot reside on the root folder.
> - Due to a Windows limitation, the file repository path cannot be on a mapped drive.

b. Click **Test Connection** to check whether you can connect to the repository using the user credentials you provided.

c. Click **Next**.

5. **Configure the connection to the LoadRunner Enterprise database server.**

a. In the **DB Connection** page, select the database type to be used in your LoadRunner Enterprise system: Oracle, Microsoft SQL, or PostgreSQL (supported for on-premises versions only).

b. Enter a name for the database server.

c. If you select a Microsoft SQL Server, choose the authentication type: SQL Authentication or Windows Authentication.

MS-SQL (SQL Auth)	Authenticates the user to the database using a database user name and password.
MS-SQL (Windows Auth)	Windows authentication relies on the user being authenticated by the operating system.

d. Configure the database administrator and user credentials:

Database Administrator Credentials	For MS-SQL: ◦ SQL Authentication: Enter the name and password of an admin database user with "dbcreator" level permissions required to install LoadRunner Enterprise on the database server. ◦ Windows Authentication: Read-only field which displays the name and password of the domain user used for the LoadRunner Enterprise installation. **Note:** This authentication mode is only supported if LoadRunner Enterprise is configured with a domain user. If it is configured with a local user, such as IUSR_METRO, only SQL Authentication will be available. For Oracle: ◦ Enter the name and password of the user with the administrative permissions required to install LoadRunner Enterprise on the database server. For PostgreSQL: ◦ Enter the name and password of a PostgreSQL superuser with "Create Database" and "CreateRole" permissions on the database server.
Database User Credentials	For SQL Authentication: ◦ Enter the name and password of a user with "public" level privileges to be used by LoadRunner Enterprise to connect to the database after the installation is complete. For Oracle: ◦ Set the default password for the new database users.

> **Note:** You can change the database administrator and user credentials at any time from the Database Password Changer utility. For details, see "Change the database administrator and user passwords" on page 75.

e. In the **Connection Details** section, select one of the following options:

- **Connection string parameters.** Select this option to enter database server information using the following fields:

Server Host	MS-SQL only: Enter the database server name. For example, **dbsrv01**. Oracle: This field is read-only. PostgreSQL: The PostgreSQL server address.

Port	MS-SQL only: Enter the database server port number, or accept the default port number. Oracle only: This field is read-only. PostgreSQL: Enter the port on which the PostgreSQL server is listening, or leave empty to use the default port (5432).
Net Service Name	Oracle only: Enter the net service name found in the local **tnsnames.ora** file. **Note:** The Oracle net service name must be in the same case as it appears in the **tnsnames.ora** file.

- **Connection string.** Select this option to manually edit the database server connection string, and provide the net service name from the local **tnsnames.ora** file.

f. Click **Test Connection** to check whether you can connect to the database server using the user credentials you provided.

g. Click **Next**.

6. **Configure the database schema.**

a. In the **DB Schema Configuration** page, enter a schema name for the Site Management database, the Site Admin database, and the LAB database.

> **Note:** The Site Management schema is created regardless of whether you are using a single or multi-tenant system.

b. If you are creating a PostgreSQL project, type the password to be used when creating the new logins which are part of the database creation process.

c. If you are creating an Oracle project, enter the following:

Tablespace	Select or type the path to a storage location that has sufficient space to store the new project. You should not use **UNDO** as the storage location.
Temporary Tablespace	Select or type the path to a temporary storage location that has sufficient space to store the new project.

d. Click **Next**.

7. **Configure security settings.**

a. Confidential data encryption

In the **Security Settings** page, enter a confidential data passphrase that LoadRunner Enterprise uses to encrypt the information. Passwords for accessing external systems (databases and LDAP) are stored by LoadRunner Enterprise after encryption. The passphrase is case-sensitive, and must contain at least 12 alphanumeric characters only.

We recommend making a note of the passphrase for future usage. If you are installing LoadRunner Enterprise on a cluster, you must use the same passphrase for all nodes.

> **Note:**
>
> - After completing the server configuration wizard, you cannot change the confidential data encryption passphrase.
> - Make sure there are no empty spaces before or after the passphrase.

b. Communication security

Enter a secure communication passphrase that LoadRunner Enterprise uses to encrypt the SSO token. Communication between LoadRunner Enterprise and other Micro Focus applications is enabled after authentication by a Single Sign-On (SSO) token.

The passphrase must contain at least 12 alphanumeric characters only.

c. Click **Next**.

8. **Configure the LoadRunner Enterprise server and IIS for SSL (available in LoadRunner Enterprise 2021 R2 and later).**

When you configure a LoadRunner Enterprise server, you can choose whether to work with a non-secure (HTTP) or a secure (SSL) connection. When you use the SSL option during server installation, a self-signed SSL certificate is automatically generated on the local LoadRunner Enterprise machine and the IIS server. Alternatively, you can import a certificate from a certified authority (CA).

> **Note:** If you intend to use the LoadRunner Enterprise server with a secure connection, make sure you have configured IIS to use SSL on the LoadRunner Enterprise server machine (you can also configure LoadRunner Enterprise to work with SSL post-installation). For details, see "Configuring LoadRunner Enterprise to work with TLS (SSL)" on page 103.

a. In the **SSL Configuration** page, select **Configure SSL for LoadRunner Enterprise** to use a secure connection.

If you are using a non-secure (HTTP) connection, clear this option and click **Next** to proceed to the next step.

b. From the **Certificate store** list, select the name of the provider that stores the certificate.

c. Select the server-side certificate file that is to be used on the listening port during an SSL handshake. You can import a certificate, or use an existing certificate.

Import a certificate	i. To import a certificate from a certified authority, select the **Import certificate** check box, and choose a certificate file (it must be in .pfx format). ii. Enter the password used to access the certificate file. iii. Enter the host name and port of the LoadRunner Enterprise server used by the agent.
Use existing certificate	i. To use an existing certificate, clear the **Import certificate** check box, and select a certificate from the **Existing certificates** list. ii. Enter the host name and port of the LoadRunner Enterprise server used by the agent.

d. Click **Next**.

9. **Define the site administrator.**

   Enter a user name and password for a site administrator. These credentials are used to create a user to log in to both LoadRunner Enterprise Administration and the Site Management console for the first time (these are two separate users, and updating one does not have any effect on the other).

   After installation, you can change the site administrator or add other site administrators.

   a. In the **LRE Administration User** page, enter a site administrator user name and password, and retype the password to confirm.

   > **Note:**
   >
   > - The user name cannot include the following characters: \ / : * ? " < > |
   > - The password cannot be longer than 20 characters.
   > - It is important that you keep a record of these credentials because you will need them to initially access LoadRunner Enterprise Administration, the Site Management console, and the System Identity Changer utility.

   b. Select a secret question for resetting the password and enter an answer.

   c. Click **Next**.

10. **Configure the mail server.**

    A mail server enables LoadRunner Enterprise users to send emails to other users in a project.

    a. In the **Mail Server Configuration** page, select **Configure Mail Server** if you plan to use a mail server. Otherwise, click **Next** and proceed to the next step.

b. Select which server to use and complete the SMTP account settings:

UI Element	Description
Address	The user's email address.
Outgoing mail server (SMTP)	The SMTP server available on your local area network.
Port	The port number used by the outgoing mail server. By default, port 25.
Use the following type of encrypted connection	Choose whether to make your connection more secure. The following options are available: `SSL` and `Start TLS`. **Note:** `SSL/TLS` is currently not supported.
Outgoing server (SMTP) requires authentication	If your SMTP server requires authentication, select this option to provide credentials for authentication. Enter the user name and password.
Send Test Email	Opens the Test Mail dialog box. Type an email address and click **Send**. A message box confirms whether the mail was sent successfully.

c. Click **Next**.

11. **Configure Site Admin and LAB schema migration.**

> **Note:** If you are creating a PostgreSQL project, proceed to the Summary step (the Migration Configuration step is not displayed).

To work with projects from a previous version of LoadRunner Enterprise (in which the projects were stored in ALM), you need to migrate data from the Site Admin and LAB schemas to LoadRunner Enterprise.

a. In the **Migration Configuration** page, select **Migrate Site Admin and LAB data and configuration** to perform the migration during the installation process.

Otherwise, click **Next** and proceed to the next step.

> **Note:**
>
> - This option is disabled if the Site Admin or LAB schemas already exist in LoadRunner Enterprise.
> - You can also migrate Site Admin and LAB configuration data post-installation from the Configuration wizard, provided you specify a new Site Admin and LAB

> schema for LoadRunner Enterprise (if you use the existing schemas nothing will happen).

b. In the **Migration Configuration (Step)** section, enter the names of the source Site Admin and LAB database schemas.

c. Select the source database type: MS-SQL (SQL Authentication), MS-SQL (Windows Authentication), or Oracle.

d. Configure the source database schema credentials:

User Name
(Oracle and MS-SQL (SQL Auth) only)
	The name of the user with the permissions required to access LoadRunner Enterprise on the database server. Note that this is not the database admin user.
	Note:
	○ For MS-SQL (Win Auth), the Windows user running the LoadRunner Enterprise Backend Service is used to access the SQL server.
	○ For MS-SQL (SQL Auth):
	• The login supplied to authenticate to the SQL server should be mapped to the ‘td’ user of the database. If you are using the same SQL server used by ALM, the ‘td’ user that is present in each database is by default mapped to the ‘td’ login, and this ‘td’ login can be supplied to perform the migration.
	• If you backed up and restored the database of the project in another SQL server, make sure you map the login supplied to perform the migration to the ‘td’ user of the database. For example, run the following SQL command:
	`--Map database user td to login John for database DEFAULT_PCPROJECT_DB USE DEFAULT_PCPROJECT_DB;`
	`GO`
	`EXEC sp_change_users_login 'Update_One', 'td', 'John';`
	`GO`

Password (Oracle and MS-SQL (SQL Auth) only)	The password of a user with the permissions required to access LoadRunner Enterprise on the database server; this is not retrieved from ALM. For Oracle: Enter the source ALM/PC12.6x Site Admin or LAB_PROJECT schema's (Oracle user) password. For MS-SQL (SQL Auth): Password for the ‘td’ user with at least read permissions, or the login mapped to the ‘td’ user of the database.

> **Note:** For the database migration, if the ALM Site Admin and LAB databases were created using SQL Authentication, you should also use SQL Authentication in the migration configuration; if ALM used Windows Authentication then you should use Windows Authentication for migration configuration.

e. In the **Connection Details** section, select one of the following options:

- **Connection String Parameters.** Select this option to enter database server information using the following fields:

Server Host	(MS-SQL only) Type the database server name. For example, **dbsrv01**.
Port	(MS-SQL only) Type the database server port number, or accept the default port number.
Net Service Name	(Oracle only) Enter the net service name found in the local **tnsnames.ora** file.

- **Connection string.** Select this option to manually edit the database server connection string, and provide the net service name from the local **tnsnames.ora** file.

f. Click **Test Connection** to check whether you can connect to the database server using the user credentials you provided.

g. Click **Next**.

12. **Check the configuration summary.**

    The **Summary** page opens, and displays the configuration settings you selected. Review and confirm the details.

    To change any settings, click **Edit** in the relevant section to open the corresponding page in the wizard, and make the necessary changes.

    Click **Start Configuration** to start the configuration.

    > **Note:** Make sure the Windows Services Manager is closed when running the configuration.

13. **Database schema creation or upgrade.**

    After the configuration process is completed successfully, the **DB Schema Creation** page opens, and displays the progress of the database schema creation.

    > **Note:** The **DB Schema Creation** or **DB Schema Upgrade** page opens, displaying the progress of the database schema creation or upgrade (depending on whether you are creating the DB schema when migrating projects from ALM, or upgrading the DB schema for existing LoadRunner Enterprise projects).

14. **The background configuration starts.**

After the DB schema has been created or upgraded, the **Configuration Process** page opens, and displays the progress bar as it performs the configurations on the relevant component.

The wizard performs the following configurations on the relevant component:

Configuration	**LoadRunner Enterprise Server**	**LoadRunner Enterprise Host**
Copies and updates configuration files.	Yes	Yes
Creates the LoadRunner Enterprise system user For information about changing the system user, see Change the LoadRunner Enterprise system user system user in the LoadRunner Enterprise Help Center.	Yes	No (The user is created when adding a host to LoadRunner Enterprise Administration)
Configures DCOM objects.	No (the DCOM objects are configured when adding a server to LoadRunner Enterprise Administration)	No (the DCOM objects are configured when adding a host to LoadRunner Enterprise Administration)
Installs LoadRunner Enterprise services: • LoadRunner Data Collection Agent • LoadRunner Remote Management Agent Service • LoadRunner Alerts Service (available in LoadRunner Enterprise • LoadRunner Backend Service **Note:** For details on how to reconfigure the port used by the LoadRunner Data Collection Agent service, see Software Self-solve knowledge base article KM01526547.	Yes	Yes (except for LoadRunner Alerts Service and LoadRunner Backend Service)
Installs LoadRunner Enterprise services: • LoadRunner Agent Service • LoadRunner Data Service • LoadRunner Load Testing Service • LoadRunner Analytics Service **Note:** If you stop the LoadRunner Analytics Service, the test will still run but there will be no online or offline results available. You can still collate and analyze results.	--	Yes

Configuration	LoadRunner Enterprise Server	LoadRunner Enterprise Host
Configures IIS: • Creates virtual directories and application pools. • Configures IIS application pools to work as 32-bit application pools. • Sets the .NET version for the application pools to .NET 4 (v4.0.30319). • Sets Integrated mode for the application pools. • Sets read and write permissions for the Modules feature. • Updates Mime type list. • Updates IIS Feature Delegation. **IIS 8.0/8.5/10:** • Add rules: IIS-ASP, IIS-ASPNET, IIS-ASPNET45, IIS-ManagementConsole, IIS-Metabase, IIS-IIS6ManagementCompatibility, IIS-StaticConten, IIS-HttpCompressionDynamic. • Disables rules: IIS-URLAuthorization **Note:** If the configuration is stuck in the "Updating IIS installation" stage (at about 40% progress) for more than 15 minutes, there might be a lock conflict if Windows Update is running in parallel, and we recommend that you cancel and restart the configuration.	Yes	--

15. **Complete the configuration.**

    Upon completion of schema creation, the **Finish** page opens.

    To view the configuration log files click the **Open Configuration Log** link. The files are also available on the LoadRunner Enterprise server or host from **<installation folder>\orchidtmp\Configuration\configurationWizardLog_pcs.txt**.

    Click **Finish** to exit the Configuration wizard.

16. **Perform additional required LoadRunner Enterprise configuration steps.**

    For details, see "Post-installation configuration steps" on page 73.

Note: After installing and configuring LoadRunner Enterprise, you need to restart the virtual machine on which the LoadRunner Enterprise server is installed.

Secure communication and system user

During installation of the LoadRunner Enterprise servers and hosts, a Communication Security passphrase is defined which enables secure communication between the LoadRunner Enterprise components. LoadRunner Enterprise also creates a default system user for use by the LoadRunner Enterprise server and hosts, the Site Management console, and the Load Generator standalone machines.

Update the Communication Security passphrase

This task describes how to update the Communication Security passphrase on the LoadRunner Enterprise system components. The Communication Security passphrase must be identical on all of the components of the system.

1. From the LoadRunner Enterprise server installation's bin directory, open the System Identity Changer Utility (**<LRE server installation directory>\bin\IdentityChangerUtil.exe**).

   > **Note:** You can run this utility from any one of the LoadRunner Enterprise servers in the system.

2. The System Identity Changer Utility opens. For user interface details, see "System Identity Changer Utility" on page 64.

   In the **Communication Security Passphrase** section, select **Change**, and enter the new Communication Security passphrase.

3. Click **Apply**.

   After the Communication Security passphrase has been successfully updated on the LoadRunner Enterprise components, you must reset IIS and restart the LoadRunner Backend Service and the LoadRunner Alerts Service on the LoadRunner Enterprise servers.

Change the LoadRunner Enterprise system user

During installation of the server and hosts, a default LoadRunner Enterprise system user, **IUSR_METRO** (default password **P3rfoRm@1nceCen1er**), is created in the Administrators user group of the server/host machines.

The LoadRunner Enterprise server is installed with the System Identity Changer Utility that enables you to manage the LoadRunner Enterprise system user on the LoadRunner Enterprise server and hosts from one centralized location. Use this utility to update the LoadRunner Enterprise system user name and password.

> **Note:** To prevent security breaches, you can replace LoadRunner Enterprise's default system user by creating a different local system user, or by using a domain user.

When you change the system user, or a user's password, the System Identity Changer Utility updates the LoadRunner Enterprise components.

To change the system user:

1. Prerequisites
   - When changing the system user, LoadRunner Enterprise must be down. That is, all users must be logged off the system and no tests may be running.
   - When changing the user password:
     - Ensure that each host is listed in the Machines table under **one alias only**.
     - In the case of a domain user, when the domain IT team notifies you that the password is to be changed, you need to temporarily change the LoadRunner Enterprise system user on the LoadRunner Enterprise server and hosts to a different user. After the domain IT team has changed the password of the domain user and has notified you of this change, you need to change the LoadRunner Enterprise system user back to the domain user on the LoadRunner Enterprise server and hosts.

   > **Note:** This utility does not apply changes to UNIX machines, Standalone load generators, or machines that are located over the firewall.

2. Launch the System Identity Changer Utility on the LoadRunner Enterprise server

   In the LoadRunner Enterprise server installation's **bin** directory, open the System Identity Changer Utility (**<LRE server installation directory>\bin\IdentityChangerUtil.exe**).

   The System Identity Changer Utility opens. For user interface details, see "System Identity Changer Utility" on the next page.

3. Change the details of the LoadRunner Enterprise user
   a. Enter the relevant details to update and click **Apply**.
   b. In the lower part of the utility window, the **Machines** table displays the status of each machine during the configuration process.
   c. The utility performs steps in the following order:
      i. LoadRunner Enterprise hosts are reconfigured first. Any failures at this phase won't stop the process from continuing.
      ii. If you are using a cluster environment with multiple LoadRunner Enterprise servers, all LoadRunner Enterprise servers except for the one from which the utility is running are reconfigured. Any failures at this phase won't stop the process from continuing.
      iii. The LoadRunner Enterprise server from which the utility is running is reconfigured. Failure at this level is critical, and will prevent the process from continuing.
      iv. The configuration shared by all LoadRunner Enterprise environments is updated. This step is dependent on the previous step succeeding.
   d. The utility attempts to configure all the hosts, even if the configuration on one or more hosts is unsuccessful. In this case, after the utility has attempted to configure all the hosts, correct the errors on the failed hosts, and click **Reconfigure**. The utility runs again on the whole

system.

For details on troubleshooting System Identity Changer Utility issues, see "Troubleshooting System Identity Changer Utility and system user issues" on page 68.

4. Verify that the system user was changed on the LoadRunner Enterprise server
   a. Open IIS Manager. Under **Sites > Default Web Site**, choose a virtual directory.
   b. Under **Authentication** select **Anonymous Authentication**. Verify that the anonymous user defined was changed for the following virtual directories: **PCS**, **LoadTest** and **Files** (a virtual directory in LoadTest).
   c. Check in the **PCQCWSAppPool** and **LoadTestAppPool** application pools that the identity is the LoadRunner Enterprise user.

System Identity Changer Utility

This utility enables you to update the LoadRunner Enterprise Communication Security passphrase, as well as the LoadRunner Enterprise system user and/or password on the LoadRunner Enterprise server, hosts, and Site Management console from one centralized location.

You can open the System Identity Changer Utility from **<LRE server installation directory>\bin\IdentityChangerUtil.exe**.

> **Note:**
>
> - When using the System Identity Changer Utility, you should always authenticate with internal authentication using the initial admin user and password provided during LoadRunner Enterprise configuration, no matter which authentication type is in use.
> - For a single tenant environment: Only a Site Admin user can log into the System Identity Changer Utility.
> - For a multi-tenant environment: Only a Site Management user can log into the System Identity Changer Utility. For details, see Multi-tenancy in the LoadRunner Enterprise Help Center.

UI Elements	Description
	Applies the selected changes on the LoadRunner Enterprise server and hosts, starting with the LoadRunner Enterprise server.
	If, when applying a change, there are errors on any of the LoadRunner Enterprise hosts, troubleshoot the problematic host machines, then click **Reconfigure**. The utility runs again on the LoadRunner Enterprise server and hosts.

UI Elements	Description
LoadRunner Enterprise User	The LoadRunner Enterprise system user details. • **Change.** Enables you to select which detail to change. ◦ **None.** Do not change the user's name or password. ◦ **Password Only.** Enables you to change only the LoadRunner Enterprise system user's password. **Note:** See "Prerequisites" on page 63. ◦ **User.** Enables you to change the LoadRunner Enterprise system user name and password. • **Domain\Username.** The domain and user name of the LoadRunner Enterprise system user. • **Password/Confirm Password.** The password of the LoadRunner Enterprise system user. • **Delete Old User.** If you are changing the user, this option enables you to delete the previous user from the machine. **Note:** You cannot delete a domain user.
User Group	The details of the user group to which the LoadRunner Enterprise system user belongs. **Group type.** The type of user group. • **Administrator Group.** Creates a user in the Administrators group with full administrator policies and permissions. • **Other.** Creates a local group under the Users group, granting policies and permissions as well as other LoadRunner Enterprise permissions. **Note:** To configure LoadRunner Enterprise with a configuration user and a restricted user, you must specify a **Group type.** If the group type is not the **Administrator Group**, you must set the group with full permission over the LoadRunner Enterprise repository prior to applying the change from the System Identity Changer Utility. To do so: 1. On the LoadRunner Enterprise server(s), navigate to the LoadRunner Enterprise repository. 2. Right-click the folder, and select **Properties**. 3. Select the **Security** tab. 4. Edit the "Group or user names" section. 5. Add the group you intend to use in the System Identity Change Utility. 6. Allow this group to have **Full control** and apply the change.

UI Elements	Description
Configuration User	If you are creating a non-administrative LoadRunner Enterprise system user, that is, if you selected **Other** under **User Group**, you need to configure a configuration user (a system user with administrative privileges) that the non-administrative LoadRunner Enterprise system user can impersonate when it needs to perform administrative tasks. For details, refer to "Change the LoadRunner Enterprise system user" on page 62. If you selected **Delete Old User** in the **LoadRunner Enterprise User** area, ensure that the configuration user you are configuring is not the same as the system user you are deleting. Alternatively, do not delete the old user. • **Domain\Username.** The domain and user name of a system user that has administrator privileges on the LoadRunner Enterprise server and hosts. • **Password/Confirm Password.** The password of a system user that has administrator privileges on the LoadRunner Enterprise server and hosts.
Communication Security Passphrase	The Communication Security passphrase that enables the LoadRunner Enterprise servers and hosts to communicate securely. • **Change.** Enables you to change the passphrase. • **New passphrase.** The new Communication Security passphrase. **Note:** This passphrase must be identical on all LoadRunner Enterprise components. For details, refer to the "Update the Communication Security passphrase" on page 62.
Machines grid	The machine configuration settings: • **Type.** Indicates whether the machine type is a LoadRunner Enterprise server or a host. • **Name.** The machine name. • **Configuration Status.** Displays the configuration status on each of the LoadRunner Enterprise components. • **Configuration complete.** The system user configuration was completed. • **Needs to be configured.** The LoadRunner Enterprise server/host is pending configuration. Displayed only after the LoadRunner Enterprise server configuration is complete. • **Configuring.....** The LoadRunner Enterprise server/host is being configured. • **Configuration failed.** The LoadRunner Enterprise server/host configuration failed. The utility displays the reason for failure together with this status. **Note:** See "Change the details of the LoadRunner Enterprise user" on page 63.

Administer a LoadRunner Enterprise server and host remotely

To perform administrative tasks on the LoadRunner Enterprise server or hosts (such as adding, configuring, or resetting a LoadRunner Enterprise server/host), LoadRunner Enterprise must use a user with administrative privileges. This must be the LoadRunner Enterprise system user with administrative privileges or, if the LoadRunner Enterprise system user is non-administrative, a configuration user.

When the LoadRunner Enterprise system user has administrative privileges and is defined on the remote machine, tasks are performed upon request. After validating the LoadRunner Enterprise system user or configuration user, LoadRunner Enterprise can perform required tasks.

Configure a non-administrator LoadRunner Enterprise system user

For stronger security, you can configure the LoadRunner Enterprise system to use a non-administrator user and a custom group (lockdown mode).

This system user has the same permissions granted to any user in the built-in 'Users' group with additional extended rights to Web services and the Micro Focus file system and registry as described below:

- Granted all the privileges described in "Required policies for the LoadRunner Enterprise system user" on the next page.
- Added to the built-in system groups **Performance Log Users** and **IIS_IUSRS** (on LoadRunner Enterprise server only).
- The custom group is added to the built-in system groups **Distributed COM Users** and **Users**.

With the above-mentioned permissions, a system user cannot perform all of the administrative system tasks. Therefore, when configuring the system to use non-administrator user, you will need to specify a configuration user (a user with administrative privileges that is defined on the LoadRunner Enterprise server and hosts).

This configuration user will be used by LoadRunner Enterprise when administrative tasks are required by system. For example, tasks for changing a system user, resetting IIS, restarting services, accessing IIS metadata, configuring DCOM.

After completing such tasks, the system user reverts back to the previous user with the limited LoadRunner Enterprise user permissions.

> **Note:** The configuration user is saved in the database, so that whenever an administrative-level system user is required to perform a task, the system automatically uses the configuration user, without prompting for the user's credentials.

Required policies for the LoadRunner Enterprise system user

This section describes the required policies LoadRunner Enterprise grants automatically to a system user.

> **Note:** This section applies to:
>
> - An administrative or non-administrative LoadRunner Enterprise user.
> - All LoadRunner Enterprise servers and hosts.

The LoadRunner Enterprise user must be granted all of the following policies:

Policy Name	Reason
Create global object (**SeCreateGlobalPrivilege**)	For Autolab running Vusers on the Controller.
Batch logon rights (**SeBatchLogonRight**)	The minimum policies required to run Web applications.
Service logon rights (**SeServiceLogonRight**)	The minimum policies required to run Web applications.
Access this computer from the network (**SeNetworkLogonRight**)	The minimum policies required to run Web applications.
Log on locally (**SeInteractiveLogonRight**)	Required by infra services. For example, after reboot, the system logs in with the LoadRunner Enterprise system user.
Impersonate a client after authentication (**SeImpersonatePrivilege**)	Required for running LoadRunner Enterprise processes under the LoadRunner Enterprise system user.

Troubleshooting System Identity Changer Utility and system user issues

This section provides information for troubleshooting issues related to the System Identity Changer Utility and the LoadRunner Enterprise system user.

Error running the Change Identity utility

Problem Description

When running **IdentityChangerUtil.exe**, you receive the following error: “Another instance is already running. Please switch to it.”

This is because there is another instance of the Change Identity utility already running.

Troubleshooting

- If you can see the other instance, you should use that one, or close it and then restart the utility.
- If you cannot see the other instance of the utility, it means that another user is running it on the same machine. Switch to the other user and close the utility before attempting to run it with a different username.

Unable to connect to the LoadRunner Enterprise Server

Problem Description

When entering the LoadRunner Enterprise site administrator credentials on the LoadRunner Enterprise server, the “Unable to connect to the LoadRunner Enterprise Server” error occurs

This error can be caused by a number of issues, including connectivity problems, security settings, or because the LoadRunner Enterprise server services are not up and running.

Troubleshooting

- Verify that the LoadRunner Enterprise Backend Service is up and running.
- Ensure Data Execution Prevention (DEP) is disabled on all LoadRunner Enterprise server and host machines.
- Ensure the Internet Explorer Enhanced Security Configuration setting is disabled on all LoadRunner Enterprise components.
- Ensure User Account Control (UAC) is disabled while logging in as the default LoadRunner Enterprise system user (**IUSR_METRO**).

Error changing the system user

The following are possible error messages you could encounter when trying to change the system user.

Error Message	Description	Troubleshooting
Can’t apply changes. Not all hosts are in idle state.	You receive this error because one or more of the hosts is currently busy with another operation.	1. Log in to LoadRunner Enterprise Administration and go to the Hosts module. Verify that all hosts are in the **Idle** state. 2. If all of the hosts are in the **Idle** state, make sure that any other hosts that belong to the host pool are not idle. 3. Open the System Identity Changer Utility again. For details, see "System Identity Changer Utility" on page 64.
Make sure you have entered a different username.	You receive this error because you are trying to change the user to the current username.	Choose a different username.

Error Message	**Description**	**Troubleshooting**
Configuration failed: Failed to find the Load Testing Service on <machine name>. Please verify that the service exists and that it is running.	This error might appear because the LoadRunner Load Testing Service isn't running, or because the SSO key is defined on the host.	• Select **Start > Run** and type `services.msc`. In the Services window, verify that the LoadRunner Load Testing Service is running. • Check that the SSO key which is defined on the host matches the SSO key defined on the LoadRunner Enterprise Server. You can check the SSO key in the following locations: ◦ On the LoadRunner Enterprise Server: **<LoadRunner Enterprise Server installation dir>\dat\PCS.config** ◦ On the host: **<LoadRunner Enterprise host installation dir>\dat\LTS.config** If the keys do not match, change the key in **LTS.config** file on the host. Then open the Services window and restart the LoadRunner Load Testing Service.

Error Message	Description	Troubleshooting
One of the following error messages appears: • Problem adding required policies • Problem adding user to group • Problem changing application pool identity • Problem changing COM settings • Problem changing IIS • Problem changing password • Problem changing PC Group • Problem creating group • Problem creating user • Problem deleting old identity • Problem removing user from Admin	You probably receive this error because the configuration user you provided does not have the required permissions to perform the requested operation.	Supply a configuration user which has administrator privileges on all the machines on which you are trying to change the user.

Unable to reconfigure hosts or the LoadRunner Enterprise Server

Problem Description

Unable to reconfigure hosts or the LoadRunner Enterprise Server from LoadRunner Enterprise Administration.

This occurs when the System Identity Utility failed to configure the LoadRunner Enterprise Server or hosts, and you have since closed the utility.

Troubleshooting

Perform the Change System User task again from the beginning. For details, see "Change the LoadRunner Enterprise system user" on page 62.

Denied access to the internal Influx database server

Problem Description

If you uninstall a host and reinstall it again, and during this time the LoadRunner Enterprise system user name or password is changed, access to the internal Influx database on the host will be denied.

This is because Influx stores its data in a folder that also includes the data of the previous authentication user. By default, the folder is under **<installation drive>\var** (the path is configurable under **<host installation>\bin\influxdb\influxdb.conf**).

Troubleshooting

You need to delete this folder in order for LoadRunner Enterprise to reconfigure the database with the new user. To avoid data loss when deleting this folder, we recommend changing the identity using the InfluxDB REST API.

Post-installation configuration steps

After running the LoadRunner Enterprise installation and Configuration wizard, you must perform additional configuration steps in LoadRunner Enterprise Administration before you can use the product.

This section includes:

- "Configure LoadRunner Enterprise servers and hosts post-installation" below
- "Log on to LoadRunner Enterprise Administration" below
- "Perform site and lab administration tasks" on the next page
- "Change the database administrator and user passwords" on page 75

Configure LoadRunner Enterprise servers and hosts post-installation

> **Note:** You can skip these steps if you configured LoadRunner Enterprise servers and hosts during the installation process.

While you can configure LoadRunner Enterprise servers and hosts during the installation process, you can also configure them post-installation from the Configuration wizard in the Start menu. To do so, you must run the wizard as an administrator.

1. Prerequisites

   Install LoadRunner Enterprise. For details, see "Install and configure LoadRunner Enterprise servers and hosts" on page 47.

2. Launch the **Server Configuration Wizard** or **Host Configuration Wizard** from the Start menu using the **Run as administrator** option.

   Alternatively, choose **Start > All Programs > Micro Focus > LoadRunner Enterprise Server/Host > Tools**, right-click **Server/Host Configuration Wizard**, and select **Run as administrator**.

   For details, see Configure a LoadRunner Enterprise server or host.

Log on to LoadRunner Enterprise Administration

LoadRunner Enterprise administration tasks are performed in LoadRunner Enterprise Administration.

To log in to LoadRunner Enterprise Administration:

1. Open your Web browser (Chrome, Internet Explorer, Edge, Firefox and Safari are supported) and type the LoadRunner Enterprise Administration URL in the following format:

   ```
   http://<LoadRunner_Enterprise_Server_name>/admin
   ```

   The LoadRunner Enterprise Administration Login window opens.
2. In the **User Name** box, type your user name. Only a Site or Tenant Admin user can log on to LoadRunner Enterprise Administration. For details, see About administrator users in the LoadRunner Enterprise Help Center.

   > **Note:** The first time you log in to LoadRunner Enterprise Administration, you must use the site administrator name that you specified during the installation of LoadRunner Enterprise (see page 56). After you log in to LoadRunner Enterprise Administration, you can define additional site administrators. For details, see Define a LoadRunner Enterprise site administrator in the LoadRunner Enterprise Help Center.

3. In the **Password** box, type the site administrator password.

   > **Note:** If you are logging in using your internal LoadRunner Enterprise password, you can reset the password by clicking **Forgot or want to change your password** (this is not applicable when using LDAP or SSO authentication).

4. Select the language for displaying the LoadRunner Enterprise user interface.

   The multilingual user interface, or MLU, provides support for multiple languages on a single instance of LoadRunner Enterprise without having to install language packs. Supported languages are English, French, Italian, Korean, German, Japanese, Russian, Simplified Chinese, and Spanish.
5. Click the **Login** button. LoadRunner Enterprise Administration opens.

Perform site and lab administration tasks

After installing LoadRunner Enterprise servers and hosts, you perform the site and lab administration tasks from LoadRunner Enterprise Administration.

1. **Log on to LoadRunner Enterprise Administration**

   For details, see "Log on to LoadRunner Enterprise Administration" on the previous page.
2. **Perform site configuration tasks**

   Configure the authentication method which allows users to log in to LoadRunner Enterprise, and define the project file repository.

   For details, see Select authentication type and Manage the project repository in the LoadRunner Enterprise Help Center.
3. **Create and maintain projects**

You can create and maintain projects, and define the limits and other settings for the project from **Management > Projects**.

For details, see Manage projects in the LoadRunner Enterprise Help Center.

4. **Create and manage users and user roles**

   You can create users and control access to a project by defining the users who can log in to the project, and by specifying the types of tasks (roles) each user may perform from **Management > Users**.

   For details, see Manage users in a project and Assign roles and permissions in the LoadRunner Enterprise Help Center.

5. **Add or reconfigure LoadRunner Enterprise hosts**

   To work with LoadRunner Enterprise hosts, you must first add them to LoadRunner Enterprise Administration and define the host's location. If the host is a load generator over a firewall, you must define the MI Listener through which the load generator communicates with the LoadRunner Enterprise server.

   When adding the hosts, the system configures the LoadRunner Enterprise user on that machine. For details, see Add a host in the LoadRunner Enterprise Help Center.

   > **Note for reconfiguring hosts after upgrading an existing LAB project:**
   >
   > If you upgrade an existing LAB Project (after uninstalling the previous version of LoadRunner Enterprise, and installing LoadRunner Enterprise 2021 or later on the hosts), LoadRunner Enterprise hosts are displayed in the **Unavailable** state, and you need to perform the following:
   >
   > a. In LoadRunner Enterprise Administration, select **Management > Hosts**.
   >
   > b. Select the hosts you want to reconfigure in the Hosts grid, and click **Reconfigure Host**.

6. **Run a system health check**

   After adding a LoadRunner Enterprise server to the system, and adding or reconfiguring LoadRunner Enterprise hosts, you should perform a system health check to make sure all components are running as expected.

   For details, see Perform a system health check in the LoadRunner Enterprise Help Center.

7. **Set the license keys**

   To run tests from LoadRunner Enterprise, you must install the appropriate LoadRunner Enterprise server and host licenses.

   For details, see Manage licenses in the LoadRunner Enterprise Help Center.

Change the database administrator and user passwords

You can change the DB Administrator and User passwords that you configured for the LoadRunner Enterprise server from the Database Passwords Changer utility in the Start menu.

1. Stop the LoadRunner Backend Service.
2. Change the DB Administrator and/or User passwords (according to the required change) on the database server.
3. Run the Database Passwords Changer utility from the start menu (**Start > All Programs > Micro Focus > Database Password Changer**), and enter the new password for the LoadRunner Enterprise DB Administrator and/or User.

   > **Note for Oracle databases only:** Changing the username password affects only the LRE_SITE_MANAGEMENT_DB and LRE_SITE_ADMIN_DB user's password.

   For more details on DB Administrator and User credentials, see the "Configure the connection to the LoadRunner Enterprise database server." on page 52
4. Upon successful completion of the utility, restart the LoadRunner Backend Service.

Install LoadRunner Enterprise silently

A **silent installation** is an installation that is performed automatically, without the need for user interaction. This section describes how to perform a silent installation of LoadRunner Enterprise components.

Before you perform the installation, review the pre-installation information, including the system requirements, described in "Before you install" on page 10.

This section includes:

- "Prerequisite software for silent installation" below
- "Customize silent installation" on page 78
- "Silently install LoadRunner Enterprise server and hosts" on page 80

Prerequisite software for silent installation

Install the prerequisite software silently by running the relevant commands as follows:

Prerequisite Software	Command
.NET Framework 4.8	`<Installation_Disk_Root_Directory>\Setup\Common\dotnet48\ndp48-x86-x64-allos-enu.exe /LCID /q /norestart /c:"install /q"` **Note:** .NET Framework 4.8 replaces the .NET Framework 4.6.2 and earlier files. If there are any applications that are using the .NET Framework 4.6.2 or earlier files and are running during the installation of .NET Framework 4.8, you may need to restart your machine. If you are prompted to restart the machine, restart it before continuing the installation. For details, see http://msdn.microsoft.com/en-us/library/hh527997%28v=vs.110%29.aspx.
.Net core hosting 3.1.3	`<Installation root directory\Setup\Common\dotnet_hosting\dotnet-hosting-<version_number>-win.exe /quiet OPT_NO_RUNTIME=1 OPT_NO_SHAREDFX=1 OPT_NO_X86=1`
Microsoft Visual C++ Redistributable for Visual Studio 2015-2019	`<Installation_Disk_Root_Directory>\Setup\Common\vc2015_2019_redist_x86\vc_redist.x86.exe /quiet /norestart`
Microsoft Visual C++ Redistributable for Visual Studio 2015-2019 (x64)	`<Installation_Disk_Root_Directory>\Setup\Common\vc2015_2019_redist_x86\vc_redist.x64.exe /quiet /norestart`
Windows Imaging Component (WIC)	`<Installation_Disk_Root_Directory>\Setup\Common\dotnet40\wic_x64_enu.exe /q /norestart`
Microsoft Data Access Components (MDAC) 2.8 SP1 (or later)	`<Installation_Disk_Root_Directory>\Setup\<environment>\prerequisites\mdac28\mdac28.exe /q:A /C:"setup /QNT"`

Prerequisite Software	Command
Microsoft Core XML Services (MSXML) 6.0	**For x64:** `msiexec /log c:\msxml.log /quiet /I <Installation_Disk_Root_Directory>\Common\msxml6\msxml6_x64.msi` **For ia64:** `msiexec /log c:\msxml.log /quiet /I <Installation_Disk_Root_Directory>\Common\msxml6\msxml6_ia64.msi`
Microsoft Windows Installer 3.1	`<Installation_Disk_Root_Directory>\Setup\Common\msi31\WindowsInstaller-KB893803-v2-x86.exe /q /norestart`
Internet Information Services (IIS)	See the Microsoft documentation for the PowerShell command required for your IIS version. **Note:** LoadRunner Enterprise Server only.

Customize silent installation

This section describes how to customize the file used for silent configuration of the LoadRunner Enterprise. The **UserInput.xml** file—installed with LoadRunner Enterprise—contains parameters for the LoadRunner Enterprise server and LoadRunner Enterprise host configurations.

You can customize the parameters in the **UserInput.xml** file. You then instruct the Installer to use the customized file for the silent configuration input.

To configure the properties in the UserInput.xml file:

1. Copy the **UserInput.xml** file from the LoadRunner Enterprise installation directory (**...\Setup\Install\[Host][Server]**) to another location.
2. Open the copy of the file and enter a user-defined value for the following property:

Property	Description
LW_CRYPTO_INIT_STRING	This passphrase must be identical to the passphrase defined during the installation.

3. **For LoadRunner Enterprise Server only:**

Property	Description
IIS_WEB_SITE_NAME	Choose the IIS web site that will be used to host the LoadRunner Enterprise server services. **Note:** • The web site must exists prior to running the configuration. • The value is optional. If no web site is specified and there is more than one defined on your machine, the configuration will use the first one (the one with the smallest ID value).
SystemUserName	Choose the name of the user that will be configured as the LoadRunner Enterprise Windows system user. **Note:** You can use a local or a domain user: • If you are using a local user, the user will be added to the Administrator group. • If you are using a domain user, the value for this property should be in the form of <domain\user>. Make sure the machine and the user are part of the same domain and that the user exists on the machine. • If you do not provide a user name, the system will use the default user name ('IUSR_METRO'). • A user name cannot include the following characters [ ] : | < + > = ; , ? * @ • If the supplied user's details are invalid (for example, the user name contains invalid characters, or the domain user does not exist), the system will use the default user name ('IUSR_METRO') instead. For details on defining a user, see "Install and configure LoadRunner Enterprise servers and hosts" on page 47.
SystemUserPwd	Choose the password for the LoadRunner Enterprise Windows system user. **Note:** • If the installer uses the default user (for example, when the value for property 'SystemUserName' is empty), the password property will be ignored and the installer will use the default password ('P3rfoRm@1nceCen1er'). • A password cannot include the following characters < > | & " ^ or space. • A password cannot be empty. If this field is left empty, the system will use the default password ('P3rfoRm@1nceCen1er'). • If using an existing user for the 'SystemUserName' property, the password must match the password used by the existing user.

4. **For LoadRunner Enterprise Host only:**

Property	Description
LRASPCHOST=1	Add this property to install LoadRunner as a LoadRunner Enterprise Host.
IMPROVEMENTPROGRAM=0	The option to participate in the VuGen improvement program is enabled by default. Add this property if you want to disable it. For details, see VuGen improvement program.

5. Save the **UserInput.xml** file.
6. Specify the location of the saved file when running the silent installation command.

Silently install LoadRunner Enterprise server and hosts

This section describes how to run the silent installation of the LoadRunner Enterprise server and LoadRunner Enterprise hosts on a Windows platform.

The silent installation is followed by the silent configuration which calls the **UserInput.xml** file for configuration parameters. You can customize the parameters in this file for the LoadRunner Enterprise server configuration. For details, see "Customize silent installation" on page 78.

You can perform a silent installation of LoadRunner Enterprise using one of the options below.

> **Note:** If you are installing Network Virtualization (NV), you must disable Windows SmartScreen before proceeding with the silent installation. To do so, open HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer in the Registry Editor, and change the Value data for "SmartScreenEnabled" to "Off".

Option 1: Install the prerequisite software and the LoadRunner Enterprise component

1. Install the prerequisite software. For details, see "Prerequisite software for silent installation" on page 76.

   > **Note:** If you are prompted to restart the computer after installing the prerequisite software, you must do so before continuing with the installation.

2. After you have installed all the prerequisite software, install the LoadRunner Enterprise component by running the appropriate command from the command line.

   LoadRunner Enterprise Server:

Silent installation with default properties	`msiexec /i <Installation_Disk_Root_Directory>\Setup\Install\Server\LRE_Server.msi`
	`INSTALLDIR="<Target Installation Directory>" NVINSTALL=Y /qnb /l*vx "<Path to log file>"`

Silent installation with customized UserInput.xml	`msiexec /i <Installation_Disk_Root_Directory>\Setup\Install\Server\LRE_Server.msi`
	`USER_CONFIG_FILE_PATH="<Full path to UserInput file>" INSTALLDIR="<Target Installation Directory>" NVINSTALL=Y /qnb /l*vx "<Path to log file>"`

Where **<Full path to UserInput file>** is the path to your customized UserInput.xml file, **<Target Installation Directory>** is the directory in which to install the LoadRunner Enterprise server, and **<Path to log file>** is full path to the installation log file.

NVINSTALL indicates whether to launch the NV installation in silent mode, once the LoadRunner Enterprise installation is done (by default, NV is not installed in silent mode).

> **Note:** Restarting the machine is required in order for NV to function properly.

LoadRunner Enterprise Host:

```
msiexec /i <Installation_Disk_Root_Directory>\Setup\Install\
Host\LoadRunner_x64.msi
USER_CONFIG_FILE_PATH="<Full path to UserInput file>" [optional
installer properties - see list below] /qn /l*vx "<Path to log file>"
```

Where **<Full path to UserInput file>** is the path to your customized UserInput.xml file, **<Target Installation Directory>** is the directory in which you want to install the LoadRunner Enterprise host, and **<Path to log file>** is full path to installation log file.

NVINSTALL indicates whether to launch the NV installation in silent mode, once the LoadRunner Enterprise installation is done (by default, NV is not installed in silent mode).

> **Note:** Restarting the machine is required in order for NV to function properly.

Option 2: Install the prerequisite softwares together with the LoadRunner Enterprise components

You can also install in silent mode using the **setup.exe** file from the LoadRunner Enterprise installation directory. This enables you to install the prerequisites in silent mode automatically before running the

MSI installation in silent mode. Using this option also invokes the correct MSI file depending on the operating system platform.

Server installation:

```
<Installation_Disk_Root_Directory>\Setup\En\setup_server.exe /s USER_
CONFIG_FILE_PATH="<Full path to UserInput file>" INSTALLDIR="<Target
Installation Directory>" NVINSTALL=Y
```

Host installation:

```
<Installation_Disk_Root_Directory>\Setup\En\setup_host.exe /s
INSTALLDIR="<Target Installation Directory>" USER_CONFIG_FILE_PATH="<Full
path to UserInput file>" NVINSTALL=Y
```

Where **<Full path to UserInput file>** is the path to your customized UserInput.xml file and **<Target Installation Directory>** is the directory in which to install the LoadRunner Enterprise server or host.

When using the **setup.exe** file, the installation log will be created under the user's temp directory.

Host installation:	%temp%\LREHost.log
Server installation:	%temp%\LREServer.log

Where **<Full path to UserInput file>** is the path to your customized UserInput.xml file, **<Target Installation Directory>** is the directory in which you want to install the LoadRunner Enterprise host, and **<Path to log file>** is full path to installation log file.

NVINSTALL indicates whether to launch the NV installation in silent mode, once the LoadRunner Enterprise installation is done (by default, NV is not installed in silent mode).

Note: Restarting the machine is required in order for NV to function properly.

Installing an upgrade in silent mode

If you are installing an upgrade, run the following command:

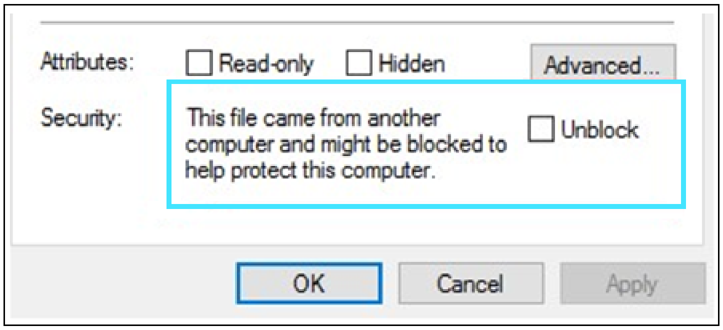
```
msiexec.exe /update <full path to msp file> [/qn] [/l*vx <full path to log file>]
```

The msp files are located in the installation package.

The **/qn** option sets the silent mode and **/l*vx** enables logging in verbosity mode.

Notes and limitations

If you attempt to download Network Virtualization installation files from the Internet or an FTP site, the files will be blocked to protect the computer from untrusted files and you will get the following message:



This file came from another computer and might be blocked to help protect this computer.

Resolution: Before installing NV, unblock the files as follows:

1. Right-click one of the NV installation executable files located in **<NV installation path>\Additional Components\Network Virtualization**, and select **Properties**.
2. If there is an **Unblock** check box in the **General** tab, select it and click **OK**.
3. Verify that the **Unblock** check box is gone.
4. Repeat for each executable file in the **Network Virtualization** folder.

Deploy LoadRunner Enterprise on AWS

LoadRunner Enterprise is certified to be installed and run under Amazon Web Services (AWS), using a BYOL (Bring Your Own License) model.

Requirements for deploying LoadRunner Enterprise on the cloud:

- All components of the cloud computing environment follow the system requirements specified in this document.
- The required ports are open for communication. For the required posts, see "Communication paths" on page 13.

> **Note:**
>
> - Cloud load generators can be provisioned using the built-in functionality of LoadRunner Enterprise. For details, see Manage Load Generators on the Cloud in the LoadRunner Professional Help Center and Provision cloud load generators in the LoadRunner Enterprise Help Center. All other components must be manually installed and configured by the user.
> - To improve performance, it is preferable to deploy the LoadRunner Enterprise server and hosts, and the database in the same region. Consult AWS for best practices about network performance.

- Cloud load generator ports are configurable. When all the components are in the cloud, the ports to use are defined by the cloud provider (they are not based on internal IT policies).

Install standalone components (Windows)

You can install standalone components that provide advanced features for working with LoadRunner Enterprise.

To install a load generator on Linux, see "Install Load Generator on Linux" on page 87.

Note: For all standalone applications, you must first manually install the prerequisite applications. For details, see "Prerequisite software for silent installation" on page 76

This section includes:

- "Available standalone components for Windows" below
- "Install standalone components" on the next page
- "Silently install standalone applications" on page 86

Available standalone components for Windows

The following standalone components are available. To install these components, see "Install standalone components" on the next page.

Component	Description
OneLG	Instead of installing a LoadRunner Enterprise Host and then configuring it as a load generator, you can install a standalone version of the load generator (OneLG). This host can behave only as a load generator, unlike the LoadRunner Enterprise host, which can also be configured as a Controller or data processor. You can use a local or a cloud-based machine to host your load generator. **Note:** If you know in advance that a particular host machine is to be used as a load generator only, we recommend that you install OneLG for the following reasons: • The installation requires less disk space • Moving the load generator's setup files is less time consuming than moving the setup files of the LoadRunner Enterprise Host.
Virtual User Generator	Virtual User Generator (VuGen) generates virtual users, or Vusers, by recording actions that typical end-users would perform on your application. VuGen records your actions into automated Vuser scripts which form the foundation of your performance tests.

Component	Description
LoadRunner Analysis	Analysis provides graphs and reports with in-depth performance analysis information. Using these graphs and reports, you can pinpoint and identify the bottlenecks in your application and determine what changes need to be made to your system in order to improve its performance.
TruClient	TruClient is a browser-based testing technology for creating test scripts that can then be used in performance testing or monitoring web applications. TruClient records your actions as you navigate through your business process. It creates a script from your actions—which you then run in performance testing.
MI Listener	The MI Listener is one of the components needed to run Vusers and monitor applications over a firewall. To install, run **SetupMIListener.exe**. For details about firewalls in LoadRunner Enterprise, see "Working with firewalls" on page 121.
Monitor Over Firewall Agent	Used to monitor servers that are located over a firewall. For details about firewalls in LoadRunner Enterprise, see "Working with firewalls" on page 121.

Install standalone components

This section describes the installation process for standalone components.

To install any of the standalone components:

1. From the LoadRunner Enterprise installation directory, run **setup.exe**. The setup program displays the installation menu page.
2. Select one of the following options: **OneLG**, **VuGen**, **Analysis**, **TruClient**, **MI Listener**, or **Monitors Over Firewall**. For details, see the *LoadRunner Installation Guide* available from the LoadRunner Professional Help Center.

Note:

- During the installation of Load Generator Standalone, MI Listener, or Monitors over Firewall components, the setup wizard prompts you to select the mode for running the installed agent. Select **LoadRunner Enterprise mode**.

  The agent runs as a service under a special account named **IUSR_METRO**. This is a local Windows account, created during the installation process (some additional LoadRunner Enterprise configuration is also added on the load generator).

  You can delete the **IUSR_METRO** account only if the LoadRunner Enterprise system user was configured to a different Windows account; otherwise the host will not function correctly.
- The Load Generator installer package, **OneLG**, is a combined installer that can be used with all LoadRunner family products. During OneLG installation, you can select to use

> the load generator with LoadRunner Enterprise, LoadRunner Professional or LoadRunner Cloud. For general information on installing and working with load generators, see the relevant Help Center:
>
> - ○ LoadRunner Professional
> - ○ LoadRunner Cloud
>
> - If you attempt to install standalone components on a system drive other than the default C drive, you will get a warning that you are out of disk space on your system drive even though you are not installing there. This is because the installer, while installing the components to the drive as specified by the user, still needs to use the Windows temporary file locations during installation.
>
>   **Workaround:** Free up space on your C system drive.

3. **MI Listener/Monitors Over Firewall installations only:** Follow the instructions in the installation wizard. After installation, the configuration wizard opens, requesting the name of the product you are working with. Select **LoadRunner Enterprise**.

Silently install standalone applications

This section describes how to perform a silent installation of the standalone applications.

> **Note:** For instructions on installing the Load Generator silently on Linux, see the *LoadRunner Installation Guide* available from the LoadRunner Professional Help Center.

Choose one of the following options:

Option 1: Install the prerequisite software and the application separately

1. Install required prerequisite software. For details, see "Prerequisite software for silent installation" on page 76.
2. Extract the Load Generator installation files to a local directory:
   a. Select an application from the **<Installation_Disk_Root_Directory>\Standalone Applications** folder.
   b. Extract the **.msi** file from the **.exe** application to the installation folder.
3. Run one of the following commands from the command line:
   - **Load Generator:**

     ```
     msiexec /i "<Installation_Folder>\OneLG_x64.msi" /qb /l*vx "<Path to
     log file>" IS_RUNAS_SERVICE=1 START_LGA="1"
     ```

   - **VuGen Standalone:**

```
msiexec /i "<Installation_Folder>\VuGen_x64.msi" /qb /l*vx "<Path to
log file>"
```

- **Analysis Standalone:**

```
msiexec /i "<Installation_Folder>\Analysis_x64.msi" /qb /l*vx "<Path
to log file>"
```

where **<Installation_Folder>** is the local directory where you saved the installation files, and **<Path to log file>** is the full path to the installation log file.

> **Note:** You can install the Load Generator component on a Linux platform to run virtual users. The Linux virtual users interact with the Controller, installed on a Windows machine. For details on installing the Load Generator on Linux, see the *LoadRunner Installation Guide* available from the LoadRunner Professional Help Center.

Option 2: Install the prerequisite software and the application together

1. Select an application from the **<LRE installation directory>\Additional Component\Applications** folder.
2. Run one of the following commands from the command line:
   - **Load Generator:**

```
SetupOneLG.exe /s /a /s IS_RUNAS_SERVICE=1 START_LGA=1
INSTALLDIR="C:\OneLG"
```

   - **VuGen Standalone:**

```
SetupVuGen.exe /s /a /s INSTALLDIR="c:\Micro Focus\VuGen_SA"
```

   - **Analysis Standalone:**

```
SetupAnalysis.exe /s /a /s
```

Install Load Generator on Linux

You can install the Load Generator component on a Linux platform to run virtual users. The Linux virtual users interact with the Controller, installed on a Windows machine. For details on installing the Load Generator on Linux, see the *LoadRunner Installation Guide* available from the LoadRunner Professional Help Center.

Deploy Dockerized load generators on Linux

This section describes how to run a Dockerized load generator on a Linux distribution.

Docker is a platform that allows you to develop, ship, and run applications via a container. For details regarding Docker, see https://docs.docker.com.

> **Note:** For supported protocols on Dockerized load generators, see the Supported Protocols guide.

Prerequisites

> **Note:** The Ubuntu image for the OneLG load generator replaces the previous Ubuntu load generator docker image.

- Install Docker on the target machine, along with its dependencies, and set up the target machine environment as required. Currently, only the 64-bit version is supported. For installation details, see https://docs.docker.com/install/.
- Obtain the predefined load generator Docker image. Two images are available, Linux-Ubuntu and RHEL.

  Pull the image from the from the relevant page, accessible from the performance testing page (https://hub.docker.com/u/performancetesting) in the Docker hub. Use the following commands and appropriate **<tag version number>**, for example, 21.00:

  For Linux-Ubuntu:

  ```
  docker pull performancetesting/microfocus_onelg_linux_ubuntu:<tag version number>
  ```

  For RHEL:

  ```
  docker pull performancetesting/load_generator_redhat:<tag version number>
  ```

Run a Dockerized load generator using the predefined image

Use the ready-to-use image to run a load generator on Docker for Linux.

> **Note:** If you need customization for your container, for example, for proxy servers, see "Run a Dockerized load generator using a custom image" on page 90.

To run a Dockerized load generator:

Run the load generator container using the following command:

Linux-Ubuntu:

```
docker run -id -p <host_port>:54345 performancetesting/microfocus_onelg_
linux_ubuntu:<tag version number>
```

RHEL:

```
docker run -id -p <host_port>:54345 performancetesting/load_generator_
redhat:<tag version number>
```

> **Note:** Check that the <host_port> on the Linux machine is available and allows incoming requests. You will specify this port on the Controller side when connecting to this load generator.

Example using SSH

The following gives a simple C# code example for running multiple load generator containers using SSH. There are container orchestrator tools which do the same, for example, Kubernetes, OpenShift, Docker Swarm, and more.

```
using (var client = new SshClient(dockerHost, dockerHostUserName,
dockerHostPasswd))
{
  client.Connect();
  for (int i =0; i > numOfContainers; i++)
  {
       string command = "docker run -id -p " + lgInitialPort + i) +
":54345 performancetesting/microfocus_onelg_linux_ubuntu:<tag
version number>";
       var terminal = client.RunCommand(command);
       if (terminal.ExistStatus != 0)
       {
       throw new Exception("Failed to create new Docker container");
       }
       Console.WriteLine("Docker LG with external port" + lgInitialPort +
i + "created.");
  }
  client.Disconnect();
}
```

Run a Dockerized load generator using a custom image

If your environment requires customized settings for running the container, for example for proxy servers, you can create a Dockerfile to build a custom image.

> **Note:** Another alternative for customized settings: Start the container; once it is running, set up the load generator environment variables, then start the load generator manually inside the container.

To run a custom Dockerized load generator:

1. Create a new folder, and within it create a file named **dockerfile**. Paste the **FROM** line, plus the required customization lines, into the file, using the appropriate LoadRunner Enterprise version for the **<tag version number>**:

   > **Note:** This customization example is for proxy: It defines an environment variable for the proxy server host and port in the target image.

   ```
   FROM performancetesting/microfocus_onelg_linux_ubuntu:<tag version
   number>
   ENV http_proxy http://my_proxy_name:port
   ```

   > **Note:** The above customization example is for a proxy. It defines an environment variable for the proxy server host and port in the target image.

2. Save the Dockerfile.
3. Open a command line at the **dockerfile** folder path and run the following command, using the name you want for your custom image:

   Linux-Ubuntu:

   ```
   docker build -t <custom dockerfile name> .
   ```

   RHEL:

   ```
   docker build -t <custom dockerfile name> .
   ```

4. Create a container for each load generator you want to use, by running the following command:

Linux-Ubuntu:

```
docker run -id -p <host_port>:54345 <custom image name>
```

RHEL:

```
docker run -id -p <host_port>:54345 <custom image name>
```

If the custom image in step 3 was built with a tag then include it in the command:

```
docker run -id -p <host_port>:54345 <custom image name>:<tag version
number>
```

> **Note:** Check that the <host_port> on the Linux machine is available and allows incoming requests. You will specify this port on the Controller side when connecting to this load generator.

After running the load generator containers

Add the load generators containers to your tests.

- For elastic hosts, see Set up elastic hosts on Windows or Linux containers in the LoadRunner Enterprise Help Center.
- For manually configure Dockerized load generators, see Add Dockerized hosts to your tests in the LoadRunner Enterprise Help Center.

Build a custom Dockerfile image

Use the sample Dockerfile content provided below as a basis for your custom file, and edit to fit your specific needs. Once you have the file, follow these steps to build a Docker image:

1. Place your Dockerfile and the load generator installation folder, **VM** (containing inst64.bin, unzip, and installer.sh), together in the same folder.
2. Switch to root user. Make sure you have Internet access and the ability to install dependencies.
3. In the directory which contains the Dockerfile, type:

```
docker build -t load_generator ./
```

Sample Dockerfile Content

The following example shows how to build a Linux image. It sets a proxy enabling the container to connect to the Internet and then installs the load generator prerequisites. It then copies the load generator installation files to the container and installs it silently. Lastly, it sets an ENTRYPOINT which tells the container what to execute when starting.

> **Note:** The selected base operating system must be one of the supported Linux distributions in the system requirements of the LoadRunner Enterprise version being used.

```
# sudo docker build -t load generator /
# Set the base image
FROM ubuntu:14.04
# Set the proxy
# ENV http_proxy http://my_proxy_name:port
# Install prerequisites for Load Generator
RUN dpkg --add-architecture i386
RUN apt-get update && apt-get install -y libc6-i386 lib32stdc++6 lib32ncurses5 libkeyutils1:i386 libglib2.0-0:i386 libidn11:i386
# Copy the Load Generator installation files to a temporary folder
RUN mkdir /opt/tmp_LG
ADD VM /opt/tmp_LG
# Install the Load Generator
RUN /bin/bash -c "cd /opt/tmp_lg; source ./installer.sh -i silent"
# Remove the installation files
RUN rm -R /opt/tmp_LG
#Start the container. If you need entry to the container, add --entrypoint to overwrite the ENTRYPOINT. If you do not need entry to the container, use "-id" to start the container.
ENTRYPOINT ["/bin/bash","-c","cd /opt/MF/MF_LoadGenerator/; source env.sh; cd bin/; ./m_daemon_setup -install; while true; do cat; done"]
```

Tips and guidelines

- Dockerized load generators, run from the predefined image, are not supported when running over a firewall. (Workaround for advanced users: You can develop your own Docker image with MI Listener support.)
- Use `docker ps` to list the containers that are running.

- To stop the load generator service:
  - Use `docker stop <load generator container name or ID>` if you want to reuse the same load generator.
  - Use `docker rm -f <load generator container name or ID>` in order to remove the load generator container.
- The Dockerfile container has an ENTRYPOINT section. The container first runs the commands in ENTRYPOINT. It sets up the environment and then starts the load generator. The command uses a While loop to wait for input, in order to keep the container from exiting. This behavior prevents you from accessing the container while it is running. Make sure to add -i while starting the container; otherwise the While loop will consume an excessive amount of CPU.
- If you need entry into the container, add an argument such as `--entrypoint=/bin/bash` when starting the container. After entering the container, set the load generator environments and start the load generator. You can then switch to the host using CTRL+p and CTRL+q while keeping the container running in the background. To access the container again, use the `docker attach container_id` command.
- To access the host network directly, use `--net=host` in place of `-p <host_port>:54345`. We recommend you use this flag if the AUT generates a lot of network activity.

Deploy Dockerized load generators on Windows

This section describes how to run a Dockerized load generator on a Windows platform.

Docker is a platform that allows you to develop, ship, and run applications via a container. For details regarding Docker, see https://docs.docker.com.

> **Note:** For supported protocols on Dockerized load generators, see the Supported Protocols guide.

Prerequisites

> **Note:** The Docker image for the OneLG load generator replaces the previous Windows standalone load generator docker image.

- Install Docker on the target machine, along with its dependencies, and set up the target machine environment as required. Currently, only the 64-bit version is supported. For installation details, see https://docs.docker.com/install/.
- Pull the Windows load generator Docker image from the from the relevant page, accessible from the performance testing page (https://hub.docker.com/u/performancetesting) in the Docker hub. Use the following command and appropriate **<tag version number>**, for example, 21.00:

  ```
  docker pull performancetesting/microfocus_onelg_windows:<tag
  version number>
  ```

Run a Dockerized load generator using the predefined image

Use the ready-to-use image to run a load generator (OneLG) on Docker for Windows.

> **Note:** If you need customization for your container, for example, for Java or to run under a specific user, see "Run a Dockerized load generator using a custom image" below.

To run a Dockerized load generator:

Run the load generator container using the following command:

```
docker run -id -p <host_port>:54345 performancetesting/microfocus_onelg_
windows:<tag version number>
```

> **Note:** Check that the <host_port> on the machine is available and allows incoming requests. You will specify this port on the Controller side when connecting to this load generator.

Run a Dockerized load generator using a custom image

If your environment requires customized settings for running the container, you can create a Dockerfile to build a custom image for Docker on Windows.

Examples for custom images:

- To use a specific user account for the processes under which the Vusers are running, to provide support for accessing network resources like script parameter files. After running, the container should be able to verify the user.
- To run Java protocols on Windows load generator containers.
- To define environment variables for proxy server host and port.

To run a custom Dockerized load generator:

1. Create a new folder, and within it create a file named **dockerfile**. Paste the following **FROM** line into the file, using the appropriate LoadRunner Enterprise version for the **<tag version number>**, and add the relevant customization lines:

   ```
   FROM performancetesting/microfocus_onelg_windows:<tag version number>
   <Customization lines>
   ```

   For customization examples, see "Examples of customized content for Dockerfiles " on the next page

> **Tip:** For information on commands that can be used in Docker files, see https://docs.docker.com/engine/reference/builder/.

2. Save the Dockerfile.
3. Open a command line at the **dockerfile** folder path and run the following command, using the name you want for your custom image:

```
docker build -t <custom dockerfile name> .
```

4. Create a container for each load generator you want to use, by running the following command (or use any Docker orchestrator tool for running containers):

```
docker run -id -p <host_port>:54345 <custom image name>
```

If the custom image in step 3 was built with a tag then include it in the command:

```
docker run -id -p <host_port>:54345 <custom image name>:<tag version
number>
```

> **Note:**
>
> - Check that the <host_port> on the machine is available and allows incoming requests. You will specify this port on the Controller side when connecting to this load generator. This is not relevant when using elastic load generators, since this is managed by the orchestrator.
> - To deploy elastic load generators, you must provide the custom image name in the Swarm orchestrator.

Examples of customized content for Dockerfiles

Example for Vusers under a specified user account

The following gives an example of dockerfile content for running the Vusers under a specified user account with network access to shared locations. Replace the values between **<>** with credentials for a valid user account in your environment, with network access to the shared resources.

> **Example:**
>
> ```
> #escape=`
> FROM performancetesting/microfocus_onelg_windows:21.00
> RUN c:\LG\launch_service\bin\magentservice.exe -remove
> ```

```
RUN c:\LG\launch_service\bin\magentservice -install
<domain>\<user name> <password>
```

Example for running Java protocols

The following gives an example of dockerfile content to run Java protocols:

Example:

```
#escape=`
FROM performancetesting/microfocus_onelg_windows:21.00
COPY .\<folder contains JDK> <target path in the container>
```

The path to the target JDK directory defined in the **COPY** line for the **<target path in the container>** must also be added to the **Java VM** runtime settings page:

Note: For Java 64-bit protocol testing, include the following command line in the dockerfile, in order to add the path to the **bin** folder for the JDK 64-bit to the machine PATH environment variable:

```
RUN powershell [Environment]::SetEnvironmentVariable(\"Path\",
$env:Path + \";<target JDK path in the container>\bin\",
[EnvironmentVariableTarget]::Machine)
```

After running the load generator containers

Add the load generators containers to your tests.

- For elastic hosts, see Set up elastic hosts on Windows or Linux containers in the LoadRunner Enterprise Help Center.
- For manually configure Dockerized load generators, see Add Dockerized hosts to your tests in the LoadRunner Enterprise Help Center.

Note: This is not relevant when using orchestrators.

Tips and guidelines

- Dockerized load generators, run from the predefined image, are not supported when running over a firewall.
- Use `docker ps` to list the containers that are running.
- To stop the load generator service:

- Use `docker stop <load generator container name or ID>` if you want to reuse the same load generator.
- Use `docker rm -f <load generator container name or ID>` in order to remove the load generator container.

- To access the host network directly, use `--net=host` in place of `-p <host_port>:54345`. We recommend you use this flag if the AUT generates a lot of network activity.

Install additional components

You can install additional components that provide advanced features for working with LoadRunner Enterprise. You install these components from the **Additional Components** directory, located in the root directory of the installation directory. The following components are available:

Component	Description
Agent for Citrix Server	Installs an optional component on the server machine that enhances VuGen's capabilities in identifying Citrix client objects.
Agent for Microsoft Terminal Server.	Used for extended RDP protocol record-replay. This component runs on the server side, and is used to create and run enhanced RDP scripts.
Applications	This folder contains the setup files for following standalone applications: Analysis, Virtual User Generator (VuGen), Load Generator, TruClient, MI Listener, and Monitors Over Firewall. Run the relevant application's setup program and follow the wizard's instructions. For details, see "Applications " on page 13.
Assembly Crawler for Analysis API	Installs a command-line utility to build a .NET configuration file for a LoadRunner Analysis API application. For details, refer to the Analysis API Reference.
IDE Add-ins	Installs add-ins for Visual Studio or Eclipse, enabling you to create NUnit or JUnit tests in your standard development environment using the LoadRunner API.
SAP Tools	The following SAP tools are available: • **SAPGUI Spy.** Examines the hierarchy of GUI Scripting objects, on open windows of SAPGUI Client for Windows. • **SAPGUI Verify Scripting.** Verifies that the SAPGUI Scripting API is enabled.
Third Parties	Includes the source code for open-source packages that are incorporated into LoadRunner Enterprise, and which have licenses with source distribution clauses.

Component	Description
Virtual Table Server	Virtual Table Server (VTS) is a web-based application that works with Vuser scripts. VTS offers an alternative to standard parameterization. Two versions of VTS are available: 32-bit and 64-bit. You can install 32-bit VTS on both 32-bit and 64-bit operating systems; 64-bit VTS can be installed only on 64-bit operating systems.
VuGen Script Converter	Installs the VuGen Script Converter that enables converting NUnit/JUnit tests to VuGen scripts in order to run them in LoadRunner Enterprise.

Uninstall LoadRunner Enterprise server and hosts

You can uninstall LoadRunner Enterprise servers and hosts using the LoadRunner Enterprise Setup Wizard or using the silent commands.

> **Note:**
>
> - When uninstalling earlier versions of LoadRunner Enterprise, the Network Virtualization components installed during the installation will be automatically uninstalled.
> - For cluster environments: Uninstall LoadRunner Enterprise from all nodes.

To uninstall LoadRunner Enterprise components using the setup wizard:

1. From the Windows Control Panel, open the Add/Remove Programs dialog box.
2. From the list of currently installed programs, select the program you want to uninstall, and click **Remove**.
   - **Micro Focus LoadRunner Enterprise <product version>** for LoadRunner Enterprise server
   - **Micro Focus LoadRunner <product version>** for LoadRunner Enterprise hosts
3. Follow the instructions in the wizard to complete the uninstall process.

To uninstall LoadRunner Enterprise components silently:

Run the applicable command from the command line.

- **LoadRunner Enterprise Server:**

```
 msiexec.exe/uninstall "<Installation_Disk_Root_
Directory>\Setup\Install\Server\LRE_Server.msi" /qnb
```

- **LoadRunner Enterprise Host**:

```
msiexec.exe/uninstall "<Installation_Disk_Root_
Directory>\Setup\Install\Host\LoadRunner_x64.msi" /qnb
```

Uninstall Load Generator from Linux

You can use the Load Generator Setup Wizard to uninstall the load generator. For details, see the *LoadRunner Professional Installation Guide* available from the LoadRunner Professional Help Center.

Post installation verification

This section describes how to verify that the installation of the LoadRunner Enterprise server and hosts was successful. The environment for this process should be a staging environment, including a LoadRunner Enterprise server and two to three LoadRunner Enterprise hosts.

> **Note:** You can run a full validation on your LoadRunner Enterprise system from LoadRunner Enterprise Administration, in the System Health page's Check System tab. For details, see Maintain system health in the LoadRunner Enterprise Help Center.

Administrator workflow

This section describes the workflow for the LoadRunner Enterprise administrator.

1. **Log onto LoadRunner Enterprise Administration.**

   For details, see Log onto LoadRunner Enterprise Administration in the LoadRunner Enterprise Help Center.

2. **Create a project administrator user.**

   For details, see Create a new user in the LoadRunner Enterprise Help Center.

3. **Create a domain.**

   For details, see Create a domain in the LoadRunner Enterprise Help Center.

4. **Create a new project.**

   Follow the steps to create the project in Create a project in the LoadRunner Enterprise Help Center, and:

   a. In the **Domain Name** list, select the domain you just created.

   b. Skip the **Main Details** for now (you will define them after adding a host and host pool in step 9).

   c. Assign the project administrator user you created above to the **Users** list.

5. **Assign more project administrators to the project - optional.**

   a. Select **Management > Projects**, and in the projects list, click the name of project you created to display the project details.

   b. In the right lower pane, click the **Users** tab, and assign another project administrator user.

6. **Verify the LoadRunner Enterprise configuration.**

   On the LoadRunner Enterprise Administration sidebar,

   - Under **Configuration**, select **Servers** and verify that the LoadRunner Enterprise Server is listed.
   - Under **Configuration**, select **Licenses** and verify the license details.

7. **Define additional hosts for the staging environment.**

For the staging environment, you should have two to three LoadRunner Enterprise hosts, where at least one host purpose is configured as Controller, and at least one host purpose is configured as Load Generator.

> **Note:** When adding hosts, fields in red marked with an asterisk (*) are mandatory. Make sure to include the operating system type, and the purpose of the host. For details, see Manage hosts in the LoadRunner Enterprise Help Center.

a. On the LoadRunner Enterprise Administration sidebar, under **Maintenance**, select **Hosts**.

b. Click the **Create New Host** + button, and define the host details.

8. **Create host pools.**
   a. On the LoadRunner Enterprise Administration sidebar, select **Maintenance > Hosts**, and click the **Pools** tab.
   b. Click the **Add New Pool** + button. The New Pool page opens, enabling you to define a new host pool.
   c. Add a name and description (optional) for the host pool.
   d. In the Linked Hosts grid, select the hosts to add to the pool, and click **Assign**. The selected hosts are added to the pool.
9. **Define project settings.**
   a. On the LoadRunner Enterprise Administration sidebar, select **Management > Projects**.
   b. Under the **Project Name** column, click the project to display the project details.
   c. In the **Main Details** tab, finish defining the project's settings. In particular, set the Vuser limit, Host limit, and Concurrent run limit. Also, select the host pool you created above for the project.

LoadRunner Enterprise configuration options

The LoadRunner Enterprise system comes with default configuration settings. These settings enable you to use LoadRunner Enterprise for its intended purpose. This chapter describes additional tuning and configuration to help you get the most out of your LoadRunner Enterprise system.

> **Note:** Not all the procedures in this chapter are suitable for all usage scenarios. You should assess which procedures are suitable to your system's needs.

This chapter includes:

Configuring LoadRunner Enterprise to work with TLS (SSL)

The following section describes how to enable TLS to ensure secure communication on LoadRunner Enterprise. It includes:

- "TLS (SSL) configuration workflow" below
- "Configure IIS to work with TLS (SSL)" on the next page
- "Distribute certificates" on page 105
- "Configure the LoadRunner Enterprise server to work with TLS (SSL)" on page 106
- "Configure LoadRunner Enterprise hosts to work with TLS (SSL)" on page 108

> **Tip:** For additional information (and examples) on how to configure secure communication on the various LoadRunner Enterprise components, see our blog series:
>
> - Configure LoadRunner Enterprise Server to support SSL
> - Configure LoadRunner Enterprise Host to support SSL

TLS (SSL) configuration workflow

This section describes the workflow for configuring the LoadRunner Enterprise server and hosts to work over TLS. You can configure both the LoadRunner Enterprise server and hosts, or the LoadRunner Enterprise server only.

For the LoadRunner Enterprise Server	1. **Configure IIS** For details, see "Configure IIS to work with TLS (SSL)" on the next page. 2. **Add the root certificate to the machine truststore** For details, see "Distribute certificates" on page 105. 3. **Configure the LoadRunner Enterprise server to work with TLS (SSL)** a. Replace the certificates* on the LoadRunner Enterprise server. For details, see "Configure LoadRunner components to work with TLS (SSL)" on page 113. b. Update and replace the relevant configuration files (update **pcs.config** internalUrl with https URL and replace **web.config**). For details, see "Configure the LoadRunner Enterprise server to work with TLS (SSL)" on page 106. c. Restart the LoadRunner Backend Service and IIS. d. Update the internal and external URLs with the "https" URL.

For LoadRunner Enterprise Hosts	1. **Add certificates to the machine truststore** For details, see "Distribute certificates" on the next page. 2. **Configure LoadRunner Enterprise hosts and load generators to work with TLS (SSL)** a. Replace the certificates* on LoadRunner Enterprise hosts and load generators. For details, see "Configure TLS (SSL) for load generators" on page 118. b. Configure secure communication on a LoadRunner Enterprise host. For details, see "Configure LoadRunner Enterprise hosts to work with TLS (SSL)" on page 108.

*The certificate files within the **<installation root>\dat\cert** folder should have the exact names of **cert.cer** and **verify\cacert.cer**, no matter if they are the default ones provided as part of the installation, or if they are your company certificates, and should be the same for all LoadRunner Enterprise components—LoadRunner Enterprise servers, hosts, and load generators.

Configure IIS to work with TLS (SSL)

This section describes the basic steps involved in setting up IIS (Microsoft Internet Information Server) on the LoadRunner Enterprise server machine to use TLS (SSL).

IIS is a prerequisite software for the LoadRunner Enterprise servers. You can configure the IIS LoadRunner Enterprise virtual directories (LoadRunner Enterprise server and host) to use TLS (SSL).

For LoadRunner Enterprise host, the root certificate of the CA should appear in the Microsoft Management Console under **Certificates (Local Computer) > Trusted Root Certification Authorities**. For details, see "Distribute certificates" on the next page.

Configure IIS to use TLS (SSL) on the LoadRunner Enterprise server machine

1. Perform the following before you configure IIS:
   - Configure your servers to support the latest TLS versions to ensure you are using only the strongest cryptographic protocols. Make sure you disable old SSL and TLS versions (SSLv2, SSLv3, TLS 1.0, and TLS 1.1) on IIS and on your operating system . For more information, see the following Microsoft articles: Transport Layer Security (TLS) registry settings and TLS version enforcement capabilities now available per certificate binding on Windows Server 2019.
   - Make sure port 443 on the LoadRunner Enterprise server is available for use by IIS.

     IIS uses port 443 to work with TLS (SSL). Since certain LoadRunner Enterprise components might also be configured to use this port, configure the LoadRunner Enterprise components to use a different port.

     > **Note:** The Remote Management agent uses port 443 by default. Use the Network and Security Manager tool to change the port being used by the agent to a new port. For

> details, see the LoadRunner Professional Help Center.

- Prevent host header injection in a Server-Side Request Forgery (SSRF) attack.

  We recommend configuring the HTTPS communication and IIS host binding for all relevant protocols (these configurations are not provided by Micro Focus by default).

  > **Note:** By not implementing the secure configuration and proper hardening of the IIS you may exposing the system to increased security risks.

2. Obtain a server certificate issued to the fully qualified domain name of your LoadRunner Enterprise server.
3. Configure IIS to work with TLS (SSL).

   Update IIS with the https binding (the same port as you used in step 1 above) and remove the http binding.

   a. Open IIS Manager, and select **Server Home > Server Certificates > Import**.

   b. Import the server certificate (in pfx format) that you obtained above.

   c. In the **Actions** pane, click **Bindings**. and then click **Add** in the Site Bindings window.

   d. In the Edit Site Binding dialog box, configure the following:

      - Type: https
      - IP address: All Unassigned
      - Port: 444
      - SSL Certificate: *.<your domain name>

   For more information, see https://docs.microsoft.com/en-us/iis/manage/configuring-security/how-to-set-up-ssl-on-iis.

Distribute certificates

Add the root certificate to the machine truststore on the LoadRunner Enterprise server, LoadRunner Enterprise hosts, and OneLG standalone load generators.

1. Extract the contents from the domain certificate in .pfx format to the personal truststore of the host.
2. Add the CA certificate to the machine's truststore.

   If your are using a secure connection for the internal URL of the LoadRunner Enterprise server, you need to establish trust to the Certificate Authority (CA) that issued your LoadRunner Enterprise server certificate.

   a. Run the following command to update the certificates using MMC (Microsoft Management Console):

   ```
   run mmc.exe
   ```

   b. In the console, select **Run > Add/Remove Snap-in**.

   c. From the list of available snap-ins, select **Certificates** and click **Add**.

   d. In the Certificates snap-in dialog box, select **Computer account**, and then click **Next**.

   e. In the Console Root tree, expand **Trusted Root Certification Authorities**. Right-click **Certificates** and select **All Tasks > Import**.

   f. In the Certificate Import Wizard, click **Next**.

   g. Click **Browse**, and navigate to the unzipped certs folder. Select **PCSecureEnvTestingCA** certificate, and click **Open**.

   h. Click **Next** in the certificate stores page of the wizard, and then click **Finish**. Wait for the import success message.

3. Repeat on all LoadRunner Enterprise machines.
4. (For LoadRunner Enterprise hosts used as Controllers only) Import the domain certificate in .pfx format to the personal truststore of the host.

Configure the LoadRunner Enterprise server to work with TLS (SSL)

This section explains how to configure secure communication on a LoadRunner Enterprise server for incoming requests from the LoadRunner Enterprise server and hosts.

To configure the LoadRunner Enterprise server to use TLS (SSL), you need to perform the following:

1. Update the **web.config** file located in the **<LRE server installation folder>\PCS** directory.

   a. Create a backup copy of the **web.config** file and save it in a different folder.

   b. To update the **web.config** file, you can replace it with the predefined **web.config-for_ssl** file. See step **1d** below.

   If you have manual changes you want to preserve in the **web.config** file, you can manually modify the file. See step **1c** below.

   c. Edit the **web.config** file. Under the **<system.servicemodel><services>** tag, there are eight areas where the following comment appears: **Uncomment to enable SSL**. Uncomment the XML lines which appear thereafter, and comment the non-TLS/SSL settings as shown in the example below.

   Example: Before

```
<endpoint binding="basicHttpBinding"
contract="HP.PC.PCS.ILabService"><identity>
<dns value="localhost"/></identity></endpoint>
<endpoint address="mex" binding="mexHttpBinding"
contract="IMetadataExchange"/>
<!- Uncomment to enable TLS/SSL ->
<!-- endpoint binding="basicHttpBinding"
bindingConfiguration="BasicHttpBinding_TransportSecurity"
```

```
contract="HP.PC.PCS.ILabService"><identity>
<dns value="localhost"/></identity></endpoint -->
```

Example: After

```
<!--<endpoint binding="basicHttpBinding"
contract="HP.PC.PCS.ILabService"><identity>
<dns value="localhost"/></identity></endpoint>
<endpoint address="mex" binding="mexHttpBinding"
contract="IMetadataExchange"/> -->
<!-- Uncomment to enable TLS/SSL -->
<endpoint binding="basicHttpBinding"
bindingConfiguration="BasicHttpBinding_TransportSecurity"
contract="HP.PC.PCS.ILabService"><identity>
<dns value="localhost"/></identity></endpoint>
```

Under the **<system.servicemodel><behaviors>** tag, there are seven areas where you need to change the **httpGetEnabled** parameter to **false**, and the **httpsGetEnabled** parameter to **true**.

Example: Before

```
<serviceMetadata httpGetEnabled="true" httpsGetEnabled="false"
/>
```

Example: After

```
<serviceMetadata httpGetEnabled="false" httpsGetEnabled="true" />
```

d. To replace **web.config** with the predefined **web.config-for_ssl** file, copy **web.config-for_ssl** from the **<LRE server installation folder>\conf\httpsConfigFiles** directory and place it under the **<LRE server installation folder>\PCS** directory.

   Rename **web.config-for_ssl** to **web.config**.

2. Open the **PCS.config** file, located in the **<LRE server installation folder>\dat** path, and update the Internal URL attribute with https to connect to LoadRunner Backend Service through a secure port:

   ```
   internalUrl="https://<lre-dns-name>:444"
   ```

3. Update the LoadRunner Enterprise server to ensure that communication with the host is secure (only required when you plan to configure hosts to work with TLS/SSL)

   If the LoadRunner Enterprise host is secured, edit the **PCS.config** file located in the **<LoadRunner Enterprise server install path>\dat** path, by changing the value of the **ltopIsSecured** parameter to **true**.

Example: Before

```
<PCSSettings ltopPortNumber="8731" ltopIsSecured="false"
StartRunMaxRetry="3" DataProcessorPendingTimeoutMinutes="2880"/>
```

Example: After

```
<PCSSettings ltopPortNumber="8731" ltopIsSecured="true"
StartRunMaxRetry="3" DataProcessorPendingTimeoutMinutes="2880"/>
```

4. Restart the LoadRunner Backend Service.
5. Restart IIS.
6. In LoadRunner Enterprise Administration, update the LoadRunner Enterprise server internal and external URLs with the https URL.

Configure LoadRunner Enterprise hosts to work with TLS (SSL)

This section explains how to configure secure communication on a LoadRunner Enterprise host for incoming requests from LoadRunner Enterprise servers.

Configure the LoadRunner Enterprise load generators

1. The default port used by a LoadRunner Enterprise host service is 8731. To configure TLS (SSL) on a host for port 8731, refer to the Microsoft Web Site: How To Configure a Port with an SSL Certificate, using the following URL: http://msdn.microsoft.com/en-us/library/ms733791.aspx.

   Below are examples of the steps described in the above link.

   a. Check that the port is not configured:

      Example:

      ```
      C:\Users\Demo>netsh http show sslcert ipport=0.0.0.0:8731
      SSL Certificate bindings:
      -------------------------
      The system cannot find the file specified.
      ```

   b. Run the netsh command:

      You can use the command below (where `certhash` is the certificate thumbprint and the `appid` parameter is a GUID that can be used to identify the owning application. You can use any valid GUID. There are many tools that can generate a GUID).

      Example:

```
C:\Users\Demo>netsh http add sslcert ipport=0.0.0.0:8731
certhash=1b337c1f17e0f96b09f803fs0c2c7b3621baf2bb appid=
{114F6E0C-EB01-4EE9-9CEF-3D1A500FD63F}
SSL Certificate successfully added
```

c. Check that the port is now configured:

Example:

```
C:\Users\Demo>netsh http show sslcert ipport=0.0.0.0:8731
SSL Certificate bindings:
-------------------------
IP:port                      : 0.0.0.0:8731
Certificate Hash             :
1b337c1f17e0f94b09f803ff0c2c7b7621baf2bb
Application ID               : {114f6e0c-eb01-4ee9-9cef-
3d1a500fd63f}
Certificate Store Name       : (null)
Verify Client Certificate Revocation : Enabled
Verify Revocation Using Cached Client Certificate Only :
Disabled
Usage Check                  : Enabled
Revocation Freshness Time    : 0
URL Retrieval Timeout        : 0
Ctl Identifier               : (null)
Ctl Store Name               : (null)
DS Mapper Usage              : Disabled
Negotiate Client Certificate : Disabled
```

2. Perform the following steps to update the **LTOPSvc.exe.config** file:

   a. Create a backup copy of the **LtopSvc.exe.config** file located under the **<install path>\bin** directory, and save it in a different folder.

   b. To update the **LtopSvc.exe.config** file, you can replace it with the predefined **LTOPSvc.exe.config-for_ssl file**. See step **2d** on page 112.

      If you have manual changes you want to preserve in the **LTOPSvc.exe.config** file, you can manually modify the file. See step **2c** below.

   c. Under the **<system.servicemodel><bindings><basicHttpBinding>** tag, there are two areas where the following comment appears: **Uncomment to enable SSL**. Uncomment the XML lines which appear thereafter.

      Example: Before

```
<binding name="BasicHttpBinding_ILoadTestingService"
closeTimeout="00:10:00"
           openTimeout="00:01:00" receiveTimeout="00:20:00"
sendTimeout="00:10:00"
             allowCookies="false" bypassProxyOnLocal="false"
hostNameComparisonMode="StrongWildcard"
             maxBufferSize="2147483647"
maxBufferPoolSize="2147483647"
maxReceivedMessageSize="2147483647"
             messageEncoding="Text" textEncoding="utf-8"
transferMode="Buffered"
             useDefaultWebProxy="true">
          <readerQuotas maxDepth="2147483647"
maxStringContentLength="2147483647"
maxArrayLength="2147483647"
          maxBytesPerRead="2147483647"
maxNameTableCharCount="2147483647" />
          <!-- Uncomment to enable TLS/SSL -->
          <!--<security mode="Transport">
            <transport clientCredentialType="None"/>
          </security>-->
        </binding>
```

Example: After

```
<binding name="BasicHttpBinding_ILoadTestingService"
closeTimeout="00:10:00"
             openTimeout="00:01:00" receiveTimeout="00:20:00"
sendTimeout="00:10:00"
             allowCookies="false" bypassProxyOnLocal="false"
hostNameComparisonMode="StrongWildcard"
             maxBufferSize="2147483647"
maxBufferPoolSize="2147483647"
maxReceivedMessageSize="2147483647"
             messageEncoding="Text" textEncoding="utf-8"
transferMode="Buffered"
            useDefaultWebProxy="true">
          <readerQuotas maxDepth="2147483647"
maxStringContentLength="2147483647"
```

```
maxArrayLength="2147483647"
          maxBytesPerRead="2147483647"
maxNameTableCharCount="2147483647" />
          <!-- Uncomment to enable TLS/SSL -->
          <security mode="Transport">
            <transport clientCredentialType="None"/>
          </security>
        </binding>
```

Under the **<system.servicemodel><services>** tag, switch between the non-secured and secured endpoints and base addresses.

Example: Before

```
<endpoint contract="HP.PC.LTOP.Services.ILoadTestingService"
address="LoadTestingService" name="basicHttp"
binding="basicHttpBinding"
bindingConfiguration="BasicHttpBinding_ILoadTestingService"/>
        <!-- Use the first endpoint for regular communication
and the second endpoint for TLS/SSL -->
        <endpoint contract="IMetadataExchange"
binding="mexHttpBinding" name="mex" />
        <!--<endpoint contract="IMetadataExchange"
binding="mexHttpsBinding" name="mex" />-->
        <host>
          <baseAddresses>
            <!-- Use the first address for regular
communication and the second address for TLS/SSL -->
            <add
baseAddress="http://localhost:8731/LTOP/LoadTestingService"/>
            <!--<add
baseAddress="https://localhost:8731/LTOP/LoadTestingServic
e"/>-->
          </baseAddresses>
        </host>
      </service>
```

Example: After

```
<service name="HP.PC.LTOP.Services.LoadTestingService"
behaviorConfiguration="CommonBasicHTTPBehavior">

        <endpoint contract="HP.PC.LTOP.Services.ILoadTestingService"
address="LoadTestingService" name="basicHttp" binding="basicHttpBinding"
bindingConfiguration="BasicHttpBinding_ILoadTestingService"/>        <!-- Use
the first endpoint for regular communication and the second
endpoint for TLS/SSL -->
        <!-- <endpoint contract="IMetadataExchange"
binding="mexHttpBinding" name="mex" />-->
        <endpoint contract="IMetadataExchange"
binding="mexHttpsBinding" name="mex" />
        <host>
          <baseAddresses>
            <!-- Use the first address for regular
communication and the second address for TLS/SSL -->
            <!--<add
baseAddress="http://localhost:8731/LTOP/LoadTestingService"/>-->
            <add baseAddress="https://localhost:8731/LTOP/LoadTestingService"/>
          </baseAddresses>
        </host>
      </service>
```

Under the **<system.servicemodel><behaviors><serviceBehaviors><behaviorname="CommonBasicHTTPBehavior">** tag, change the **httpGetEnabled** parameter to **false**, and the **httpsGetEnabled** parameter to **true**.

Example: Before

```
<serviceMetadata httpGetEnabled="true" httpsGetEnabled="false"
/>
```

Example: After

```
<serviceMetadata httpGetEnabled="false" httpsGetEnabled="true" />
```

d. To replace **LTOPSvc.exe.config** with the predefined **LTOPSvc.exe.config-for_ssl** file, copy **LTOPSvc.exe.config-for_ssl** from the **<install path>\conf\httpsconfigfiles** directory and place it under the **<install path>\bin** directory.

   Rename **LTOPSvc.exe.config-for_ssl** to **LTOPSvc.exe.config**.

3. Restart the Windows service "LoadRunner Load Testing Service".

> **Note:** If the "LoadRunner Load Testing Service" does not start after configuring the LoadRunner Enterprise host to listen on HTTPS, see Software Self-solve knowledge base article KM03101264.

4. Run the following command:

```
<install path>\bin\lr_agent_settings.exe -check_client_cert 1 -restart_
agent
```

5. After you finish configuring the LoadRunner Enterprise host to support TLS (SSL), reconfigure any hosts that are part of the environment.

Configure LoadRunner components to work with TLS (SSL)

You must update CA and TLS certificates if they were created with LoadRunner tools (Controller, MI Listener, Load Generators, Monitors Over Firewall) or they do not contain the required extension information for the CA certificate being used.

You also need to update CA and TLS certificates for the LoadRunner Enterprise server which communicates with load generators for LAB-related operations. Make sure the certificate files within the **<LRE server installation folder >\dat\cert** folder have the exact names of **cert.cer** and **verify\cacert.cer**, no matter if they are the default ones provided as part of the installation, or if they are your company certificates.

For details on how to obtain the required certificates, see Secure Communication with TLS (SSL) in the LoadRunner Professional Help Center.

> **Note:** After configuring secure communication with TLS, you need to restart the services. To do so, you can either:
>
> - Run **LoadRunner Agent Service** and **LoadRunner Remote Management Agent Service**.
> - Alternatively, run the following command:
>
>   ```
>   lr_agent_settings.exe -restart_agent
>   ```

Working with the LoadRunner Enterprise agent

The LoadRunner Enterprise agent runs on the load generators and enables communication between the Controller, Load Generators, and MI Listeners (in over firewall configurations). The agent receives instructions from the Controller to initialize, run, pause, and stop Vusers. At the same time, the agent also relays data on the status of the Vusers back to the Controller.

Run the LoadRunner Enterprise agent as a process

In some cases, running GUI Vusers on remote machines, or terminal sessions, the LoadRunner Enterprise Agent must run as a process.

To change the LoadRunner Enterprise Agent from a service to a process:

On the host machine, select **Start > Programs > Micro Focus > LoadRunner > Tools > Agent Runtime Settings Configuration**, and select **Manual log in to this machine**.

Run the LoadRunner Enterprise agent as a service

In most cases, the LoadRunner Enterprise Agent runs as a service.

To change the LoadRunner Enterprise Agent from a process to a service:

On the host machine, select **Start > Programs > Micro Focus > LoadRunner > Tools > Agent Runtime Settings Configuration**, and select **Allow virtual users to run on this machine without user login**, and enter a valid user name and password.

Configure the agent on load generator machines

When working with protocols that use network files or Web protocol Vusers that access the Internet through a proxy server, the Load Generator agent must have network privileges. Note that the default user created by LoadRunner Enterprise, **System**, does not have network privileges.

By default, the agent runs as a service on the Load Generator machines. You can either run the agent as a process or you can continue running the agent as a service. To continue running it as a service, configure it to run the session using the local system account or another user account with network access privileges.

Map network drives when running the agent as service

For all Windows platforms, when the user is logged off, the service cannot resolve the mapping of network drives. In cases when the service cannot work with mapped network drives, use the full path to the directory, for example, `<\\<machine-name>\<directory>\>`.

LoadRunner Remote Management Agent

The LoadRunner Remote Management Agent Service enables you to manage remote machines from LoadRunner Enterprise Administration.

The agent is hosted on a Windows-based operating system, and is run as a service under a Local System account which has extensive privileges.

Note: We recommend changing the Local System account to run the service with the minimal permissions required for its operation (see below for details).

Change user under which the services are running

To run the agent service with a less-privileged user, change the user under which the service is running. To do so, configure a limited user account with restricted privileges (such as a Windows service account), that allows the user to perform only the necessary actions required by the system.

When creating a limited user account for running the agent service, we recommend using a Standalone Load Generator. Otherwise you will have to reconfigure the service to run under this user account each time the LoadRunner Enterprise server or host are reconfigured (since the process recreates the LoadRunner Remote Management Agent Service with the default Local System account privileges).

> **Note:** Remote rebooting of hosts and running remote installations is not supported when the Remote Management Agent service is running under a non-admin user account.

Recommended configuration for Linux load generators

You can increase the number of file descriptors, process entries, and amount of swap space by configuring the kernel.

For details and recommendations on improving Linux Load Generator performance, see the *LoadRunner Professional Installation Guide* available from the LoadRunner Professional Help Center.

Recommended change to the TEMP folder used by the load generator

This section describes how to manually change the default TEMP folder used by the load generator to store data during a test run. The TEMP folder is predefined, and is based on the load generator installation folder.

Why change the location of the folder?

- The TEMP folder also contains the script. Depending on the machine and the script, this path can get very long, and exceed the character limitation set by Windows.
- You want to use a different folder or drive instead of the default one.

> **Note:** You cannot change the TEMP folder location if your load generator is configured over a firewall (whether the firewall is enabled or disabled).

Before changing the TEMP folder

Note the following before changing the TEMP folder used by the load generator:

- The change will actually be made on the LoadRunner Enterprise Host that is serving as a Controller. Therefore, such change would only apply to the load generators using this Controller.
- If you are using the same load generators with a new Controller, you will need to reapply this change on the new Controller.

To change the TEMP folder:

1. Log onto the LoadRunner Enterprise Host machine.
2. Verify that the **Wlrun.exe** process is down.
3. Open **<LG installation folder>\config\Wlrun7.ini** in a text editor.
4. Add the line "UserRemoteTmpDir=<Custom temp location>" under the **'[Host]'** section
5. Save the change.

Enable downloading standalone applications

This section explains the steps necessary to enable you to download standalone applications from the Download Applications window.

To enable downloading standalone applications:

1. Navigate to the **<LRE server installation directory>\Additional Components** folder. This directory contains the applications' execution (**.exe**) files.

   > **Note:** The necessary **.exe** files for downloading VuGen, Analysis, Standalone Load Generator, Monitor over Firewall, and MI Listener, are located in the **Applications** directory, which is contained within the **Additional Components** directory.

2. On the LoadRunner Enterprise server, navigate to the **Downloads** directory, which is located in **<LRE server installation directory>\PCWEB\Downloads**.
3. To enable downloading an application, copy the relevant execution file (**.exe**) from the **<LRE server installation directory>\Additional Components** folder to the **Downloads** directory on the LoadRunner Enterprise server.

   > **Note:** You may need to refresh the Download Applications window for the changes to take effect.

Customize the Download Applications window

You can edit and customize the appearance of the Download Applications window. To customize the window, edit the **downloads.xml** file located in the **Downloads** directory on the LoadRunner Enterprise server.

The following tags in the **downloads** file control the following features on the window. Edit the tags as desired to change the appearance of the window.

- **App Name.** The name of the application.
- **Image.** Whether the application's icon appears to the left or to the right of the name.
- **File Name.** If you changed the name of the application's execution file, you must update this section so that it matches the new name of the execution file.
- **Description.** The application's description.

To customize the Download Applications window:

1. (Recommended) Make a backup copy of the **downloads.xml** file before customizing the appearance of the Download Applications window.
2. Open the **downloads.xml** file, and update the tags as required.

   For example:

```
<app name="MyNewApp" image="assets/images/download-
applications/my_Icon.svg">
  <file name="my_file_name.exe">
<description>My file description...</description>
  </file>
  </app>
```

> **Note:** The Download Applications window supports a multilingual user interface for the default applications only. Any changes to the default application tags, and new applications that are added to the **downloads.xml** file, are not supported by MLU.

Enable MS-SQL Windows authentication

This section describes how to configure an MS-SQL database with Windows authentication.

> **Note:** The procedure below requires you to make changes to the MS-SQL database. It is strongly recommended that you make these changes using the SQL Server Management Studio tool.

To enable Windows authentication:

1. Verify that the LoadRunner Enterprise server and database server all belong to the same domain, and that there is a domain user with administrator privileges common to all the machines.
2. Change users to domain users using the System Identity Utility. For details, see Change the LoadRunner Enterprise system user in the LoadRunner Enterprise Help Center.
3. Download the SQL Server Management Studio tool from the Microsoft Download Center (http://www.microsoft.com/downloads/en/default.aspx).
4. In SQL Server Management Studio, perform the following actions:

a. In the Object Explorer pane, expand the **Security** folder.

b. Right-click **Logins** and select **New Login**.

c. Enter the domain user in the **Login name** box, and make sure that **Windows Authentication** is selected.

> **Note:** Verify that the domain user is assigned the same **Server Roles** as the database administrative user **(td_db_admin)**.

5. Make sure that the relevant project is created in LoadRunner Enterprise Administration with the **MS-SQL (Win Auth)** database type. For details, see the LoadRunner Enterprise Help Center.

Configure TLS (SSL) for load generators

This section describes how to configure TLS (formerly SSL) communication to the load generators. It describes how to create and install a Certification Authority and a Client Certificate for working with TLS to secure communication to your load generators. It also describes how to enable TLS from LoadRunner Enterprise Administration.

Create and copy digital certificates

1. Create a Certification Authority (CA)

> **Note:** This step describes how to create a CA using the **gen_ca_cert.exe** utility. If you are working on a Linux platform, use the **gen_ca_cert** utility instead.

On one of your LoadRunner Enterprise hosts, run the **gen_ca_cert** command from the **<LRE host installation folder>\bin** with at least one of the following options:

- -country_name
- -organization name
- -common_name

This process creates two files in the folder from which the utility was run: the CA Certificate (**cacert.cer**), and the CA Private Key (**capvk.cer**).

> **Note:** By default, the CA is valid for three years from when it is generated. To change the validation dates, use the **-nb_time** (beginning of validity) and/or **-na_time** (end of validity) options.

The following example creates two files: **ca_igloo_cert.cer** and **ca_igloo_pk.cer** in the current folder:

```
gen_ca_cert - country_name "North Pole" -organization_name "Igloo
Makers" -common_name "ICL" -CA_cert_file_name "ca_igloo_cert.cer" -
CA_pk_file_name "ca_igloo_pk.cer" -nb_time 10/10/2013 -na_time
11/11/2013
```

2. Install Certification Authority (CA)

   You need to install the CA on the hosts that you want to enable TLS communication including Controllers, LoadRunner Enterprise servers, Load Generators, and MI Listeners.

   Run the **gen_ca_cert** utility from the **<Installation root folder>\bin**
   folder with one of the following parameters:

   - **-install <name/path of the CA certificate file>**. Replaces any previous CA list and creates a new one that includes this CA only.
   - **-install_add <name/path of the CA certificate file>.** Adds the new CA to the existing CA list.

   > **Note:**
   >
   > - The `-install` and `-install_add` options install the certificate file only. Keep the private key file in a safe place and use it only for issuing certificates.
   > - If your load generator is over firewall, install the CA on the MI Listener machine.

3. Create a Client Certificate

   > **Note:** This step describes how to create a client certificate using the **gen_cert.exe** utility. If you are working on a Linux platform, use the **gen_cert** utility instead.

   On one of your LoadRunner Enterprise hosts, run the **gen_cert** command from the **<LoadRunner Enterprise host root folder>\bin** folder with at least one of the following options:

     - -country_name
     - -organization_name
     - -organization_unit_name
     - -eMail
     - -common_name

   It is important to note the following:

   - The CA Certificate and the CA Private Key files are necessary for the creation of the certificate. By default, it is assumed that they are in the current folder, and are named **cacert.cer** and **capvk.cer** respectively. In any other case, use the **-CA_cert_file_name** and **-CA_pk_file_name** options to give the correct locations.
   - The certificate file is created in the folder from which the utility was run. By default, the file name is **cert.cer**.

4. Install a Client Certificate

   You need to install the client certificate on the hosts that you want to enable TLS including LoadRunner Enterprise hosts (used as Controllers), LoadRunner Enterprise servers, Load Generators, and MI Listeners.

   Run the **gen_cert** utility from the **<LoadRunner Enterprise host root folder>\bin** folder with the following parameter:

   ```
   -install <name/path of the client certificate file>
   ```

   > **Note:**
   >
   > - Steps 3 and 4 describe how to install the same client certificate. Alternatively, you can create a new client certificate on each machine.
   > - Make sure the certificate files within the **<installation root>\dat\cert** folder have the exact names of **cert.cer** and **verify\cacert.cer**, no matter if they are the default ones provided as part of the installation, or if they are your company certificates.

5. On the load generator machines, open LoadRunner Enterprise Agent Configuration and click **OK** to restart the agent configuration. On the MI Listener machines, open Agent Configuration and click **OK** to restart the agent configuration.

Enable TLS communication for load generators in LoadRunner Enterprise Administration

1. Log onto LoadRunner Enterprise Administration. For details, see "Log on to LoadRunner Enterprise Administration" on page 73.
2. On the LoadRunner Enterprise Administration sidebar, under **Maintenance** select **Hosts**.
3. Under the **Host Name** column, click the name of an existing host or load generator over a firewall host.

   Alternatively, click **New Testing Host** + to create a new host.
4. In the Host Details or New Host page, select **Enable SSL**.

Working with firewalls

Using firewalls

You can set up your LoadRunner Enterprise system to run Vusers and monitor servers over a firewall.

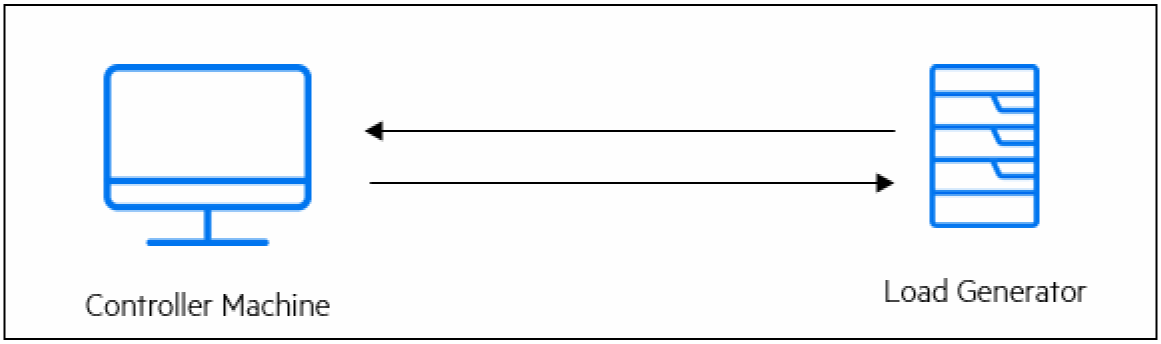
This chapter includes:

About using firewalls in LoadRunner Enterprise

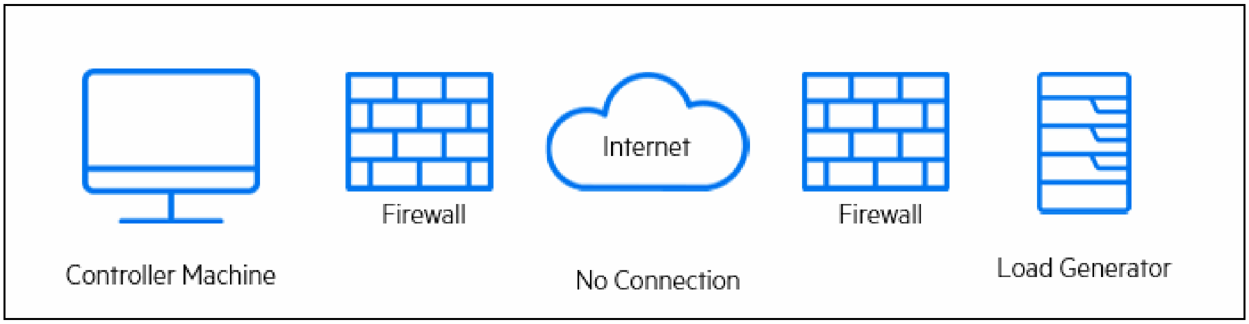
Working with a firewall means that you can prevent unauthorized access to or from a private network, on specific port numbers.

For example, you can specify that no access is allowed to any port from the outside world, with the exception of the mail port (25), or you can specify that no outside connection is allowed from any ports to the outside except from the mail port and WEB port (80). The port settings are configured by the system administrator.

In a regular performance test (not over a firewall), the Controller has direct access to the LoadRunner Enterprise agents running on remote machines. This enables the Controller to connect directly to those machines.



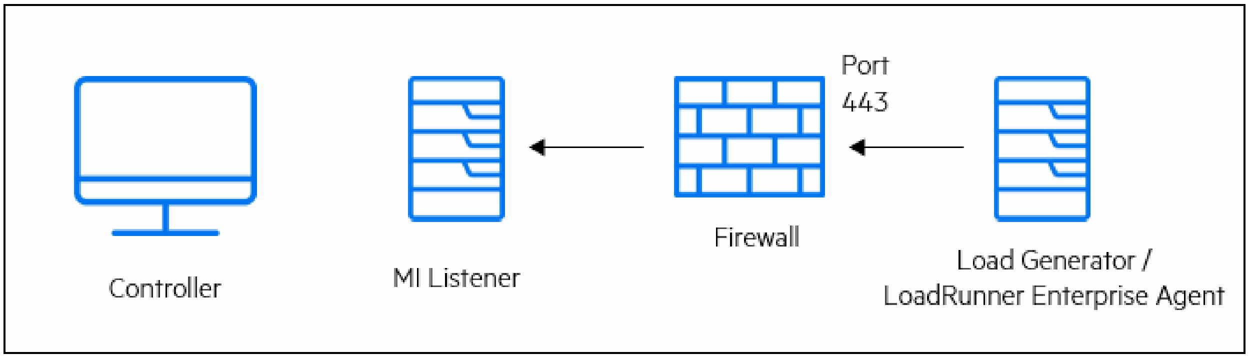
When running Vusers or monitoring applications over a firewall, this direct connection is blocked by the firewall. The connection cannot be established by the Controller, because it does not have permissions to open the firewall.



LoadRunner Enterprise solves this problem by using secure TCP over proxy. This communication is secure by using TLS (formerly SSL). For details on communication over proxy, see "Set up your deployment (TCP or TCP over proxy)" on page 128.

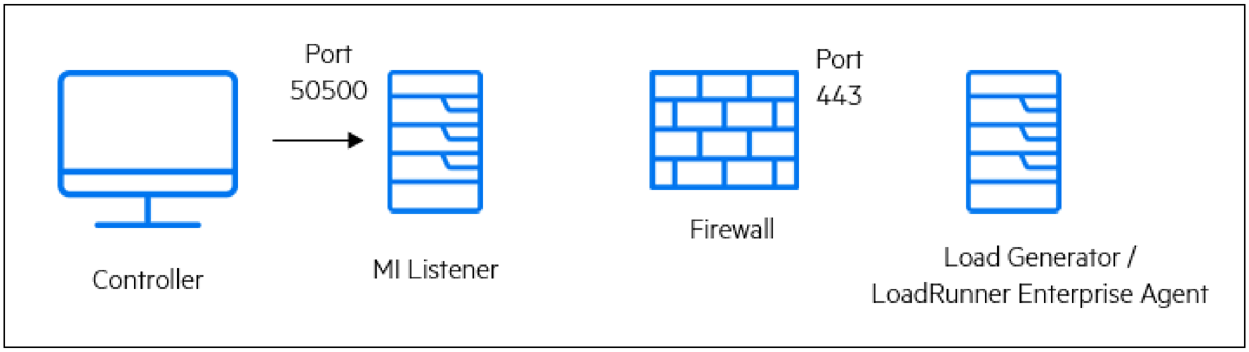
LoadRunner Enterprise agent is already installed on load generators (running Vusers over a firewall), and on Monitor Over Firewall machines (that monitor the servers that are located over a firewall). The agent communicates with the MI Listener machine on port 443.

The MI Listener is a component that serves as router between the Controller and the LoadRunner Enterprise agent.

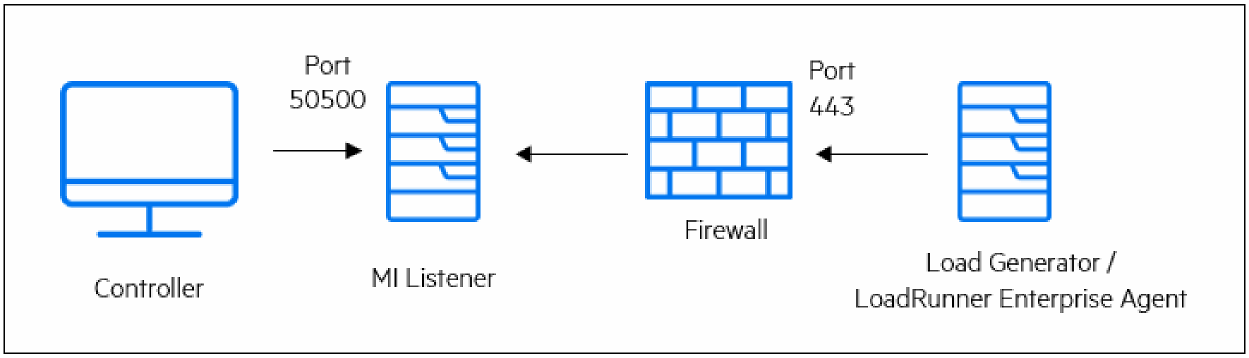


When the LoadRunner Enterprise agent connects to the MI Listener, the MI Listener keeps a listing of the connection to the agent using a symbolic name that the agent passed to it.

When the Controller connects to the MI Listener, it communicates to the MI Listener on port 50500.

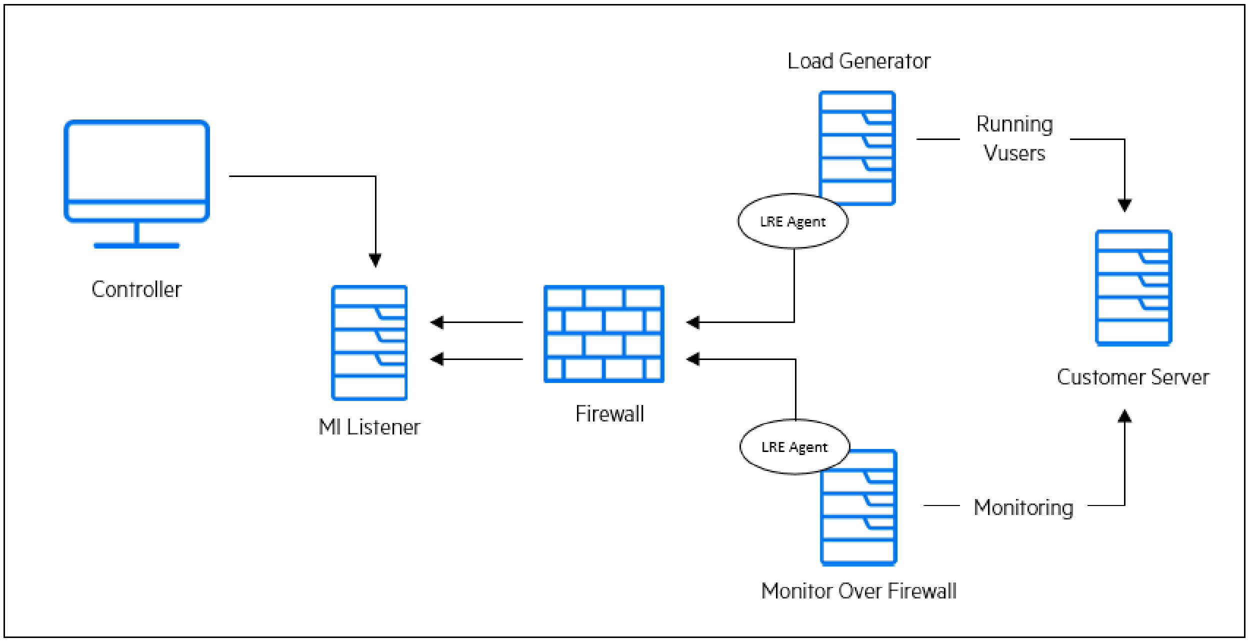


The Controller uses a symbolic name for the agent, and provides the MI Listener machine's name. If there has been a connection from the agent with the same symbolic name to this MI Listener, the connection is made between the Controller and the agent. After you have a connection with the agent, you can run Vusers over firewall or monitor AUT machines behind the firewall.



Example of over firewall deployment

The following diagram is a basic example of a LoadRunner Enterprise deployment over a firewall.



As explained in the previous section, the LoadRunner Enterprise agent is installed on both the load generator machine and the Monitor Over Firewall machine. During installation, the LoadRunner Enterprise agent is added as a Windows service.

The MI Listener serves as a router between:

- The agent on the load generator machine and the Controller, enabling the Controller to run Vusers over a firewall.
- The agent on the Monitor Over Firewall machine and the Controller, enabling the Controller to monitor the servers that are located over a firewall.

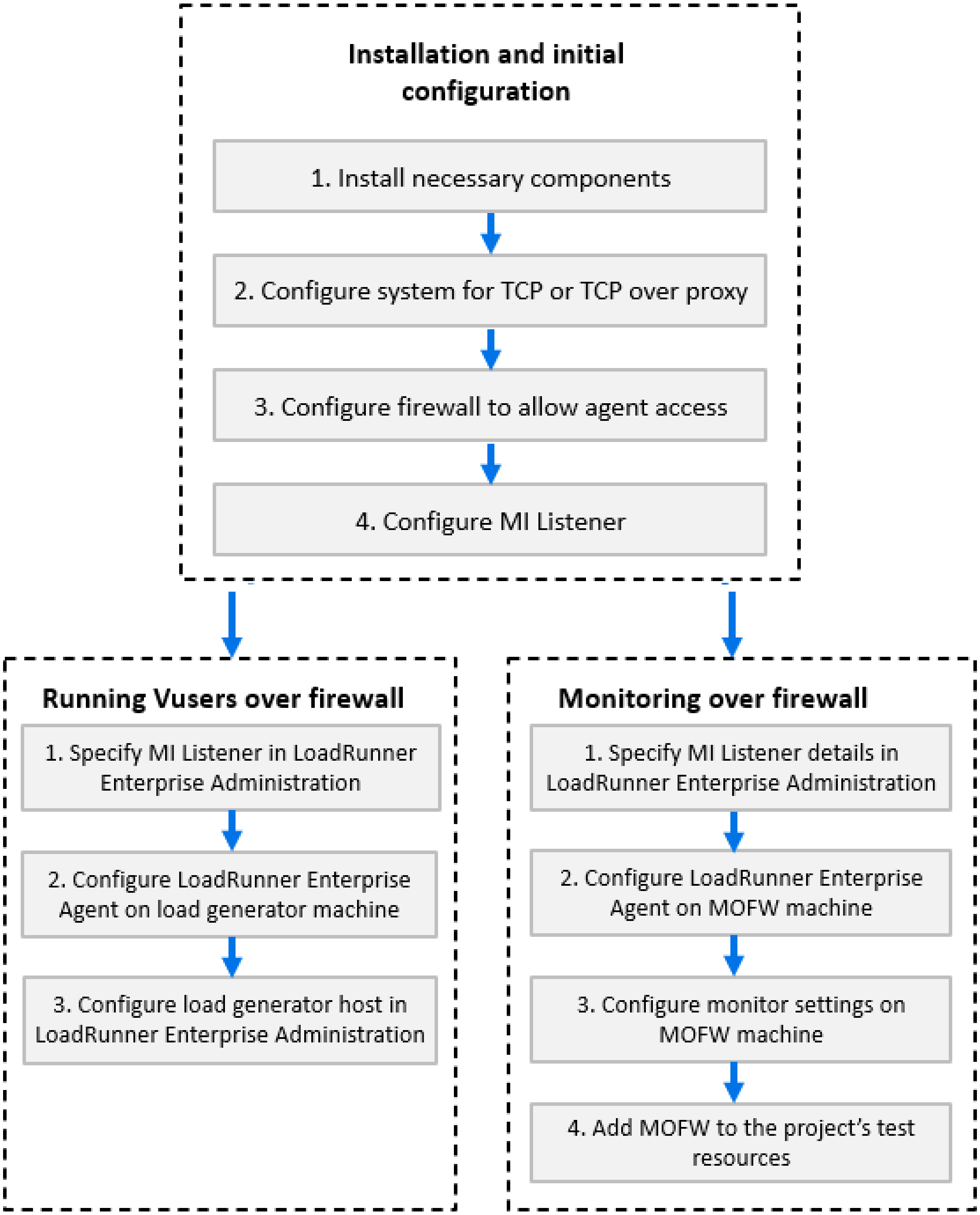
Set up the system to use firewalls: basic steps

Setting up the system to use firewalls involves the following stages of configuration:

Stage	Description
Installation and initial configuration	Install the necessary components and perform initial configuration settings. For details, see "Install over firewall components" on page 127, and "Initial configuration of the over firewall system" on page 128.
Enabling running Vusers over a firewall	When there is a firewall between the Controller and load generator host machines, set up the system to run Vusers over the firewall. For details, see "Run Vusers over a firewall" on page 133.

Stage	Description
Enabling monitoring over a firewall	Set up your system to monitor the application under test (AUT) when there is a firewall between the Controller and the AUT. For details, see "Monitor over a firewall" on page 138.
Checking Connectivity	After installing and configuring all the necessary components, check that you are able to establish a connection between the LoadRunner Enterprise agent, the MI Listener, and the Controller machine. For details, see "Check connectivity" on page 150.

The following flow chart provides a general outline of the steps that you need to perform to set up your system to work with firewalls.


Installation and initial configuration
1. Install necessary components
2. Configure system for TCP or TCP over proxy
3. Configure firewall to allow agent access
4. Configure MI Listener
Running Vusers over firewall
1. Specify MI Listener in LoadRunner Enterprise Administration
2. Configure LoadRunner Enterprise Agent on load generator machine
3. Configure load generator host in LoadRunner Enterprise Administration
Monitoring over firewall
1. Specify MI Listener details in LoadRunner Enterprise Administration
2. Configure LoadRunner Enterprise Agent on MOFW machine
3. Configure monitor settings on MOFW machine
4. Add MOFW to the project's test resources

Install over firewall components

To enable over firewall communication, ensure that you have installed the following LoadRunner Enterprise components:

Component	Description
MI Listener	Serves as a router between the Controller and the LoadRunner Enterprise agent. You install the MI Listener component on a dedicated machine. For installation instructions, see "Install standalone components (Windows)" on page 84. For instructions on configuring the MI Listener machine, see "Configure the MI Listener" on page 130.
Monitor Over Firewall component	Used to monitor the servers that are located over a firewall. You install the Monitors over Firewall component on a dedicated machine. For installation instructions, see "Install standalone components (Windows)" on page 84. For information about configuring the Monitor Over Firewall machine, see "Monitor over a firewall" on page 138.

Initial configuration of the over firewall system

After you have installed the necessary components, you are ready to configure your over firewall system.

To perform initial configuration of your over firewall system:

1. **Configure the system according to TCP or TCP over proxy.**

   See "Set up your deployment (TCP or TCP over proxy)" below.

2. **Modify the firewall settings to enable communication between the machines on either side of the firewall.**

   See "Configure the firewall to allow agent access" on page 130.

3. **Configure the MI Listener.**

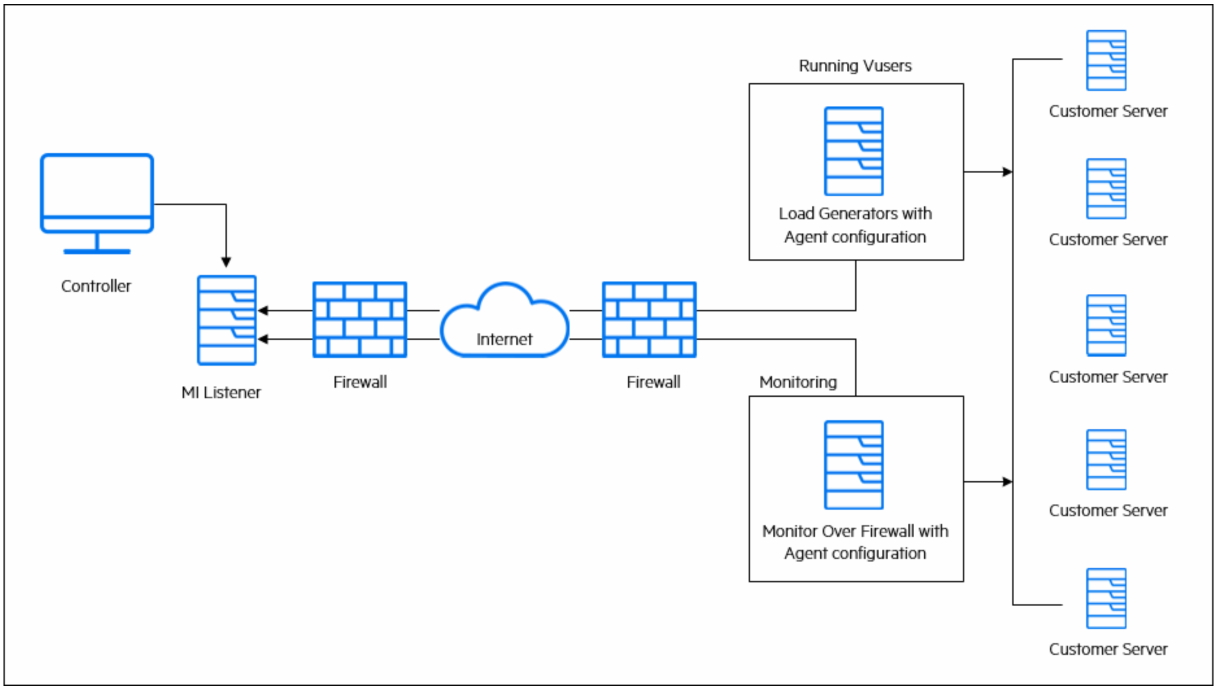
   See "Configure the MI Listener" on page 130.

Set up your deployment (TCP or TCP over proxy)

To run Vusers or monitor servers over the firewall, configure your system according to one of the following configurations. Note that these configurations contain a firewall on each LAN. There may also be configurations where there is a firewall for the Over Firewall LAN only.

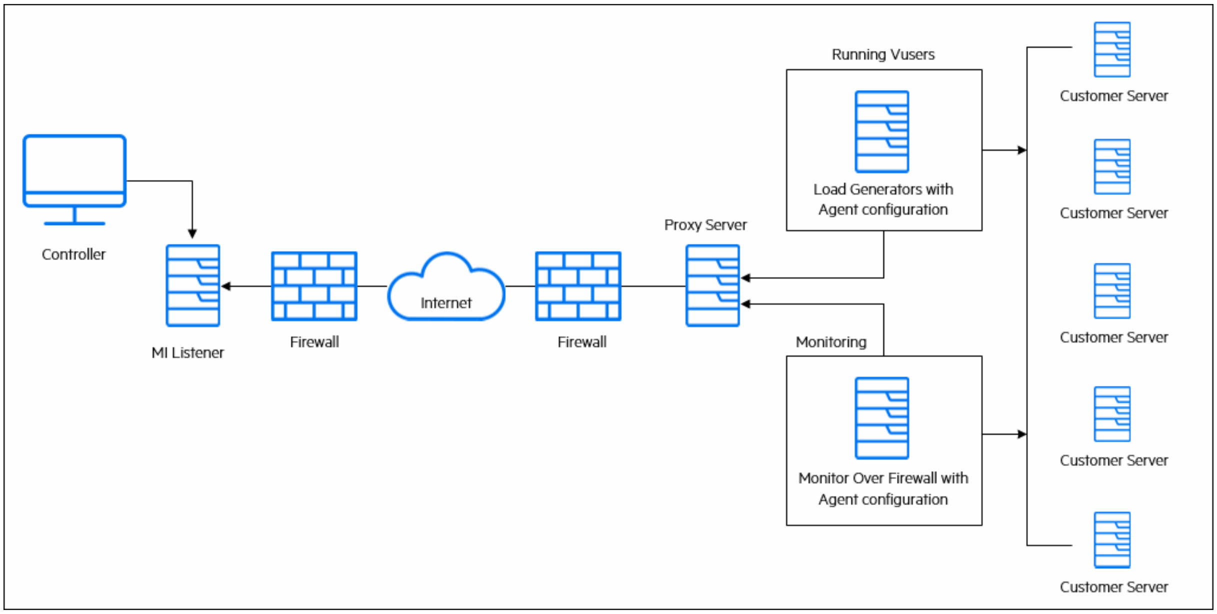
- **TCP configuration**

  The TCP configuration requires every LoadRunner Enterprise agent machine behind the customer's firewall to be allowed to open a port in the firewall for outgoing communication.



- **TCP over proxy configuration**

  In the TCP over proxy configuration, only one machine (the proxy server) is allowed to open a port in the firewall. Therefore it is necessary to tunnel all outgoing communications through the proxy server. The proxy server must support HTTP tunneling using the CONNECT method.



Configure the firewall to allow agent access

You modify your firewall settings to enable communication between the machines inside the firewall and machines outside the firewall.

TCP configuration

The LoadRunner Enterprise agent attempts to establish a connection with the MI Listener using port 443, at intervals specified in the Connection Timeout field in the Agent Configuration dialog box. To enable this connection, allow an outgoing connection on the firewall for port 443. The agent initiate the connection and the MI Listener communicates with the Load Generator through the connection.

TCP over proxy configuration

The LoadRunner Enterprise agent attempts to establish a connection with the MI Listener, using the proxy port specified in the Proxy Port field, and at intervals specified in the Connection Timeout field in the Agent Configuration dialog box. When the connection to the proxy server is established, the proxy server connects to the MI Listener. To enable this connection, allow an outgoing connection on the firewall for port 443. The proxy server can then connect to the MI Listener, and the MI Listener can connect back to the agent through the proxy server. From this point on, the agent listens to commands from the MI Listener.

Local System account configuration

If you intend to start the LoadRunner Agent Service from the Local System account, you need to grant it permissions. If you do not provide permissions, the monitor graph will not display any data.

To grant it permissions, add a local user on the AUT machine with the same name and password as the local user on Agent machine. Add the AUT local user to the Performance Monitor Users group and restart the Agent process.

Configure the MI Listener

To enable running Vusers or monitoring over a firewall, you need to install the MI Listener on one or more machines in the same LAN as the Controller outside the firewall. For installation instructions, see, "Install standalone components (Windows)" on page 84.

To configure the MI Listener:

1. On the MI Listener server, open port 443 for the incoming traffic.
2. Select **Start > Administrative Tools > Services**, and stop **LoadRunner Agent Service**.
3. Select **Start > All Programs > Micro Focus > LoadRunner > Advanced Settings > MI Listener Configuration**, or run

   ```
   <LoadRunner root folder>\launch_service\bin\MILsnConfig.exe
   ```

4. Set each option as described in the following table:

Option	Description
Check Client Certificates	Select **True** to request that the client send a TLS/SSL certificate when connecting, and to authenticate the certificate. **Default value:** False
Private Key Password	The password that may be required during the TLS/SSL certificate authentication process. **Default value:** none

Click **OK** to save your changes or **Use Defaults** to use the default values.

5. Select **Start > Administrative Tools > Services**. To restart the LoadRunner Agent Service, select **Start > All Programs > Micro Focus > LoadRunner > Advanced Settings > Agent Service**.
6. Make sure that no Web Servers are running on the MI Listener or Monitor over Firewall machine. These servers use port 443 and will not allow the access required by the listening and monitoring processes

Specify MI Listeners

In LoadRunner Enterprise Administration, you specify one or more MI Listeners to enable running Vusers or monitoring data over a firewall.

To add an MI Listener:

1. On the LoadRunner Enterprise Administration sidebar, under **Maintenance > Hosts**, select **MI Listeners**.
2. In the MI Listeners tab, click the **Add New MI Listener** + button. The New MI Listener page opens.

3. Enter the following details:

Field	Description
MI Listener Name	The host name of the MI Listener. **Note:** If you have two different IP addresses for the same MI Listener—one for internal communication with the Controller and a second for public communication with a Load Generator located over a firewall—enter the **internal IP address** here. Enter the public IP address in the **Public IP** field (see below).
Description	A description of the MI Listener.
Public IP	The public IP address of the MI Listener. **Note:** If you have two different IP addresses for the same MI Listener, one for public communication with a Load Generator located over a firewall and a second for internal communication with the Controller, enter the public IP address here. Enter the **internalIP address** in the **MI Listener Name** field (see above).
Purpose	The role designated to the MI Listener: • Monitoring over a firewall • Running Vusers over a firewall

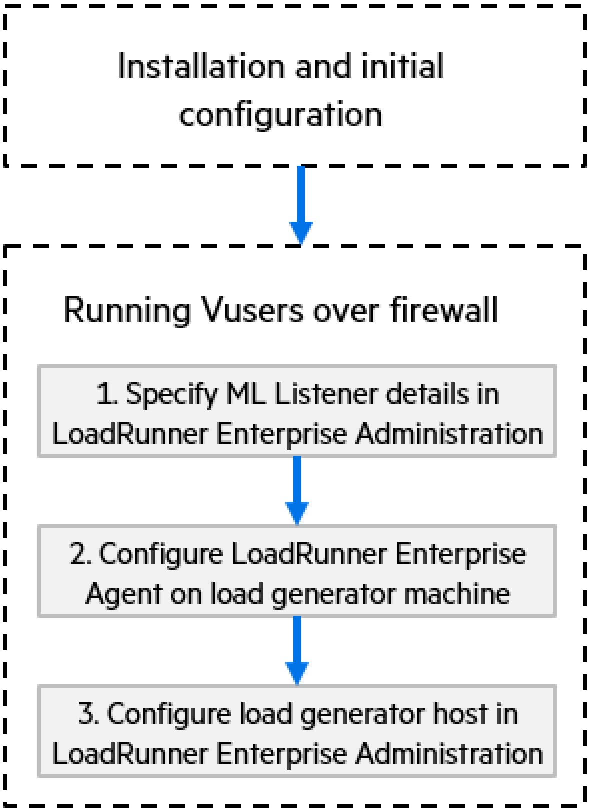
4. Click **Save**. The MI Listener is added to the grid.

Run Vusers over a firewall

You can set up LoadRunner Enterprise to run Vusers over a firewall.

This chapter includes:

Run Vusers over a firewall: basic steps


Installation and initial configuration
Running Vusers over firewall
1. Specify ML Listener details in LoadRunner Enterprise Administration
2. Configure LoadRunner Enterprise Agent on load generator machine
3. Configure load generator host in LoadRunner Enterprise Administration

> **Note:** Before you configure your system to run Vusers over the firewall, ensure that you have completed the configuration steps described in "Initial configuration of the over firewall system" on page 128.

To run Vusers over a firewall:

1. In LoadRunner Enterprise Administration, specify the details of the MI Listener that will be used to run Vusers over the firewall. For details, see "Specify MI Listeners" on page 131.
2. Configure the LoadRunner Enterprise agent on each Load Generator machine that will run over a firewall to communicate with the MI Listener.

   For information on how to configure the LoadRunner Enterprise agent, see "Configure the LoadRunner Enterprise agent" on page 145.

   > **Note:** After you configure the LoadRunner Enterprise agent on the Load Generator machine, you can edit the configuration settings from LoadRunner Enterprise Administration. For details, see Manage hosts in the LoadRunner Enterprise Help Center.

3. In LoadRunner Enterprise Administration, configure the relevant Load Generator hosts to run over a firewall. For details, see "Configure hosts to run Vusers over a firewall" below.

Configure hosts to run Vusers over a firewall

To use a LoadRunner Enterprise host to run Vusers over a firewall, you need to configure the relevant hosts as Load Generators in LoadRunner Enterprise Administration.

Part of the process of configuring a LoadRunner Enterprise host involves selecting a location for your host. For example, locations can be defined according to physical areas. The location also determines whether the host is located over a firewall.

Before you configure the host, you need to ensure that you have added a location over a firewall. When you are configuring a host to operate over a firewall, you select a location that is located over a firewall.

This section describes the basic steps of how to add a host as a Load Generator for running Vusers over a firewall. For detailed information about adding hosts in LoadRunner Enterprise, refer to the LoadRunner Enterprise Administration Guide.

To configure a host to run Vusers over a firewall:

1. **Add the location that is over a firewall.**
   a. In LoadRunner Enterprise Administration, select **Maintenance > Hosts** and click the **Locations** tab.
   b. Click **Add New Location** +. The New Location dialog box opens.
   c. Enter the following details:

Field	Description
Location Name	The name of the host location. The name should have a logical connection to the host location.
Description	A description of the host location.
Over Firewall	Indicates whether the host location is over a firewall.

2. **Add the over firewall host.**
   a. On the LoadRunner Enterprise Administration sidebar, select **Maintenance > Hosts**.
   b. Select the **Hosts** tab, and then click **Create New Host** +.
   c. In the New Host dialog box, enter the following details:

Field	Description
Host Name	The fully qualified domain name or IP address of the host that is assigned when creating the host.
Description	A description of the host.
Purpose	Select a purpose for the host. Note that a host over a firewall can only have a Load Generator purpose.
Source	Select the host's source: **Local** if the host exists in your testing lab, or **Cloud** if the host was provisioned from a cloud provider.
Priority	A rank assigned to the host. The higher the priority you give the host, the more likely the host will be allocated to a test. There are a number of criteria to consider when assigning priority. The main considerations are whether the host is a dedicated machine or a shared resource, and the type of hardware installed on the machine.
Status	Indicate the current status of the host.
Location	The location of the host that is over the firewall.
Installation	Select the installation type of the host. For a standalone installation of the Load Generator, select **OneLG**.
MI Listener	Enter the IP address or host name of the MI Listener that enables data collection.
Enable SSL	Indicates whether the Load Generator is to communicate with the Controller via TLS (formerly SSL) or not. This option is available when the load generator is located over a firewall. **Note:** The load generator uses TLS to communicate with the Controller during runtime only. For non runtime functionality (including collating results), the Load Generator does not use Tas the communication protocol.
Belongs to Pools	The host pools to which the host is assigned. Host pools enable you to control which hosts are allocated to which projects.

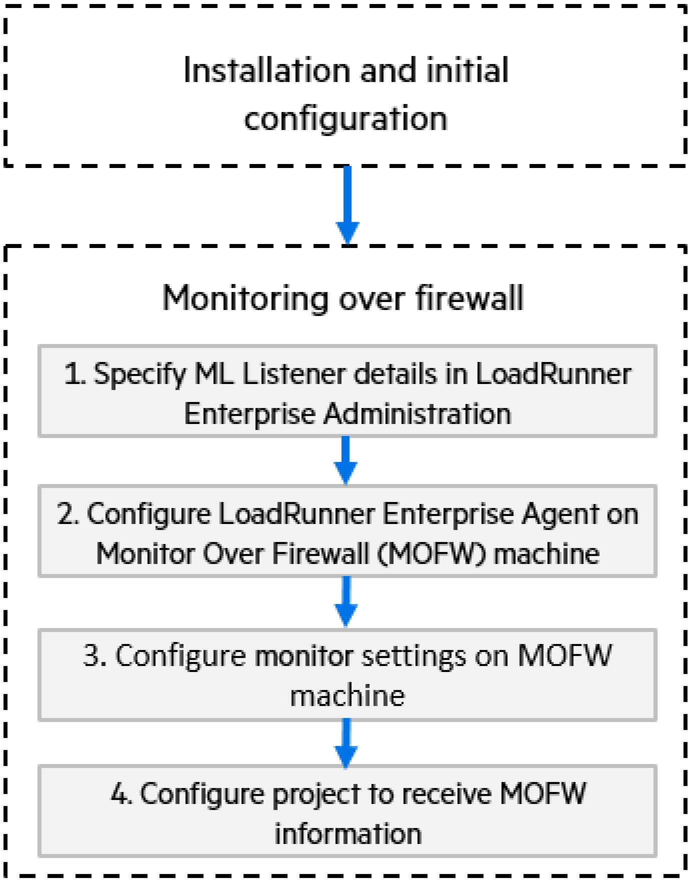
Field	Description
Host Attributes	Attributes of the host. **Example:** Memory, strength, installed components

Monitor over a firewall

You can set up LoadRunner Enterprise to monitor servers over a firewall.

This chapter includes:

Monitor over a firewall: basic steps


Installation and initial configuration
Monitoring over firewall
1. Specify ML Listener details in LoadRunner Enterprise Administration
2. Configure LoadRunner Enterprise Agent on Monitor Over Firewall (MOFW) machine
3. Configure monitor settings on MOFW machine
4. Configure project to receive MOFW information

> **Note:** Before you configure your system to monitor servers over a firewall, ensure that you have completed the configuration steps described in "Initial configuration of the over firewall system" on page 128.

To set up your system to monitor servers over a firewall:

1. In LoadRunner Enterprise Administration, specify the details of the MI Listener that will be used to monitor servers over the firewall. For details, see "Specify MI Listeners" on page 131.
2. Configure the LoadRunner Enterprise agent on each Monitor Over Firewall machine to communicate with the MI Listener.

   For details, see "Configure the LoadRunner Enterprise agent" on page 145.

3. Use the Monitor Configuration tool to configure the servers to monitor and define specific measurements that LoadRunner Enterprise collects for each monitored server.

   For details, see "Configure monitor settings" on the next page.

4. In the relevant project, establish a connection between the tests you are running and the Monitor Over Firewall machines.

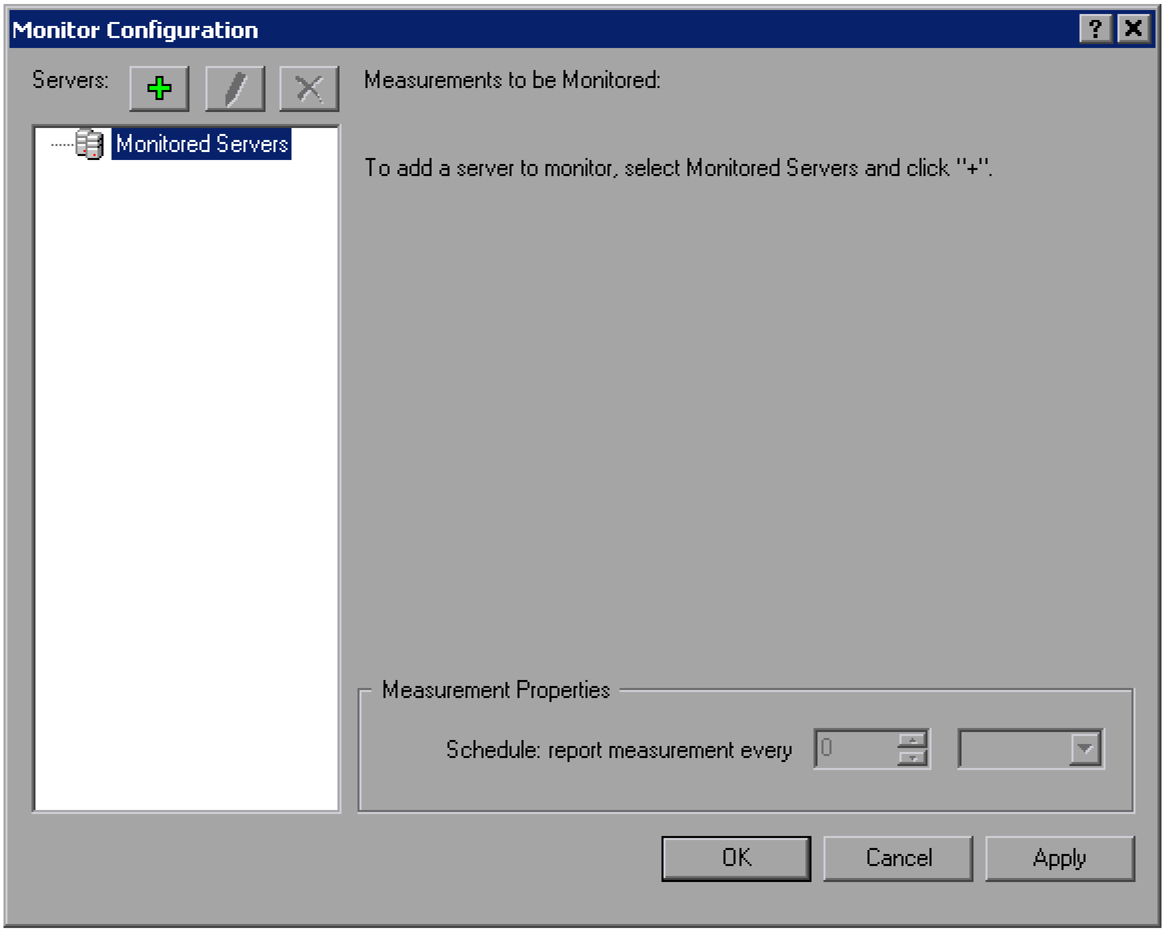
   For details, see "Configure the project to receive monitor over firewall information" on page 143.

Configure monitor settings

You configure the monitor settings from the Monitor Over Firewall machine, using the Monitor Configuration tool. You select the type of monitors to run and the server whose resources you want to monitor, add the measurements to monitor for each server, and specify the frequency at which the monitored measurements are to be reported.

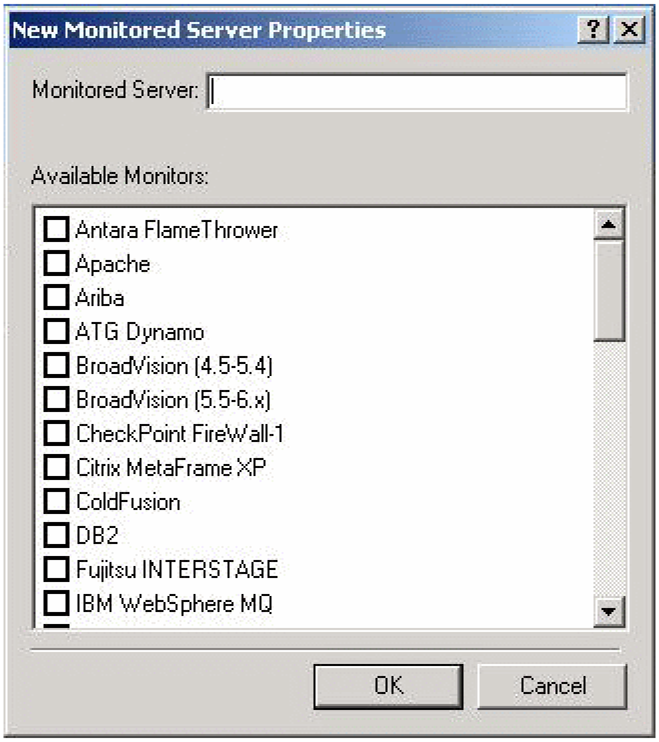
To configure monitor settings:

1. On the Monitor Over Firewall machine, choose **Start > Programs > Micro Focus > LoadRunner > Advanced Settings > Monitor Configuration**. For machines without the complete LoadRunner Enterprise installation, choose **Start > Programs > Server Monitor > Monitor Configuration.** The Monitor Configuration dialog box opens.



To add a server to monitor, select Monitored Servers and click "+".

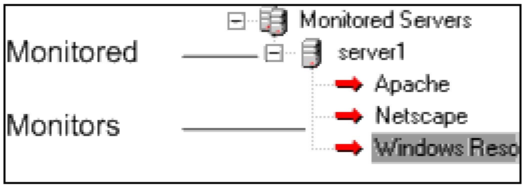
2. Click the **Add Server** button ✚. The New Monitored Server Properties dialog box opens.



3. In the **Monitored Server** box, type the name or IP address of the server whose resources you want to monitor.

> **Note:** To add several servers simultaneously, you can specify IP ranges, or separate the server names or IP ranges with commas. For example, `255.255.255.0-255.255.255.5`, or `server1, server2`.

4. From the **Available Monitors** list, select the monitors suitable for the server being monitored.
5. Click **OK** to close the New Monitored Server Properties dialog box. The Monitored Servers list is displayed in the Monitor Configuration dialog box.



Default measurements are displayed for some of the monitors in the Measurements to be Monitored section. You can specify the frequency at which to report the measurements in the Measurement Properties section.

6. To add additional monitored servers to the list, repeat the steps above.
7. To edit the monitor configuration properties for a server, click the **Edit** button . The Monitored Server Properties dialog box opens enabling you to edit the monitors for the server

whose resources you are monitoring.

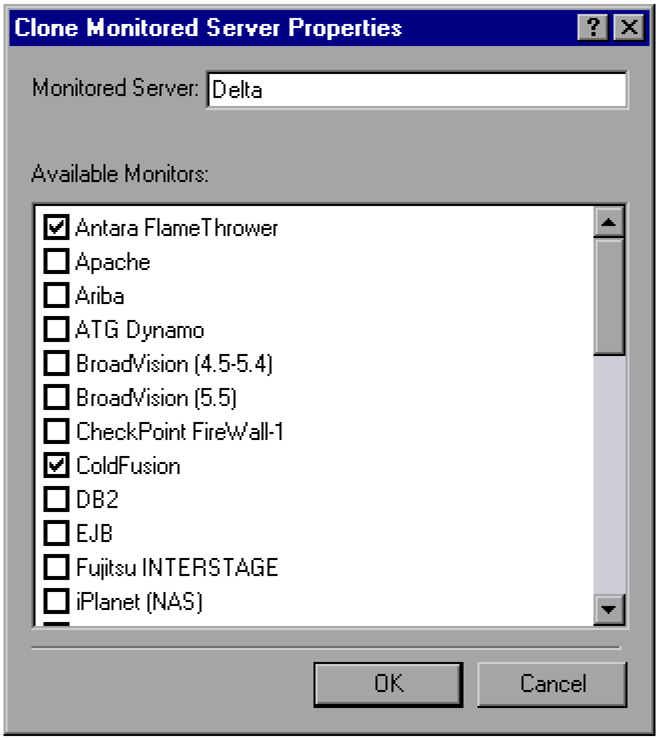
8. Click **Apply** to save your settings.

Clone a monitored server's properties

To monitor the same properties on different server machines, you can clone a selected server's properties using the Clone Monitored Server Properties dialog box.

To clone a monitored server's properties:

1. Open the Monitor Configuration dialog box.
2. Right-click the server you want to clone, and select **Clone**. The Clone Monitored Server Properties dialog box opens.



Clone Monitored Server Properties

Monitored Server: Delta

Available Monitors:

☑ Antara FlameThrower
□ Apache
□ Ariba
□ ATG Dynamo
□ BroadVision (4.5-5.4)
□ BroadVision (5.5)
□ CheckPoint FireWall-1
☑ ColdFusion
□ DB2
□ EJB
□ Fujitsu INTERSTAGE
□ iPlanet (NAS)

3. In the **Monitored Server** box, type the name or IP address of the cloned server you want to create.

> **Tip:** To create several cloned servers simultaneously, you can specify IP ranges, or separate the server names or IP ranges with commas. For example, `255.255.255.0-255.255.255.5`, or `server1, server2`.

4. The **Available Monitors** list displays the monitors that were selected for the server being cloned. Select additional suitable monitors for the cloned server.
5. Click **OK** to close the Clone Monitored Server Properties dialog box. The cloned server is displayed in the Monitored Servers list.
6. Click **Apply** to save your settings.

Add and remove measurements

After you configure one or more server machines to monitor, you add measurements to monitor for each server. If LoadRunner Enterprise added default measurements, you can edit them as required.

To add a measurement to monitor:

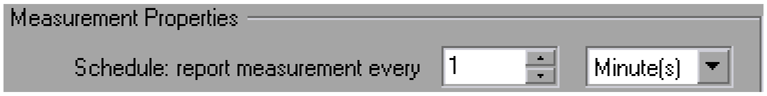
1. Open the Monitor Configuration dialog box.
2. Select a server from the Monitored Servers list.
3. Click the **Add Measurement** button ✚. Select the appropriate monitor. A dialog box opens, enabling you to choose measurements for the monitor you selected.
4. Select the measurements that you want to monitor, and click **OK**.
5. Click **Apply** to save your settings.

To remove a measurement from the measurements list:

1. Select the measurement, and click the **Delete** button ✕.
2. Click **Apply** to save your settings.

Configure measurement frequency

After you have configured monitor measurements, you set a schedule for reporting each measurement.



Measurement Properties

Schedule: report measurement every 1 Minute(s)

To configure measurement frequency:

1. In the Monitor Configuration dialog box, under the **Measurement Properties** section, select the configured server measurement you want to schedule.
2. Specify the frequency at which you want LoadRunner Enterprise to report the measurement.
3. Click **Apply** to save your settings.

Configure the project to receive monitor over firewall information

After you configure the monitors, you configure the project to receive Monitor Over Firewall information during performance test runs.

> **Note:** The steps in the section are described in more detail in the section about monitor profiles in the LoadRunner Enterprise User Guide.

To configure the project to receive Monitor Over Firewall information:

1. Add a monitor over firewall which can be accessed by performance tests in this project.
   a. From the LoadRunner Enterprise navigation toolbar, click ≡ and select **Monitors** (under **Assets**).
   b. Click **New Monitor Over Firewall**.
   c. Enter a name, the machine key, and select the MI Listener with which the monitor is to connect.
2. Select the Monitor Over Firewall agent to use in a specific performance test.
   a. In the Test Plan module, select a performance test, and click **Edit Test** to open the test in the Performance Test Designer window.
   b. In the Monitors tab, select the Monitor Over Firewall agent.

Edit monitor over firewall machines during a test run

While a performance test is running, you can change the status of a Monitor Over Firewall agent or add another monitor to the test.

To modify the Monitor Over Firewall machines:

1. On the Test Run page, click the **Monitors** button ▾ and select **Monitors Over Firewall**. The Monitors Over Firewall dialog box opens.
2. You can view the Monitor Over Firewall agents that are monitoring the test, as well as their connection status.
   - To connect or disconnect a Monitor Over Firewall agent, click the **Connect/Disconnect** button.
   - To add a Monitor Over Firewall agent to the test, select it from the **Add Monitor Over Firewall** list.

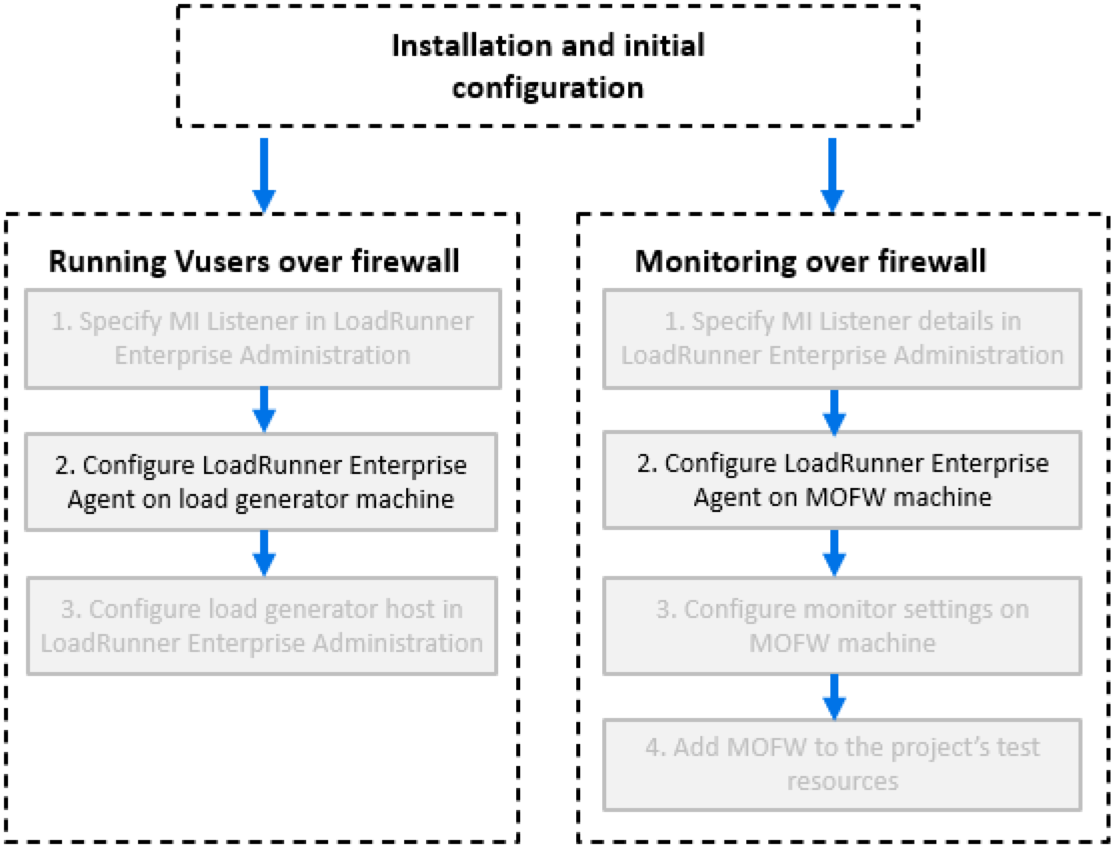
Configure the LoadRunner Enterprise agent

You can set up your LoadRunner Enterprise system to run Vusers and monitor servers over a firewall. As part of the process of setting up your LoadRunner Enterprise system to work over firewalls, you configure the LoadRunner Enterprise agent.

This chapter includes:

Configure LoadRunner Enterprise agents over the firewall: basic steps

For LoadRunner Enterprise to work over firewalls, you need to configure the LoadRunner Enterprise agent on each Load Generator machine that will be running over a firewall and on each Monitor Over Firewall machine.


Installation and initial configuration
Running Vusers over firewall
1. Specify MI Listener in LoadRunner Enterprise Administration
2. Configure LoadRunner Enterprise Agent on load generator machine
3. Configure load generator host in LoadRunner Enterprise Administration
Monitoring over firewall
1. Specify MI Listener details in LoadRunner Enterprise Administration
2. Configure LoadRunner Enterprise Agent on MOFW machine
3. Configure monitor settings on MOFW machine
4. Add MOFW to the project's test resources

You configure the LoadRunner Enterprise agent to communicate with the MI Listener. The MI Listener serves as a router between the LoadRunner Enterprise agent and the Controller.

Configure the Windows LoadRunner Enterprise agent

This section describes how to configure the LoadRunner Enterprise Agent on Windows machines to communicate with the MI Listener.

To configure the LoadRunner Enterprise agent on Windows machines:

1. Select **Start > Programs > Micro Focus > LoadRunner > Advanced Settings > LoadRunner Enterprise Agent Configuration**, or run **<LoadRunner Enterprise root>\launch_service\bin\AgentConfig.exe**.

   The Agent Configuration dialog box opens.

2. Select **Enable Firewall Agent**.
3. Click **Settings**. The Agent Configuration dialog box displays a list of settings.
4. Set each option as described in "Agent configuration settings " on the next page. Pay careful attention to the first three settings.
5. Click **OK** to save your changes.
6. When prompted, click **OK** to restart the LoadRunner Enterprise agent.
7. Check the connection status between the LoadRunner Enterprise agent and the MI Listener.
   a. Change the Agent Runtime settings to run as a process and check the status. For details, see "Run the LoadRunner Enterprise agent as a process" on page 114.
   b. If the status is OK, revert back to running it as a service. For details, see "Run the LoadRunner Enterprise agent as a service" on page 114.

> **Notes:**
>
> - When you configure the LoadRunner Enterprise agent on Windows machines, the Remote Management agent is automatically configured with the same settings. The Remote Management agent enables you to manage remote machines from LoadRunner Enterprise Administration.
> - After you have configured the LoadRunner Enterprise agent on the Load Generator machine, you can edit the configuration settings from LoadRunner Enterprise Administration. For details, see the Help Center.

Configure and run the Linux LoadRunner Enterprise agent

Load Generator hosts can be installed on Linux machines. This section describes how to configure and run LoadRunner Enterprise agents on Linux machines.

> **Note:** As part of the process of configuring the LoadRunner Enterprise Agent on Linux machines, you also need to configure the Remote Management agent. The Remote Management agent enables you to manage remote machines from LoadRunner Enterprise Administration.

To configure the LoadRunner Enterprise Agent on Linux machines:

1. Activate the firewall service for the LoadRunner Enterprise agent:
   a. Open **<LoadRunner Enterprise root folder>/dat/br_lnch_server.cfg** in a text editor.
   b. In the **Firewall** section, set **FireWallServiceActive** to **1** and save your changes.
2. Activate the firewall service for the Remote Management agent:
   a. Open **<LoadRunner Enterprise root folder>/al_agent/dat/br_lnch_server.cfg** in a text editor.

b. In the **Firewall** section, set **FireWallServiceActive** to **1** and save your changes.

3. Run **agent_config** from the **<LoadRunner Enterprise root folder>/bin** directory and enter the agent configuration settings (see "Agent configuration settings " below).

> **Note:** When you set the agent configuration settings, they are applied to both the LoadRunner Enterprise and Remote Management agents.

4. Restart the LoadRunner Enterprise agent for the configuration changes to take effect.
5. Restart the Remote Management agent for the configuration changes to take effect.

a. To stop the Remote Management agent, run the following command from the **<LoadRunner Enterprise root folder>/al_agent/bin** directory:

```
al_daemon_setup -remove
```

b. To start the Remote Management agent, run the following command from the **<LoadRunner Enterprise root folder>/al_agent/bin** directory:

```
al_daemon_setup -install
```

Agent configuration settings

The following table provides an explanation of the agent configuration settings:

Setting	Default Value	Description
MI Listener name	none	The host name, fully qualified domain name, or IP address of the MI Listener.

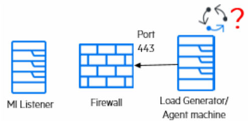
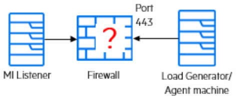
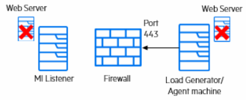
Setting	Default Value	Description
Local Machine Key	none	A symbolic string identifier used to establish a unique connection between the Controller host and the agent machine, via the MI Listener machine. When configuring a Monitor Over Firewall agent, you can enter any logical name, using lowercase letters only. When configuring the agent on a load generator to run Vusers over a firewall, you must use the format `hostname_locationname` where: • `hostname` is the name of the host as found in LoadRunner Enterprise Administration's Hosts page. • `locationname` is the name of the host location as found in LoadRunner Enterprise Administration's Host Locations page.
Connection Timeout (seconds)	20 seconds	The length of time you want the agent to wait before retrying to connect to the MI Listener machine. If zero, the connection is kept open from the time the agent is run.
MI Listener User Name	none	The user name needed to connect to the MI Listener machine.
MI Listener Password	none	The password needed to connect to the MI Listener machine.
Server Domain	none	The domain name needed to connect to the MI Listener machine. This field is required only if NTLM is used.
Connection Type - TCP/HTTP	TCP	Select either **TCP** or **HTTP**, depending on the configuration you are using.

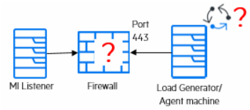
Setting	Default Value	Description
Connection Type - HTTP	none	If you select **HTTP**, configure the following: • **Proxy Name.** The name of the proxy server. The proxy server must support HTTP tunneling using the CONNECT method. This field is mandatory if the **Connection Type** setting is **HTTP**. • **Proxy Port.** The proxy server connection port. This field is mandatory if the **Connection Type** setting is **HTTP**. • **Proxy User Name/Password.** The credentials of a user with connection rights to the proxy server. • **Proxy Domain.** The user's domain if defined in the proxy server configuration. This option is required only if NTLM is used.
Use Secure Connection (SSL)	disabled	Enable to connect using the TLS (formally SSL) protocol. When a proxy server is used, TLS is enabled by default and cannot be disabled. If you enable this option, enter the following information: • **Check Server Certificates.** Authenticates the TLS certificates that are sent by the server. ◦ Select **Medium** to verify that the server certificate is signed by a trusted Certification Authority. ◦ Select **High** to verify that the sender IP matches the certificate information. This setting is available only if **Use Secure Connection** is set to **True**. • **Private Key Password.** The password that might be required during the TLS certificate authentication process. This option is relevant only if the **Client Certificate Owner** option is enabled.

Check connectivity

To run Vusers or monitor servers over a firewall, you must be able to establish a connection between the LoadRunner Enterprise agent, MI Listener, and the Controller machine.

If you encounter connectivity problems after installing and configuring all the necessary components, check the table below for troubleshooting tips.

Check	Solution
To check that the Firewall service was activated on the agent machine:  Port 443 ? MI Listener Firewall Load Generator/ Agent machine	- **Windows Installation:** a. Change the Agent Runtime settings to run as a process and check the status. For details, see "Run the LoadRunner Enterprise agent as a process" on page 114. b. If the status is OK, revert back to running it as a service. For details, see "Run the LoadRunner Enterprise agent as a service" on page 114. Otherwise, you need to reconfigure the LoadRunner Enterprise Agent on your Windows machine. For details, see "Configure the Windows LoadRunner Enterprise agent" on page 146. - **Linux Installation:** In the temporary directory of the LoadRunner Enterprise Agent machine, locate the **<local_machine_key>_connected_to_MI_Listener** file. If the file is missing, this indicates that the **FirewallServiceActive=1** is not set in the [FireWall] section of the Agent Settings. For details, see "Configure and run the Linux LoadRunner Enterprise agent" on page 147.
To check that port 443 is open:  Port 443 ? MI Listener Firewall Load Generator/ Agent machine	On the agent machine, open a command prompt window, and type the following: `telnet <MI_Listener_IP> 443.` **Example:** `telnet 111.111.111.1111 443` If port 443 is open, a new Telnet window opens. If port 443 is not open, contact your network administrator.
To check that port 443 is available:  Web Server Web Server Port 443 MI Listener Firewall Load Generator/ Agent machine	If a web server is running on the MI Listener or Monitor Over Firewall machine, port 443 does not allow the access required by the listening and monitoring processes. Contact your network administrator to change the web server port.

Check	Solution
To check connectivity between the agent and the MI Listener, when running the LoadRunner Enterprise Agent as a service:  Port 443 ? ? MI Listener Firewall Load Generator/ Agent machine	When running the LoadRunner Enterprise Agent as a service, do the following: - Check that port 443 is open. See " To check that port 443 is open: " on the previous page. - Check that the Agent Settings and Agent Configuration are correctly set. For details, see "Configure LoadRunner Enterprise agents over the firewall: basic steps" on page 146. - Run the agent as a process by launching **<Installation>\Launch_service\bin\magentproc.exe**. If you are successful, this indicates an authentication issue with the LoadRunner Agent Service. Browse to the **Administrative Tools > Services > LoadRunner Agent Service** and change the properties of this service to `System User Account`, or provide the username and password of a user who has administrative privileges on this machine.

Troubleshooting

Troubleshooting installation issues

This chapter provides troubleshooting for issues that arise when installing LoadRunner Enterprise components and during initial configuration.

This chapter includes:

Default monitor measurements not displayed in online graphs on OneLG

Problem Description

Default monitor measurements are not displayed in online graphs when using OneLG hosts.

This occurs when LoadRunner Enterprise is configured with a local user.

Troubleshooting

Create a user account on OneLG hosts with the same credentials and permissions as the LoadRunner Enterprise account.

For example, if you used the default local user (IUSR_METRO) on LoadRunner Enterprise servers and hosts, create the IUSR_METRO user and add it to the Administrators group on the OneLG machine.

Unable to load Windows 8 Explorer shell after installing LoadRunner Enterprise host

Problem description

After installing LoadRunner Enterprise host on Windows 8 and rebooting the machine, the Windows Explorer shell fails to load.

Troubleshooting

UAC is enabled on your machine. To disable, perform the following steps:

1. Choose **Start > Run**.
2. To open the registry editor, type `Regedit` in the Run dialog box.
3. Disable UAC and restart your machine. For details on how to disable UAC, see: http://gallery.technet.microsoft.com/Registry-Key-to-Disable-UAC-45d0df25.

Host silent installation stops after installing .NET Framework 4.8

Problem description

Running the Host installation in silent mode using `setup_host.exe /s` fails to complete the installation. The installation process stops after installing .NET Framework 4.8.

Troubleshooting

.NET Framework 4.8 replaces the .NET Framework 4.6.2 and earlier files. If there are any applications that are using the .NET Framework 4.6.2 or earlier files and are running during the installation of .NET Framework 4.8, you may need to restart your machine. If you are prompted to restart the machine, restart it before continuing the installation. For details, see http://msdn.microsoft.com/en-us/library/hh527997%28v=vs.110%29.aspx.

Working with LoadRunner Enterprise when Windows Firewall is enabled

Problem description

To work with LoadRunner Enterprise, we recommend that you disable the Windows Firewall on all host machines. To enable LoadRunner Enterprise to work with the Windows Firewall enabled, the Windows Firewall must be reconfigured.

Troubleshooting

The Windows Firewall must be configured to allow inbound and outbound communication on specific ports used by LoadRunner Enterprise.

The following configurations are required for all LoadRunner Enterprise machines in the system (servers and hosts), except for SiteScope.

LoadRunner Enterprise server:

Process / Service	Direction	Protocol	Local Port	Remote Port	Path
Datacollectionagent.exe	Inbound	TCP	3333	Any	<LoadRunner Enterprise Server install dir>\bin \datacollectionagent.exe
World Wide Web Services (HTTP Traffic-In)	Inbound	TCP	80	Any	Service
LoadRunner Remote Management Agent Service	Inbound	TCP	54245	Any	<LoadRunner Enterprise Server install dir> \al_ agent\bin \alagentservice.exe
ALWrapperServer.exe	Outbound	TCP	Any	54245	<LoadRunner Enterprise Server install dir>\bin \ALWrapperServer.exe
LRECoreAPI.exe	Outbound	TCP	Any	1433, 1521, or 5432 (Use 1433 for MS SQL Server, 1521 for Oracle, and 5432 for PostgreSQL) **Note:** These are the default ports.	
w3wp.exe	Outbound	TCP	Any	8080, 8731, 3333	
		HTTP	Any	8086	

Hosts:

Process / Service	Direction	Protocol	Local Port	Remote Port	Path
Datacollectionagent.exe	Inbound	TCP	3333	Any	<Host install dir>\bin \datacollectionagent.exe
LoadRunner Remote Management Agent Service	Inbound	TCP	54245	Any	<Host install dir> \al_agent\bin \alagentservice.exe
LoadRunner Agent Service	Inbound	TCP	54345, 50500	Any	<Host install dir>\ launch_service \bin\magentservice.exe
System	Inbound	TCP	8731	Any	
Influxdb.exe	Inbound	HTTP	8086	Any	<Host install dir>\bin\influxdb\Influxdb.exe
LTOPSvc.exe	Outbound	TCP	Any	80, 8080	<Host install dir>\bin \LTOPSvc.exe
AnalyticsSvc.exe	Outbound	HTTP	Any	8086	<Host install dir>\bin\AnalyticsSvc.exe

LoadRunner Enterprise uninstall fails or freezes

Problem description

This error may present itself in various ways:

- Uninstall of LoadRunner Enterprise did not complete successfully.
- Uninstall of LoadRunner Enterprise is taking a long time and seems to have frozen.
- When trying to uninstall LoadRunner Enterprise again, LoadRunner Enterprise is not found in Add/Remove Programs.

Troubleshooting

- Reboot the machine and uninstall again (unless LoadRunner Enterprise no longer appears in Add/Remove Programs).
- Alternatively, you can:
  a. Open a command prompt and run:

     <Host installation path>\bin\HP.PC.PCS.Configurator.exe /CFG:..\dat\setup\lts\xml\Configurator.xml /G:Uninstall

  b. Delete **LoadRunner Enterprise Host** from **Start menu > Programs > Micro Focus**.
  c. Delete the product from the MSI manager using the Windows Installer CleanUp Utility (http://www.windows-installer-cleanup-utility.com/).

Cannot log in to LoadRunner Enterprise via the client machine: JavaScript Error

Problem description

Login to LoadRunner Enterprise fails, and the following error is displayed:

JavaScript is not installed or is disabled in your browser.

Troubleshooting

This problem is related to running JavaScript in your browser.

To resolve this issue:

1. In Internet Explorer, select **Tools > Internet options >Security**.
2. Select **Internet zone.**
3. Click **Custom Level**.
4. Make sure that **Active Scripting** is enabled.
5. Enable the following items under **ActiveX controls and Plug-ins**:
   - **Automatic prompting for ActiveX controls**
   - **Binary and script behaviors**
   - **Run ActiveX controls and plugins**
   - **Script ActiveX controls marked safe for scripting**

Initializing Run page does not load when starting a test run

Problem description

When starting a test run, the host is added, but the Initializing Run page does not load.

Troubleshooting

The client machine needs to have access to the machine. For example, if the Administrator inserted the machine name without the domain, you might need to add the IP address and machine name to the host file (C:\WINDOWS\system32\drivers\etc\hosts) on the client machine.

Unable to run the LoadRunner Enterprise component installation from a network drive

Problem description

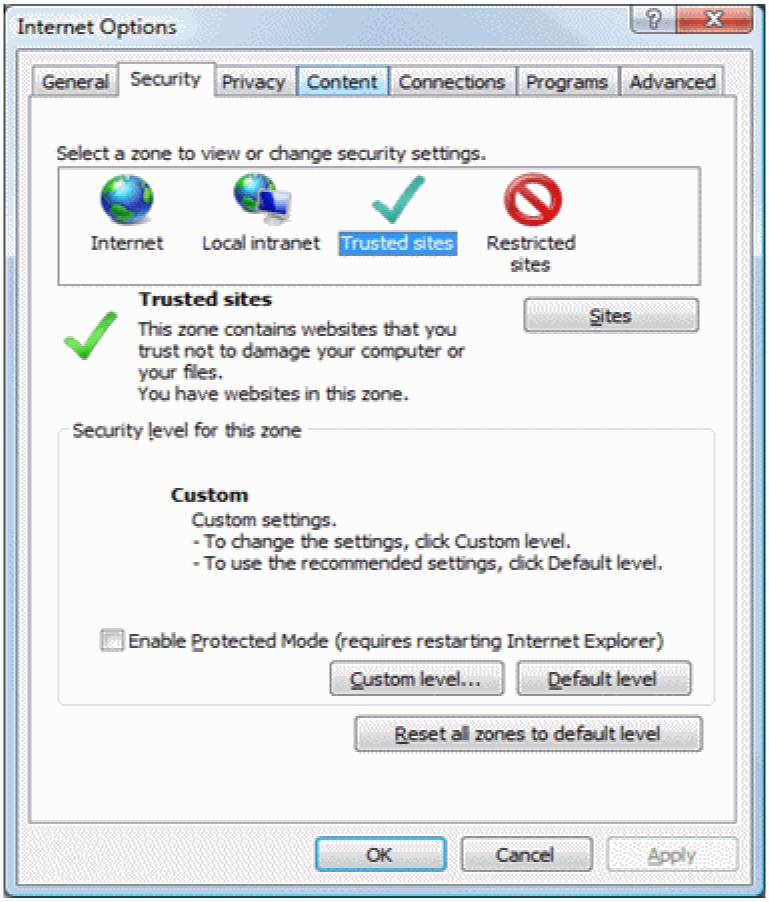
Cannot run the setup (LoadRunner Enterprise server or host) when attempting to run it from a network drive.

Troubleshooting

To run **setup.exe** from a network location, you need to add the network server location to your Trusted Sites, and then run setup.exe again.

To add the network server to your Trusted Sites in Internet Explorer:

1. Open **Tools > Internet Options**.
2. Select the **Security** tab and click **Trusted Sites**:



Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

□ Enable Protected Mode (requires restarting Internet Explorer)

3. Click **Sites**.
4. In the Trusted Sites dialog box, add the location of the network server where the LoadRunner Enterprise component setup file is located, to the list of trusted sites.

Unable to install LoadRunner Enterprise components from the installation directory

Problem description

Nothing happens when clicking the installation option from the LoadRunner Enterprise installation directory.

Troubleshooting

1. Make sure the user running the installation has sufficient permissions to launch executable files.
2. Restart the machine and try again.

Unable to install a LoadRunner Enterprise component if the default port is in use

Problem description

The installation cannot use a default port because it is already in use.

Troubleshooting

If the installation cannot use a default port because it is already in use, change the port as per the instructions in the following table:

Component	How to change the port
LoadRunner Enterprise Server IIS	To change this port, see http://support.microsoft.com/kb/149605.
LoadRunner Enterprise host	To change port 8731 to a different port: 1. On each LoadRunner Enterprise host, open **LTOPSvc.exe.config** (located in **<LRE host Installation directory>\bin\**) and change all four occurrences of **8731** to a new port number. Restart the **LoadRunner Load Testing Service**. 2. On the LoadRunner Enterprise server, open **pcs.config** (located in **<LRE server installation directory>\dat\**). Under **PCSSettings**, change **ltopPortNumber** to the new port number.

Component	How to change the port
MI Listener	To change port 443 to a different port, perform the following steps on the following machines: - Controller machine (if used as MI Listener) - Load Generator machine - MI Listener To change port 443: 1. Open **<Component installation directory>\launch_service\dat\mdrv.dat**. and locate the **[launcher]** section. 2. Add **OFWPort=<port>**, where <port> is the new port number. 3. Go to **<Component installation directory>\launch_service\dat\channel_configure.dat** and locate the **[General]** section. 4. Add **OFWPort=<port>**, where <port> is the new port number. 5. Restart the agent. **Note:** There is no support for changing port 50500.
LoadRunner Agent	Changing the port for a Controller machine: 1. Stop 'LoadRunner Agent Service'. 2. Open for edit the file: <Install folder\dat\merc_agent.cfg 3. Under the [Attributes] section, add the line: "AgentPort=<New Port Value>" 4. Restart the service. Changing the port for a Load Generator machine: 1. Stop 'LoadRunner Agent Service'. 2. Open for edit the file: <Install folder\launch_service\dat\merc_agent.cfg 3. Under the [Attributes] section, add the line: "AgentPort=<New Port Value>" 4. Restart the service.

Component	How to change the port
Autolab Agent (RemoteManagementAgent)	This service is used to perform administration tasks on all LoadRunner Enterprise machines. By default, Autolab Agent is using port 54245. The port number can be changed. However, the new value must be configured on each machine (server, host, Load Generator). To change the port: 1. Stop 'RemoteManagementAgent'. 2. Open <Install folder>\launch_service\al_agent\dat\merc_agent.cfg 3. Under the [Attributes] section, add the line: "AgentPort=<New Port Value>“ 4. Restart the service.
SiteScope (Topology)	In LoadRunner Enterprise, change the port of the Topology entity to the same port as that defined during the SiteScope configuration.
SiteScope (Topology) - SSL	In LoadRunner Enterprise, change the port of the Topology entity to the same port as that defined during the SiteScope configuration.
SiteScope (Monitor Profiles)	In LoadRunner Enterprise, change the port of the Monitor Profile entity to the same port as that defined during the SiteScope configuration.

Unable to use non-default ports in Microsoft SQL

Problem Description

LoadRunner Enterprise does not work on non-default ports in Microsoft SQL.

Troubleshooting

The Microsoft SQL instance must use a static port. The correct port must be defined in the connection string.

LoadRunner Enterprise information displayed in IIS and ASP.NET response headers

Applicable in versions: LoadRunner Enterprise 2021 R2 and later

Problem Description

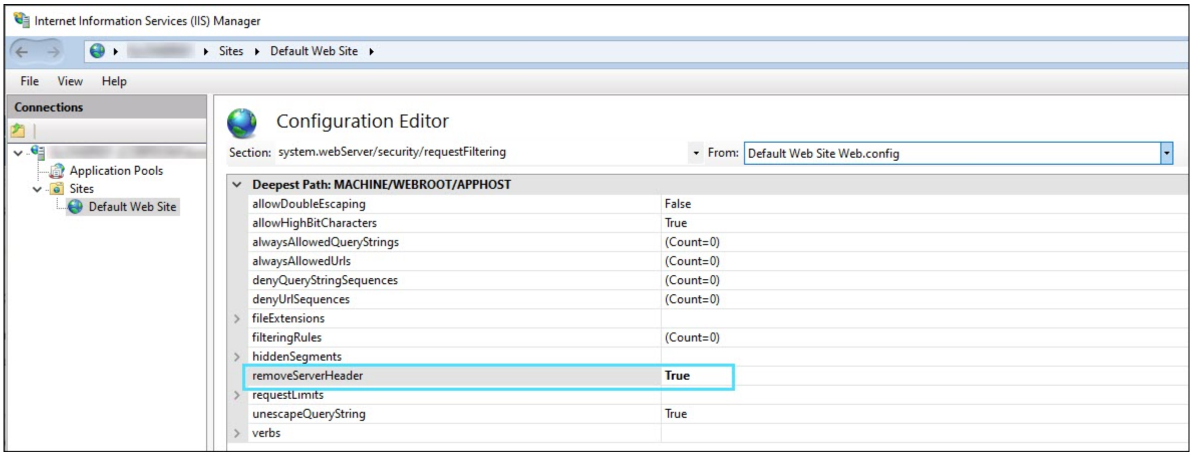
LoadRunner Enterprise information is disclosed in the IIS and ASP.NET response headers.

Troubleshooting

To prevent LoadRunner Enterprise information being disclosed in the IIS and ASP.NET response headers, we recommend removing the server- and version-specific headers from the default Web site, or any other site that was used for the LoadRunner Enterprise installation.

If using IIS 10.0 or later:

1. Open IIS Manager.
2. Select the server in Connection tree view.
3. Expand **Sites**, and select **Default Web Site**.
4. Open the Configuration Editor User Interface module, and in the Section combo box, select **system.webServer/security/requestFiltering**.
5. Change the value of the **removeServerHeader** property to **True**.



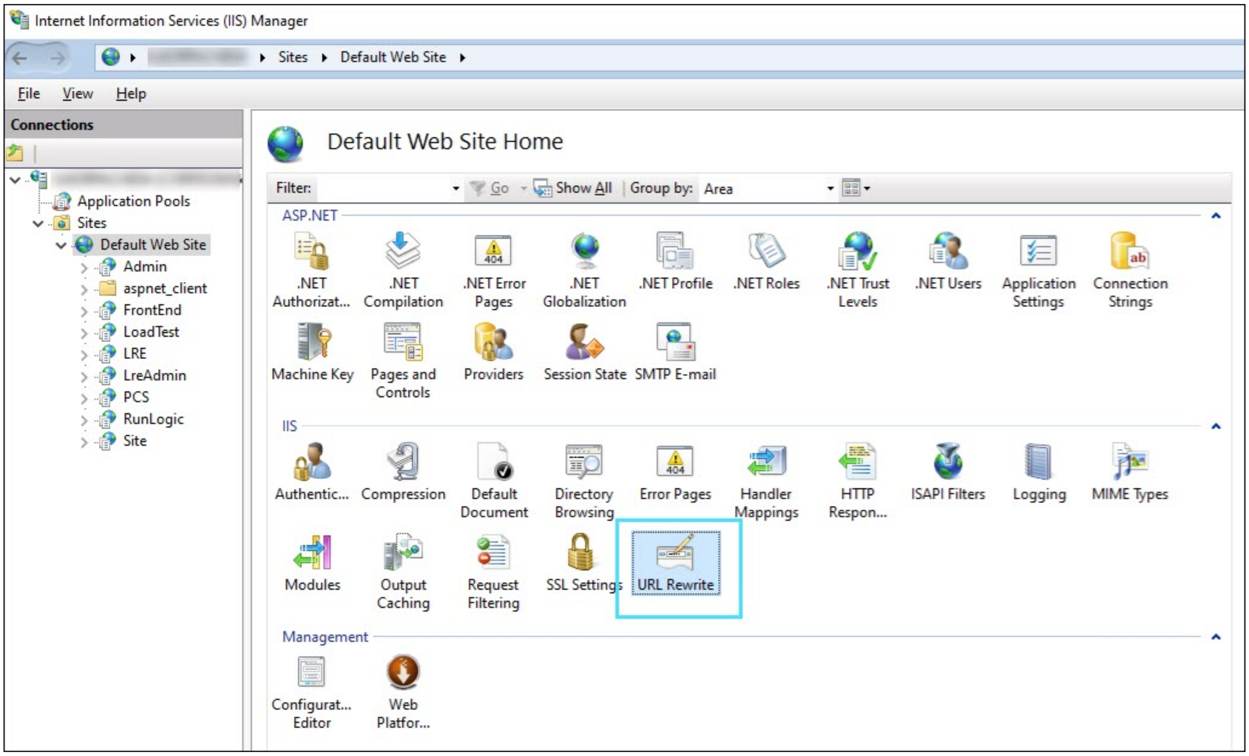
Section: system.webServer/security/requestFiltering

From: Default Web Site Web.config

Deepest Path: MACHINE/WEBROOT/APPHOST	
allowDoubleEscaping	False
allowHighBitCharacters	True
alwaysAllowedQueryStrings	(Count=0)
alwaysAllowedUrls	(Count=0)
denyQueryStringSequences	(Count=0)
denyUrlSequences	(Count=0)
fileExtensions	
filteringRules	(Count=0)
hiddenSegments	
removeServerHeader	**True**
requestLimits	
unescapeQueryString	True
verbs	

If using an earlier version of IIS:

In IIS Manager, use the **URL Rewrite** extension for removing these HTTP headers.



No error message when a test fails to start

Problem description

An error message is not issued when a performance test fails to start.

Troubleshooting

This problem is possibly caused by the configuration process. Validate the following:

- The **LoadRunner Load Testing Service** in running on the host machine under the system account.
- The LoadRunner Enterprise user (**IUSR_METRO**) exists.
- In the **wlrun7.ini,** under the **%systemroot%** folder, make sure that **IsOrchid** and **IsOrchid10** are both set to 1. For details, see Software Self-solve knowledge base article KM1098097.

Unable to display online topology monitors

Problem description

When running a performance test that contains topology, the topology monitors data is not shown. You may get the following error when clicking the topology tab view: This node does not have a monitor.

Troubleshooting

1. On the Host machine, validate that **EnableInUi** is set to **1** in **<install folder> dat\online_graphs\online_resource_graphs.rmd**
2. In Sitescope, set the monitor frequency value (by default it is set to 10 minutes). Make sure it is set for less than 10 seconds.

Unable to configure LoadRunner Enterprise server or host when the process is used by another process

Problem description

After running the LoadRunner Enterprise Server Configuration wizard, the following error is displayed in the log file:

"The process cannot access the file 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config' because it is being used by another process."

This problem occurs when the configuration updates the .NET machine.config file while it is in use by another process (for example, IIS). When the file is in use, the update fails.

Troubleshooting

Restart the machine and start the LoadRunner Enterprise Server Configuration wizard.

LoadRunner Enterprise configuration host fails to start the 'LoadRunner Center Data Service'

Problem description

After running the LoadRunner Enterprise Host Configuration wizard, the following error is displayed in the log file: **"Failed starting service 'LoadRunner Data Service'"**

This problem occurs if the **influxdb.exe** process and the LoadRunner Enterprise Host Configuration wizard are running at the same time.

Troubleshooting

Make sure the **influxdb.exe** process is not running before you run the LoadRunner Enterprise Host Configuration wizard.

LoadRunner Enterprise service fails to start after successful configuration

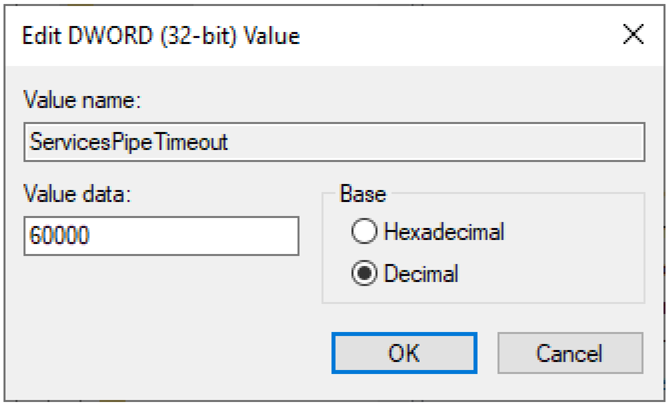
Problem description

The LoadRunner Enterprise service fails to start after successfully configuring the LoadRunner Enterprise server.

Troubleshooting

Increase the global timeout for the service startup in the Windows registry. By default, the timeout is 30000 milliseconds and the registry value does not exist.

1. Open **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control** in the Registry Editor.
2. Add a new **DWORD value** (name it **ServicesPipeTimeout**), set **Base** to **Decimal**, and type a value of 60000 (equivalent to 60 seconds).



Edit DWORD (32-bit) Value

Value name: ServicesPipeTimeout

Value data: 60000

Base

○ Hexadecimal

● Decimal

Configure LoadRunner Enterprise to work with secure cookies over a secure connection

Problem description

By default, the LoadRunner Enterprise environment works with a cookie over both HTTP and HTTPS. For requests over HTTPS only, you need to configure LoadRunner Enterprise and LoadRunner Enterprise Administration to secure the cookie.

Troubleshooting

> **Note:** By not setting the **requireSSL** cookie configuration, you may be exposing the system to increased security risks.

Setting secure cookies on LoadRunner Enterprise web pages

1. Log onto the LoadRunner Enterprise server machine.
2. Open the **<LRE server installation folder>\PCWEB\web.config** file for editing.
3. Search for ‘requireSSL’ in the file (there should be two occurrences), and set the **requireSSL** attribute to **true**.
4. Save the file.
5. Open the **<LRE server installation folder>\PCWEB\bin\HP.PC.Web.UI.UserSite.dll.config** file for editing and repeat steps 3 and 4.
6. Repeat steps 1-5 for each LoadRunner Enterprise server in the same environment.

Setting secure cookies on LoadRunner Enterprise Administration web pages

1. Log onto the LoadRunner Enterprise server machine.
2. Open the **<LRE server installation folder>\PCWEB_ADMIN\web.config** file for editing.
3. Search for the section 'httpCookies'.
   - If it exists, set the value of the **requireSSL** attribute to **true**.
   - If the section does not exist, add the following element under the **<system.web> XML** element:

     ```
     <httpCookies httpOnlyCookies="true" requireSSL="true" />
     ```
4. Save the file.
5. Repeat steps 1-4 for each LoadRunner Enterprise server in the same environment.

Unable to log on to the database server

Problem description

You receive the following error message: Problem encountered when application tried to connect to database.

Troubleshooting

Verify that the database server host name, type, username, and password are correct. Consult your database administrator if you are unsure.

Incorrect time range displayed in online graph

Problem Description

Changing the time zone on the LoadRunner Enterprise Server or any external analysis database, results in the incorrect time range being displayed when running a performance test in the online graph.

Troubleshooting

To ensure the correct time range for running the performance test is displayed in the online graph, verify the time zone is synchronized on the LoadRunner Enterprise Server and any external analysis database servers.

Unable to install Network Virtualization (NV) components

Problem Description

Windows SmartScreen prevented NVinstaller.exe from running. As a result, NV Components could not be installed.

Troubleshooting

Disable Windows SmartScreen before proceeding with the NV installation.

1. Open **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer** in the Registry Editor.
2. Change the Value data for **SmartScreenEnabled** to "Off".

Send Us Feedback

Let us know how we can improve your experience with the Installation Guide.
Send your email to: docteam@microfocus.com

MICRO® FOCUS

Java™ COMPATIBLE